Document Title:	**Technical Environment Description**
Document Type:	Architecture
Release:	S30
Abstract:	This Document describes the technical architecture of the Pathway Horizon system at BI3S30
Document Status:	Draft
Originator & Department:	Peter Wiles (Tel 7 GRO - ASD
Contributors:	
Internal Distribution:	ASD
External Distribution:	As defined by Pathway Programme Director

Approval Authorities

Name	Position	Signature	Date
Peter Jeram	Programme Director		
Tony Drahota	Pathway ASD Manager		

Chapter 0 - Document Control

0.1 DOCUMENT HISTORY

Version	Date	Reason for Issue	Associated CP/ PinICL Nos.
2.1	12/05/1997	Formal issue	
2.2		Unissued version passed from AGW to PRW	
3.0		Limited circulation Chapter by Chapter for comments	
3.1	17/12/1997	Issued to JHB Direct Reports for comments	
3.2	17/04/1998	Incorporates comments on Version 3.1. Initially issued Chapter by Chapter for Formal Review, then recombined and issued on date given.	
3.3	05/05/1998	Final draft for CSR, to be submitted for Baselining.	
4.0	10/06/1998	Initial Baseline for NR2	
4.1	25/08/1998	Incorporates Network Redesign for NR2	
4.2	14/09/1998	First draft for NR2+.	
4.3	10/12/1998	Revised Draft for NR2+	
4.4	12/03/1999	Further Draft for NR2+	
4.5		Further Draft for NR2+ [not issued]	
4.6	03/08/1999	First Draft for CSR+, incorporating removal of the BPC.	
4.7	09/03/2001	Second draft for CSR+	Various
4.8	22/10/2002	Major revision for BI3 and S30, including Network Banking Service (NBS) and Debit Card Service (DCS) and their supporting infrastructure	Various

0.2 REVIEW DETAILS

Review Comments by:	
Review Comments to:	Peter.Wiles GRO

Mandatory Review Authority	Name
ASD	Tony Drahota
Optional Review/Issued for Information	
Programme Director	Peter Jeram
Consultancy Services	Dave Hollingsworth
Development	Gill Jackson
ASD	Richard Herbert
	Allan Hodgkinson
	Mark Jarosz
	Gareth Jenkins
	Glenn Stephens
	Geoffrey Vane
APDU	Mark Taylor
	Rex Dixon
IPDU	Ian Morrison
	Simon Fawkes
	James Stinchcombe
PTU	Alan D'Alvarez
Customer Requirements	Tony Hayward

(*) = Reviewers that returned comments

0.3 ASSOCIATED DOCUMENTS

The information provided by this Document has been derived from a number of other documents that are listed below.

References in each case are to the latest Version of the document held in PVCS.

Ref	Identifier	Vers.	Title	Source
ACDBSUP	DE/SPG/002		AutoConfig Downloader/Listener Support Guide	PVCS
ACP	RS/POL/003		Access Control Policy	PVCS
ACSRR	TD/DES/094		Agent and Correspondence Server Resilience and Recovery at Release 2+	PVCS
ADEF	SD/DES/116		Audit Data Extraction & Filter High Level Design Specification for CSR+	PVCS
ADSR	SD/DES/115		Audit Data Storage & Retrieval High Level Design Specification for CSR+	PVCS
AOO	AD/PDN/001		Pathway Agents: Operational Overview for CSR+	PVCS
APSCHLD	AP/DES/012		APS Counter High Level Design Specification	PVCS
APPRHLD	TD/DES/034		High Level Design for Application Recovery after Fail-over using Maestro	PVCS
APSHLD	AP/DES/004		APS Design Specification (Release 2+)	PVCS
APSHHLPD	AP/DES/015		APS Host High Level Physical Design	PVCS
APSMART	AP/DES/006		Implementation of Smart and Memory Cards for APS	PVCS
APSSUP	AP/DOC/003		APS Support Guide	PVCS
APSWS	AP/DOC/002		APS Workstation User Guide	PVCS
ATFS	CR/FSP/006		Audit Trail Functional Specification	PVCS
AUDITARC	TD/ARC/016		Audit Architecture	PVCS
AUDM	IA/MAN/005		Horizon System Audit Manual	PVCS
AUDP	RS/POL/005		ICL Pathway Audit Policy	PVCS
AUTOCF	TD/DES/097		AutoConfig Requirements for CSR+	PVCS
BUSVOLS	PA/PER/032		Horizon Existing Service Business Volumes	PVCS
BUSVOLSN	PA/PER/031		Horizon New Service Business Volumes	PVCS
CA	BP/CON/180-253		Codified Agreement	PVCS
CAORR	TD/DES/050	.0	CAPS and OBCS Access Service Interfaces - Resilience and Recovery for Release 2	PVCS
CCFG	TD/DES/087		CacheCfg High Level Design Specification	PVCS
CNTD	BP/DES/003		Counter Hardware Design Specification	PVCS
CNTSUP	SY/MAN/004		Steady State Counter Management Support Guide	PVCS
CRYPT	RS/DES/001		Cryptography Design	PVCS
CRYPTA			Cryptographic Architecture	T.A.Parker
CSMSR	TD/DES/086		Correspondence Server Message Store Backup and Recovery for Release 2	PVCS
CTRSCH	TD/DES/109		Counter Application Scheduler HLD	PVCS
DWHARC	DW/ARC/010		CSR+: Data Warehouse Architecture Specification	PVCS
DWHLD	DW/HLD/002		BI3 Data Warehouse High Level Design Specification	PVCS
EACRR	SY/SOD/002		ACRR Improvements for Network Banking - System Outline Design	PVCS

EPOSSHLD	EP/DES/019		EPOSS High Level Design	PVCS
EPOSSSUP	EP/MAN/001		EPOSS Operational Support Guide	PVCS
EVL	RS/REQ/007		Event Logging and Error Reporting Policies for Crypto Code	PVCS
FAILSAFE	Startup.doc	0.1	NT Fail-safe Start-up	M.Conneely
FTMS	TD/DES/107		File Transfer Managed Service at CSR+	PVCS
FTMSRR	TD/STR/007		FTMS Resilience and Recovery Strategy for CSR+	PVCS
FTMSSUP	TD/MAN/015		FTMS Support Guide	PVCS
FW	TD/DES/038		Network Infrastructure Firewall Requirements	PVCS
FWCONFIG	SD/DES/103		FireWall-1 ~ Logical Filter Requirements	PVCS
GENAPI	TD/STD/004		Generalised API for OPS/TMS	PVCS
HADDIS	TD/STD/001		Host Applications Database Design and Interface Standards	PVCS
HOSTSS	TD/STR/001		Host Systems Storage Strategy	PVCS
HUTHDR	CR/PRP/004		POCL Disaster Recovery Interface Service Proposal	PVCS
IMPSTRAT	IM/STR/026		Installation Strategy	PVCS
ISDNSUP	DE/SPG/001		ISDN Call Monitor Support Guide	PVCS
KMACDB	RS/DES/041		KM Interfaces with AutoConfig Process	PVCS
KMADF	RS/REQ/014		Interface Specification for KMA Data Feeds	PVCS
KMAHLD	RS/DES/018		KMA Design	PVCS
KMHLD	RS/DES/010		Key Management High Level Design	PVCS
KMICDD	RS/DES/032		KM Interactive Channel Detailed Design	PVCS
KMP	RS/DES/020		Key Management Platform Specifications	PVCS
KMPG	RS/PRO/037		Key Management Process Guide	PVCS
KMPROXY	RS/DES/060		KM Proxy Detailed Design	PVCS
KMSSUP	RS/MAN/012		KMS Support Guide for SSC	PVCS
LFS	LF/DES/003		Logistics Feeder Service - High Level Design	PVCS
LFSSUP	LF/MAN/001		Logistics Feeder Service Systems Management Support Guide	PVCS
LIFT	D06A-9999-B057/01		Financial Keyboard Specification	Fujitsu Australia Ltd
LUC	AD/DES/036		High Level Design of Cluster Lookup Service for CSR+	PVCS
MBS	SD/DES/128		CSR+ Message Broadcast Service	PVCS
MISARCH	DW/ARC/001		Data Warehouse: Architecture Specification	PVCS
MISDES	TD/DES/115		MIS CSR+ SIP14 Infrastructure Design	PVCS
MISSUP	DW/PRD/123		CSR+ DWh: Operational Support Guide	PVCS
NBSE2ESDS	NB/SS/007		System Design Specification for Network Banking End-to-End Service	PVCS
NBSSUP	TD/MAN/020		Network Banking Support Guide	PVCS
NFR	TD/REQ/004-018		Non-Functional Requirements Catalogue	PVCS
NTDOM	RS/DES/080		NT Domain Structure Design for Pathway	PVCS
NTIMP	RS/DES/081		Implementation Build Guide for NT Platforms	PVCS
NTSEC	RS/DES/081		Implementation Build Guide for NT Platforms	PVCS
NUMAQ			NUMA-Q 2000 Framework Strategy	C.Phillips (Sequent)
NWARCH	TD/ARC/002		Network Architecture	PVCS
NWD	TD/DES/059		Network Infrastructure High Level Network Design - CSR & CSR+	PVCS
OBCS	BP/DES/008		OBCS Design Specification	PVCS
OBCSCNTR	OB/DES/007		OBCS High Level Design – Counter	PVCS
OBCSSUP	OB/MAN/002		OBCS Operational Support Guide	PVCS
OCMSHLD	TD/DES/106		Outlet Change management Service High Level Design	PVCS

OLS	PA/PRO/025		Pathway On-Line Standards	PVCS
OPSMENU	SD/SPE/016		Horizon OPS Menu Hierarchy	PVCS
PBS	SD/DES/001		Product Breakdown Structure Meta-Model	PVCS
PCCSUP	DE/SPG/005		AutoConfig PCConfig Products Support Guide	PVCS
PERFOV	PA/PER/005		Pathway Performance - Overview	PVCS
PERFSERV	PA/PER/007		Pathway Performance - Services	PVCS
PIU			Counter Revolution – Modernising the Post Office Network	Govt. Performance and Innovation Unit
PIURESP	CR/REP/021		The PIU Report - Pathway Analysis & Commentary	PVCS
PMSHLD	TD/STR/002		Pathway Performance Management Service Design	PVCS
PMSSOD	PA/PER/030	.1	Performance Management Service Outline Design	PVCS
R2RESIL	TD/DES/031		Release 2 Resilience and Recovery Strategy	PVCS
RDDSHLPD	RD/DES/047		RDDS High Level Physical Design	PVCS
RDMS	RD/DES/046		RDMC High Level Physical Design	PVCS
RMDSSUP	RD/MAN/006		RDDS Host System Support Guide	PVCS
RECONFIG	Reconfig.doc		Autoconfiguration Design Proposal	PVCS
RKM	RS/REQ/009		Requirements for Key Management	PVCS
SADD	CR/FSP/004		Service Architecture Design Document	PVCS
SCO	TD/DES/048		Riposte Mirroring for Single Counter Outlets at Release 2	PVCS
SDSINF	TD/SDS/001		System Design Specification for 2001/02 Horizon Infrastructure Enhancements	PVCS
SECURID	RS/DES/004		Use of SecurID Token Authentication for Release 2	PVCS
SFS	RS/FSP/001		Security Functional Specification	PVCS
SPOL	RS/POL/002		Pathway Security Policy	PVCS
SSHSUP	DE/SPG/003		OpenSSH Auditing and Logging Server Support Guide	PVCS
STYLE	SD/STD/001		Pathway Horizon Office Platform Service Style Guide	PVCS
SWDIST	SY/MAN/002		Horizon Software Distribution	PVCS
TIMESV	TD/DES/030		Time Services Specification	PVCS
TIMSUP	SY/MAN/001		Time Services Support Guide	PVCS
TIVOLI			High Level Tivoli Design Approach for Sorbus - Pathway Project	PVCS
TPS	TI/DES/001		TPS Host Technical Specification	PVCS
TRC	Remcon.doc		SYSMAN - Tivoli Remote Console Facility	PVCS
VPN	TD/ARC/019		VPN Architecture	PVCS
VPNHLD	RS/DES/046		VPN High Level Design	PVCS
VPNLAN	RS/DES/073		Systems Outline Design for Encryption of the Outlet LANs using VPN	PVCS
VPNSUP	RS/MAN/009		VPN Operational Support Guide	PVCS

Note: This document was first published before an Approved version of PA/TEM/001 existed.

0.4 Abbreviations & Definitions

Hyperlinks within the *Definition* of a Term in this Sub-Section are in general links to the definition itself within this Sub-section. Hyperlinks from the *Term* itself point to the most complete use or detailed specification of the term within the body of the Document.

0.4.1 Abbreviations

Term	Definition
10baseT	LAN standard for communication over UTP at 10 Mbps
100baseT	LAN standard for communication over UTP at 100 Mbps
ACC	{DSS} Area Computer Centre; contains a VME-based SX mainframe system with which Horizon needs to interwork
ACDB	Auto Configuration Data Base
ACE	{ACE/Client and ACE/Server are trademarks of Security Dynamics Ltd}
ACF	Auto Configuration File; file, unique to each Counter position, that is maintained by the Auto Configuration Database Server and "replayed" to the Counter when needed
ACL	Access Control List
AIS	Application Interface Specification; part of an Application's design documentation
AP	Automated Payments
API	Application Programming Interface
APPU	Automated Payment Peripheral Unit; used to read and recharge Smart Cards issued by the Utilities
APS	Automated Payment Service; provided by POCL to the utilities and implemented in Horizon
AS	Agent Server; part of the vertical Application structure
ASCII	American Standard Code for Information Interchange
ATE	Automatic Targeting Engine; Tivoli enhancement that smooths the flow of software distribution modules to a rate that does not overload the ISDN Routers.
ATM	Asynchronous Transfer Mode; very efficient fibre-based protocol running at 155 Mbps
BA	{DSS} Benefit Agency
BMC	{Supplier of Patrol Systems Management software}
BST	British Summer Time
BT	British Telecom
C	{A UNIX-derived programming language}
C++	{Object oriented version of C}
CAPO	Card Account at Post Office; the official brand name of POCA (Post Office Card Account).
CESG	Communications Electronic Security Group; Government organisation based in Cheltenham with responsibility for the

	use of encryption within Government contracts
CHAP	Challenge Handshake Authentication Protocol; Microsoft protocol used prior to CSR+ to support authentication in **ISDN**
CIR	Committed Information Rate
CKS	Crypto Keystore Service
CLIP	Calling Line Identity Presentation; BT facility whereby a called ISDN service can be informed of the telephone number of the caller
COM	{Microsoft} Common Object Management(?)
CORBA	Common Object Request Broker Architecture; support infrastructure used by Tivoli
COS	COS/Manager is a product which enhances the security of Sequent Dynix systems
CP	Change Proposal
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CS (2)	Correspondence Server; part of the vertical Application structure
CS (1)	Pathway Customer Services
CSR	Core Systems Release
CSR+	Core Systems Release plus
CSV	Comma Separated Values
DCE	{OSF} Distributed Computing Environment
DCOM	{Microsoft's} Distributed Common Object Management
DCS	Debit Card System; Horizon service that supports payment by Debit Card
DDL	Data Description Language
DLL	Dynamic Link Library
DLT	Digital Linear Tape
DMZ	De-Militarised Zone; area behind a Firewall
DNS	Department of National Savings; a Client of POCL
DSA	Digital Signature Algorithm; part of X.509 standard. It is an asymmetric crypto algorithm that can be used to sign data so that it can be verified without needing to know the Private Key used to create the signature
DSS	Department of Social Security; a Client of POCL. Now renamed *Department of Work and Pensions* DWP)

DWP	Department of Work and Pensions; previously known as the DSS
E3	34 Mbps ATM link
EACRR	Enhanced ACRR - A new improved ACRR introduced at BI3
EAM	Equipment Access Module; node on the Energis fibre connections from which a tap is taken into a Campus
EDS	Electronic Data Systems. They run the DSS VME Mainframes at the ACCs.
EFT	Electronic Funds Transfer
EFTPoS	Electronic Funds Transfer at Point of Sale; generic industry name for the service provided by DCS in Horizon
EMC	{Supplier of disks for Sequent Servers}
EoD	End Of Day
EPOSS	Electronic Point Of Sale Service; Counter application supported by Horizon
ESNCS	Electronic Stop Notice Control System; DSS system that provides Stop Notices for stolen, expired or fraudulent Benefit Books.
FAD	Financial Accounts Division {part of POCL}. A FAD Code is used to identify an Outlet
FCS	Fujitsu Core Services
FDDI	Fibre-optic Distributed Data Interface
FEK	Filestore Encryption Key
FR	Frame Relay
FRIACO	Fixed Rate Internec Access Call Origination
FSCS	Fujitsu Services Core Services
FTF	File Transfer Facility
FTMS	File Transfer Managed Service; application that is configured to support the needs of particular pairs of External Interface Gateways
FTP	File Transfer protocol
GB	Gigabyte
Gbps	Giba*bit* per Second
GINA	Graphical Identification and Authentication DLL; responsible for user authentication in Windows NT
GMT	Greenwich Mean Time. Some authorities with no sense of history choose to call this Universal Time Co-ordinate, or UTC. Not here, we don't.

GPS	Global Positioning System; used to derive accurate Time information for servers
GUI	Graphical User Interface
HCI	Human Computer Interface
HLD	High Level Design
HMG	Her Majesties Government
HP	Hewlett Packard
HSO	{VME} High Security Option
HTML	Hypertext Mark-up Language; standard used for production of Internet type pages
IP	Internet Protocol
IPR	Intellectual Property Rights
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ISV	Independent System Vendor
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria; set of joint criteria adopted by the Governments of several European countries
K-value	{Random string used to generate a crypto key}
Kbps	Kilo*bits* per Second
KEK	Key Encrypting Key
Kerberos	{**OSF** supplied distributed security mechanism}
KMA	Key Management Application
KMAS	KMA Server
KMS	Key Management Service
LAN	Local Area Network
LAR	Logical Access Router
LCR	Logical Campus Router
LFS	Logistics Feeder System; interface to PO Ltd's SAPADS system, used to ensure that Outlets have adequate and timely supplies of stock including cash.
LLD	Low Level Design
LSA	Local Security Authority; part of the Windows NT security architecture
LUC	{Multi-Cluster} Look Up Server; called by an Agent to identify which Cluster an Outlet belongs to

MA	Merchant Acquirer
MB	Megabyte
MB/sec	Mega*bytes* per Second
Mbps	Mega*bits* per second
MIS	Management Information System
MKS	Managed Key Service
MoP	Method of Payment: cash, credit card, debit card, television stamps etc.
NAO	National Audit Office
NDIS	Network Device Interface Standard
NFS	Networked File System
NIFTP	Network Independent File Transfer Protocol
NMS	Network Management Server; platform used to perform network management functions.
NTFS	Windows NT File System
NTP	Network Time Protocol
NUMA	Non Uniform Memory Addressing
NUMA-Q	{Sequent implementation of NUMA architecture}
OBCS	Order Book Control Service; application which supports a similarly named DSS application
OCMS	Outlet Change Management System
OCX	OLE Custom Control
ODBC	Open Database Connectivity
OLAP	{Oracle's} On-Line Analytical Processor
OLE	Object Linking and Embedding {Microsoft standard}
OPS (1)	Oracle Parallel Server
OPS (2)	Outlet Processing System
OSF	Open Software Foundation
OSI	Open Systems Interconnection
PC	Personal Computer
PO Ltd	PO Ltd
PVCS	{Configuration Management tool used by Pathway}
PFI	Private Finance Initiative
PIN	Personal Identification Number
PinICL	Internal Pathway incident tracking database used to support development, and the operational service (via HSHD)

PK	Public Key
PL/SQL	Procedural Language FOR Oracle Databases
PMMC	Post Master's Memory Card
POCL	Post Office Counters Ltd
POLO	Post Office Log On; process used by Post Office Managers when switching on a Counter PC
PPP	Point-to-Point Protocol
PRI	(ISDN) Primary Rate Interface; server level interface supporting 30 concurrent ISDN connections
PSBR	Public Sector Borrowing Requirement
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QCIC	
RAD	Rapid Application Development
RAID	Redundant Array of Independent Discs
RAMBUTAN	{Hardware crypto algorithm devised by CESG}
RAP	Remote Authentication Process
RCD	Release Contents Description; Pathway document defining the contents of a Release
RDBMS	Relational Data Base Management System
RDDS	Reference Data Distribution Service
RDMC	Reference Data Management Centre; Application which feeds "soft" data to Counter Applications
RDMS	Reference Data Management System; ditto
RIPOSTE	Retail Integrated Point Of Sale system in a Transaction Environment; infrastructure product from Escher which supports the core of the Horizon architecture
RMS	Riposte Message Service; message storage and replication mechanism which runs on Correspondence Servers and Counter PCs
RPC	Remote Procedure Call
SAS	Secure Attention Sequence {in Windows NT}
SCSI	Small Computer Systems Interface
SDH	Synchronous Data Hierarchy
SHA	Secure Hash Algorithm
SHVS	(Intel's) Single High Volume Server
SI	Software Issue

SLA	Service Level Agreement
SLAM	Service Level Agreement Monitor ; an MIS Application
SLCA	Service Level Contract Administration; an MIS Application
SMA	Synchronous Multiplexor Add-drop; terminator on the Energis connection from an EAM into a Campus
SMG	FSCS Systems Management Group at Lytham St Annes
SMP	Symmetric Multiple Processor
SMS	Streamline Merchant Services; subsidiary of Royal Bank of Scotland that provides Merchant Acquirer services to PO Ltd in support of DCS
SNMP	Simple Network Management Protocol
SOD	System Outline Design; document produced at an early stage in the specification of an Application
SQL	Structured Query Language; language commonly used to access Relational Database systems
SRDF	Symmetrix Remote Data Facility; EMC technology used to replicate disk array data between two Campuses
SSC	{Pathway} System Support Centre based at Bracknell.
TACACS	Terminal Access Controller Access Control System; used to authenticate Telnet and other access to Campus systems. It runs on the Network Management Server
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TED	Technical Environment Description; this document
TIP	Transaction Information Processing; PO Ltd Application which handles transaction data returned from Horizon
TME	Tivoli Management Environment; suite of systems management products
TMR	Tivoli Management Region; hierarchical subset of the total systems management load where manageability, security or scalability constraints make it unwise to support the entire system in one unit
TMS	Transaction Management Service; contractual name for some of the services carried out by Riposte
TPS	Transaction Processing System; application which collects transaction information and returns it to TIP
TPMS	Transaction Processing Management System; VME infrastructure product
UDP	User Datagram Protocol
UKSS	United Kingdom System Service; Help Desk that handles

	hardware failures and replacements in Outlets
UNIX	{Widely used operating system available in a number of variants}
URL	Uniform Resource Locator; an Internet web site identifier
UTC	Universal Time Co-ordinate; virtually equivalent to GMT but a term that doesn't upset the French
UTP	Unshielded Twisted Pair; standard for cabling within offices
VB	Visual Basic; PC application development tool
VME	Virtual Machine Environment; operating system of the Fujitsu SX mainframe systems
VPN	Virtual Private Network; security service that provides encryption over the ISDN links between Outlets and Campuses, and over the Outlet LAN
WAN	Wide Area Network
XA	{An X/OPEN transaction demarcation protocol}
Z	{Conventional symbol for an} Encryptor

0.4.2 Definitions

The following terms, when capitalised as shown, have specific meanings that are used throughout the TED.

Term	Definition
Access LAN	LAN in the Campuses to which all Outlets are linked via appropriate Routers. It is separated from the VPN Layer by the Logical Access Routers.
Agent	A Process which transforms data passing between the Host Layer and the Counter Layer. It usually, though not always, runs on an Agent Server.
Agent Layer	Architectural layer containing the services running on the Agent Servers
Agent Server	Platform running under Windows NT Server which provides a transformation between the data used by Riposte and that used by the Host or Client
AP Client	A Client of POCL for whom PO Ltd provides Automated Payment (AP) services using swipe or Smart Cards
Application	A self-contained collection of data and code which satisfies all the data processing requirements of a particular corporate function
Archive Service	Service running on an Audit Server. Responsible for writing all necessary audit information to bulk storage media., and for retrieving it should this be necessary

Audit Server	Server responsible for gathering audit information; writing it to DLT tapes for long-term storage; and retrieving it when needed.
Audit Workstation	Workstation at the Campuses or Pathway's Feltham HQ used for access to audit data
Authentication Server	Server in each Campus running the ACE/Server and Enterprise Centre services; used for additional authentication of users requiring access to Campus servers and Routers
Auto-Configuration Database	Database which is populated with details of Outlets which are scheduled to be installed in the near future, and used by Counter PCs at the Outlet when it is first switched on
Bar Code Reader	Hand held device attached to a Counter PC. Used to read a bar code from a document or retail item.
Boot Server	Windows NT server within each Campus which is the first location accessed by a newly installed Counter PC
Bubble Help	Help information obtained on a Counter PC by touching an "information" Icon before touching another Icon
Build	Combination of a specific Platform type and a set of Capsules running on that Platform
Bulk Harvester Agent	Agent which reads a potentially large amount of information from Riposte in bulk
Bulk Loader Agent	Agent which loads information into Riposte in bulk
Business Volumetrics	Workload information provided by PO Ltd during the Procurement process
Button	Icon on the Riposte Desktop which can be "pressed" by the user to invoke a particular action.
CA Workstation	Secure Workstation used to hold the current Certification Authority certificate that verifies Public Keys in Horizon.
Campus	One of two Data Centres, located at Bootle and Wigan, which contain the main Horizon servers
Campus LAN	High-speed (100baseT) LAN linking most of the Platforms in a Campus
Capsule	The minimum portion of any Application which must run within a single Platform
Checkpoint	Riposte facility to generate and store a Marker over all Outlets
Customer	A member of the public transacting, or seeking to transact, business with PO Ltd through any of the Services
Client	Customer of PO Ltd which uses the Horizon functionality to sell or provide goods or services to **PO Ltd** customers.
Client System	Computer system owned by a POCL Client and with which Horizon is required to interwork

Cluster	Group of Correspondence Servers which support a common set of up to 5,000 Outlets. All messages related to these **Outlets** are replicated across all members of the Cluster
Collection	Riposte pseudo-database. Records are keyed by Outlet, type and other information
Corporate System	Computer system supporting the management needs of Pathway
Correspondence Layer	Architectural layer containing the services running on the Correspondence Servers
Correspondence Server	Platform running under Windows NT Server which supports the Riposte Message Service and interfaces to both Agent Servers and Counter PCs
Counter Application	Component of an Application which is implemented on the Counter PC and provides functionality which is visible to the Counter Clerk
Counter Clerk	User of a Counter PC in an Outlet
Counter Layer	Architectural layer containing the services running on the Counter PC
Counter PC	PC and associated peripherals used to provide a range of counter services within an Outlet
Crypto Key	Generic name for a piece of information used to encrypt or decrypt some other piece of data
Cryptware Server	Secure server holding the Certification Authority certificate used to verify the VPN Keys.
Data Warehouse	Computer system which contains a wide variety of information relating to the services carried out by Pathway
Derived Volumetrics	Volumetric information derived from the supplied Business Volumetrics and modified by a knowledge of the operation of the Horizon system
Diffie-Hellman	A cryptographic protocol which enables two end-points using symmetric encryption to mutually establish a shared secret that can be used as the key for further communication between them.
Domain Controller	Windows NT server Platform used to control Log-on to other Windows NT servers and workstations
Energis	Supplier of Wide Area Network services to Pathway
Enquiry Agent	Agent which listens for a message from a Counter PC and obtains a response which is passed back to the Counter
Enterprise Centre	Name for the system that is used to configure Firewalls. It runs on the Authentication Server.
External Interface Gateway	Platforms, used in pairs with one in a Campus and the other on a remote site; used to transfer data between Horizon and the site

Firewall	Network component which protects a network from malicious access by users on the outside
Flat File	File with no inherent structure; a logical structure may be imposed by the Application which generates the file
Frame Relay	Switching protocol used over the Energis ATM Network for connection to suppliers and some Outlets
Gateway PC	One PC within a multi-Counter Outlet, used to support communication with the Campus on behalf of the other Counter PCs
Group	Riposte name for a number of Counter PCs at the same Outlet. Messages generated at one are replicated on all other members of the Group
Help Desk	Set of users who answer telephone calls from Outlet, PO Ltd or Client staff
Horizon	Horizon is the name used by PO Ltd to describe the system made available to Outlet staff. In this document, it is further used to describe the infrastructure that supports and provides those services.
Horizon Systems Help Desk	Help Desk used by Outlet staff who encounter problems with the Counter PCs and other kit supplied by Pathway
Host Layer	Architectural layer containing the services running on the **Host Servers**
Host Central Server	**Host Server** based on a Sequent NUMA-Q Server
Host Server	A server running the part of an Application which provides business functionality and persistent data storage
HP OpenView	Network management software from HP used to manage network components
Impulse	Riposte feature whereby an event happens on a peripheral (for example a swipe of a magnetic card) and an associated procedure is automatically invoked
Interactive Harvester Agent	Agent which runs continuously listening for the appearance of a Riposte message of a particular type
Interactive Loader Agent	Agent which runs continuously listening for a record appearing in a Host database; when one appears, it writes it to Riposte
Key	See Crypto Key
Key Management	Covers the tasks involved in the generation, distribution and revocation of keys used for encryption
KMA Server	Server used to hold the Key Management Database. It is responsible for the distribution of new Keys to platforms that require them.
Logical Access	Router which separates the Access LANs from the VPN Servers

Router	
Logical Campus Router	Router which separates the main Campus LAN, to which the Campus Servers are attached, from the LAN(s) used to connect to the VPN Servers
Maestro	Now renamed Tivoli Workload Scheduler; a scheduling package from Unison Software (now part of IBM), used to schedule work on Host and Agent Servers
Marker	Riposte facility to obtain and store the latest message sequence numbers for all Counters in an Outlet
Client PC	PC used within Pathway to extract or view management information from the MIS
Mode	Riposte facility to define the state of a Counter PC. Certain Desktop functions are not available in some Modes
Network Management Server	SUN Solaris Server in each Campus running HP OpenView, used to manage the Routers, Hubs and other network equipment
Order Book	Book containing coupons each of which entitles the holder to receive a benefit payment.
Outlet	Post Office or Sub Post Office location
Pathway	Fujitsu Service (Pathway) Limited
Peripheral Broker	Riposte component which handles peripherals attached to a Counter PC
Peripheral Impulse	see Impulse
Persistent Object	Riposte messages used for permanent storage of standard values and other data
PIN Pad	Hardware device that is attached to a Counter PC and used by the customer to enter a PIN value to authenticate a financial transaction
Platform	A computer of a particular type running a particular set of Capsules
POCL Client	An organisation for which PO Ltd provides Counter services in its Outlets.
PowerHelp	Support Help Desk system used on the Horizon Systems Help Desk
Product Breakdown Structure	Way of defining the set of system components which go to comprise Builds and Releases
Priority Message	Riposte message which causes the ISDN Line between the Outlet and the Campus to be raised immediately; all pending messages are then transferred in each direction

Private Key	Crypto Key that is part of a Public/Private Key Pair used in an assymetric encryption process. It must be kept secret by the owner of the key pair. Data encrypted under the Private Key can be decrypted by anyone in possession of the Public Key.
Public Key	Crypto Key that is part of a Public/Private Key Pair used in an asymmetric encryption process. It is exposed to other parties that may need to communicate with the owner of the key pair. Data encrypted under the Public Key can only be decrypted by use of the Private Key.
Public/Private Key Pair	Pair of Crypto Keys, one of which is kept secret by the owner and the other which is published to anyone who may wish to communicate with the owner or verify a signature generated by the owner.
Real Time Message Port	Means of obtaining Priority Messages as soon as they arrive at the Correspondence Server, rather than when they arrive in their normal sequence
Red Pike	Symmetric encryption algorithm originating in CESG and used for a number of purposes within Horizon
Reference Data	Data used to populate and control the operation of the Counter Applications
Release	A Build which is authorised for delivery onto the live systems
Retail Broker	Riposte component which handles EPOSS Counter Applications
Secret Key	Crypto Key which is used in a symmetric encryption process, and thus must be kept secret by the two parties to the exchange.
SQL Server	Microsoft database product (part of Back Office) used by the Auto Configuration Database, Key Management Application and Outlet Change Management Service
TeamWARE Crypto	Filestore encryption product used on Counter PCs to encrypt the Riposte Message Store and swap file. It uses the Red Pike algorithm. The filestore is unlocked by information held on the PMMC.
Time Server	Server which broadcasts a time signal for all servers on the Campus LAN to synchronise with
Tivoli Management Environment	Suite of Systems Management software
Tivoli Software Distribution	Component of **Tivoli** responsible for software distribution
TME Management Framework	Set of Tivoli software used to provide underlying systems management services to both managed and managing systems
Touch Screen	Display screen which responds to a user touching the screen surface as if he or she had “clicked” a Mouse button at that point

VPN Server	Server which acts as a VPN gateway between the Campus LAN and the Access LAN, and has the ability to encrypt or decrypt traffic to and from external locations such as Outlets

0.5 CHANGES AT THIS VERSION

0.5.1 Changes Between Versions 4.8 and 4.7

0.5.1.1 General

ICL Pathway is now known as "Fujitsu Services (Pathway) Limited", abbreviated in this Document to "Pathway".

Changes made at this Version are printed and displayed in a red font, like this.

0.5.1.2 Releases Covered

This includes changes introduced at the following Releases:

▪ M1	
▪ S03	
▪ S06	
▪ S10	
▪ BI1	SYSMAN facilities for NBS
▪ S11	
▪ BI2	Infrastructure enhancements for NBS
▪ S20	
▪ BI3	Introduction of NBS
▪ S30	Introduction of DCS

and their intervening "buckets" (e.g. BI2R)

0.5.1.3 Introduction of NBS

The most significant change is the introduction of the *Network Banking Service* (NBS). This has a significant impact on the Horizon infrastructure, and generates a large number of changes throughout this Document

0.5.1.4 Introduction of DCS

In parallel with the development of NBS, the Horizon system is also enhanced to support the *Debit Card System* (DCS), which provides *Electronic Funds Transfer at Point of Sale* (EFTPoS) facilities for debit cards.

0.5.1.5 Removal of Redundant Platforms

A number of Platforms whose removal was foreshadowed in the previous Version have been removed from the Document. These platforms are made redundant for one of the following reasons.

- The completion of the Outlet rollout has removed the need for the Rollout Database Server (RoDB) and its clients
- Similarly, the ECCO Migration Laptops and their Migration Agent Server are no longer required
- Completion of the migration of all AP Clients to a direct connection, rather than via HAPS, removes the need for the HAPS platforms
- The SLAM Cache DB Server has been removed as it is no longer needed

0.5.1.6 Other Changes

POCL has changed its name to PO Ltd. This is reflected in the document, other than in the names of Platforms and other configuration items (such as Crypto Keys) where it is thought unnecessary to change the names at this point.

0.5.2 Changes Between Versions 4.7 and 4.6

0.5.2.1 PSTN Replaced by Frame Relay and Satellite Links

PSTN is now no longer to be provided as an Outlet connection mechanism at CSR+. It may be introduced at a future Release. At CI4R, satellite communications are introduced for those Outlets that cannot be reached by ISDN. The satellite infrastructure uses the Frame Relay mechanisms already introduced.

0.5.2.2 Systems Management

Chapter 12 “Systems Management” has been extensively restructured. It includes a description of the systems management products developed for Pathway by the FSCS SMG.

0.5.2.3 Supportability

Chapter 14 "Usability" has been enhanced to include some initial consideration of the ways in which "supportability" is built into the system design and operation.

0.5.2.4 Structural Changes

In each case where the horizontal application structure is described, the descriptions are now ordered “bottom up”, with the Counter layer described first and the external interface layer last.

0.5.3 Changes between Versions 4.6 and 4.5

0.5.3.1 Removal of the Benefit Payment Card

V4.6 incorporates the profound consequences of removing the Benefit Payment Card (BCP) from the Pathway system. This arises from the outcome of the long-standing Treasury Review of Pathway, and the change of direction by Government in response to DSS' lack of interest in, or inability to, continuing with the BCP.

The changes as a consequence of this are too numerous to mention here. In summary, any mention of the following has been removed:

- BES
- BPS
- CAPS
- CMS
- De La Rue
- FCMS
- OSI/TP
- PAS
- Parcel Force
- Royal Mail
- Thomas De La Rue

The somewhat smaller Releases NR2 and NR2+ have been renamed as CSR and CSR+.

Platforms and communications links purely involved in supporting the BPC applications have been removed, and code involved only in those applications has been removed from the remaining platforms.

The Host systems have been simplified.

0.5.3.2 Structural Changes

Architecture Team maintains an architectural database that records all Platforms, applications and their components and other data that underpins this Document. Data from Reports generated by that Database has been incorporated at appropriate points within this Document.

0.5.3.3 Other Changes

0.5.3.3.1 Chapter 16 - Security

The range of Crypto Keys managed by KMS at CSR+ has been restricted. The remaining Keys will be managed by KMS at a Release provisionally known asR3.

0.5.4 Changes between Versions 4.5 and 4.4

0.5.4.1 Chapter 9 - Network Services

Logical Campus Routers (LCRs) renamed Logical Access Routers (LARs), and Logical Fanning Routers renamed Logical Campus Routers (LCRs).

Data Warehouse and Host Central Servers connect via what is in effect a separate LAN to the Campus WAN Routers.

Revised network connections to take account of the fact that the RoDB Server is now in Feltham.

Removal of direct access from Oracle and Sequent.

0.5.4.2 Chapter 10 - Platforms

As directed by Chapter 16 "Security", anti-virus software is required on all Workstations except those in Outlets.

0.5.5 Changes between Versions 4.4 and 4.3

- Additional material on Key Management, including updates to the list of Platforms involved.
- Additional material on VPN.

0.5.6 Changes between Versions 4.3 and 4.2

0.5.6.1 Changes for CSR+

- Inclusion of KMS Platforms and Application components.
- Inclusion in Chapter 10 "Platforms" of Sequent's latest NUMA-Q framework strategy.

0.5.6.2 Changes between CSR and CSR+

- Replacement of SE70 Host Central Servers by NUMA-Q servers clustered with the Data Warehouse server.
- Use of the Data Warehouse node as the principal failover system for the Host Central Server, with the second Campus acting purely as a disaster standby site for the principal Campus.

0.5.7 Changes between Versions 4.2 and 4.1

0.5.7.1 Introduction of CSR+

Version 4.2 reflects the first draft of the TED for CSR+. Changes indicated in V4.1 as intended for CSR+ have been brought into the main body of the document.

In addition, the network design for CSR continues to evolve.

0.5.8 Changes between Versions 4.1 and 4.0

0.5.8.1 Chapter 2 - Business Context

Updated to reflect the need for Horizon to carry out reconciliation both within and between business data streams returned to PO Ltd.

0.5.8.2 Chapter 4 - Overview

Updated to reflect the need for applications to carry out reconciliation.

Minor modifications to introduce flat panel displays in Outlets

There are minor modifications to bring the network description in line with [NWD]. There are major modifications to Figure 4.12 (the Big Picture).

0.5.8.3 Chapter 5 - Application Architecture

This Chapter is updated to indicate the need for, and types of, reconciliation. This covers data reconciliation both within Applications, and between Applications and TPS.

Figure 5.3, and the associated text, are amended to show the Riposte archive process running on the Correspondence Server.

The Chapter emphasises that Counter Applications must always check their Access Controls.

0.5.8.4 Chapter 7 – Information Management

Statement added to the effect that the Character Set to be used within Horizon is ISO 8859-1 (Latin Alphabet Number 1).

0.5.8.5 Chapter 8 – User Interface

Now includes a description of the Riposte *MemoView* facility.

0.5.8.6 Chapter 9 - Networking Services

This Chapter has been extensively rewritten to bring it in line with [NWD], which defines the network redesign for CSR. The principal purpose of this redesign is to set the stage for the introduction of VPN at CSR+.

0.5.8.7 Chapter 10 - Platforms

Additional Network Devices as defined in [NWD]. New Counter PC hardware as in CP 1265.

Introduction of flat panel displays in Outlets.

Indicates that the KMAS will use space on the EMC Disk Array, to ensure its data is replicated across both Campuses.

0.5.8.8 Chapter 12 - Systems Management

Amended to include a description of Tivoli Remote Console, as in CP 1379.

0.5.8.9 Chapter 13 - Availability

Amended to include revised Campus network availability details from [NWD].

0.5.8.10 Chapter 14 – Usability

Amended to include a description of the functions of the Riposte *MemoView* facility.

0.5.8.11 Chapter 15 - Performance

Amended to include revised Campus network capacity details from [NWD].

Data has been added relating to the size of the Data Warehouse database, and to the capacity of the inter-site links.

0.5.8.12 Chapter 16 - Security

Revision to the Counter PC authentication mechanisms to anticipate the introduction of VPN at CSR+.

0.6 CHANGES EXPECTED

0.6.1 General

This Document will be kept in line with major changes to the architecture of the Horizion system. These are likely to include a "downsizing" of the overall architecture, using a single Campus rather than the two Campuses described in this Document. In addition, a number of PO Ltd back end systems are expected to be incorporated into the systems run within the Pathway Campus.

0.6.2 Changes to Horizon Architecture

Chapter 17 "Potential for Change" examines in detail the likely changes beyond BI3, and the migration implications of these.

0.6.3 Changes to Document Structure

- The Architecture Team Web Site now contains a Hypertext version of this Document, with a comprehensive set of internal hyperlinks. Additional hyperlinks will be added as the Document is modified.

0.7 CONTENTS

0.7.1 Table of Contents

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

Chapter 1 - Introduction

1.1 PURPOSE

This document describes the technical infrastructure architecture for the Horizon system provided by Pathway to enable *Post Office Ltd* (PO Ltd) to meet its requirements for automation in Post Offices. It describes both the Logical and Physical architecture, and reviews it from a number of different perspectives including those of performance, availability and security.

It describes how this architecture is related to and influences the development of Applications that provide business functionality to PO Ltd and to its major Clients such as Girobank and the *Department of Work and Pensions (DWP).*

The document serves three purposes.

- It is *descriptive*, in the sense that it provides a full and high-level technical description of the infrastructure that supports and constrains the Horizon business Applications
- It is *prescriptive*, in the sense that it defines the architectural standards that apply to any new business Applications that may be defined in the future.
- It is *directive*, in that it leads the reader on to further, more detailed material, or to the actual standards that are only summarised here.

It has no contractual standing and has no formal relationship to the *Service Architecture Design Document* ([SADD]), which defines the services provided to PO Ltd. It does describe the ways in which these services are implemented, as they impose capacity and other constraints that can materially affect the ability to absorb new Applications.

Its primary audience is the designers and developers of these Applications and of the underlying infrastructure.

It is generally available to all members of Pathway and its suppliers within Fujitsu Services, but should be treated as COMPANY CONFIDENTIAL. It may, in the future, be disclosed to PO Ltd under the terms of a new Horizon Contract.

Any changes to the infrastructure or generic application architecture are introduced by Change Proposals. At intervals, Approved Change Proposals are incorporated into this document.

1.2 SCOPE

This document constitutes the top level of the Horizon technical description, and identifies all the Platforms and infrastructure products used, their interconnections, major attributes and business objectives. Two lower layers of documents are defined. They elaborate on the following areas.

- The architecture of the major business Applications
- The detailed architectural standards in major *layers* of the system. These layers are described in Chapter 4 "Overview", and their use elaborated on in Chapter 5 "Application Architectures".

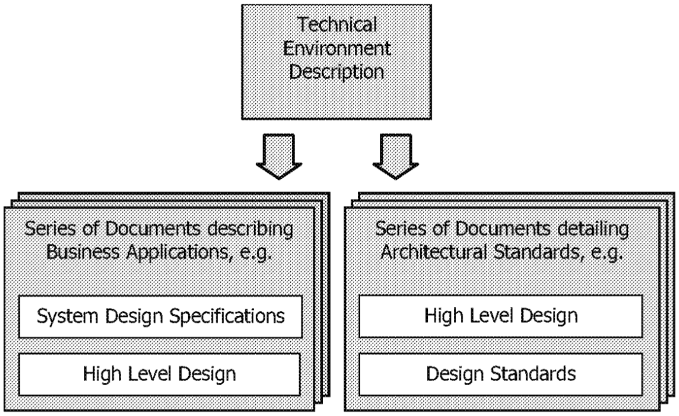
Technical Environment Description
Series of Documents describing Business Applications, e.g.
System Design Specifications
High Level Design
Series of Documents detailing Architectural Standards, e.g.
High Level Design
Design Standards

Figure 1.1 - Architectural Document Structure

The document defines the steady state solution once the System Release known as S30 is introduced into general use. It thus includes a description of the *Network Banking Service* (NBS) and *Debit Card System* (DCS), which are added in BI3 and S30 respectively.

> *Speculative material, author's comments, or features that may or may not be introduced, are indicated like this.*

This document does not include detailed information about specific application functionality, only the general architecture within which those Applications are developed and run.

1.3 STRUCTURE

Horizon is a large and complex system, and this document reflects that. Most readers will be interested in particular aspects of it, and will not wish to read the entire document. It has thus been sub-divided into a number of Chapters, in such as way as to simplify the reader's task.

As an additional help to the Pathway reader, the text of this Document is also held on the ASD Website. It is split into a number of "web pages", each corresponding to one of these Chapters.

- Chapter 2 describes the *Business Context* within which Horizon is developed and implemented.
- Chapter 3 describes the different IT *perspectives* from which it is necessary to view Horizon.
- Chapter 4 provides an *Overview* of the purpose and major components of Horizon, and its logical and physical architecture. It describes the structure of the principal Applications used to deliver the business services, and the *Logical Architecture* that includes the ancillary services such as the *Management Information System* (MIS)

and the Security facilities. It maps this on to a *Physical Architecture* that defines all the Platforms used to support the business and ancillary services.

Chapters 5 to 12 then describe individual aspects of the solution. These reflect eight Technical Elements as previously defined in Fujitsu Services' OPEN*framework* reference model.

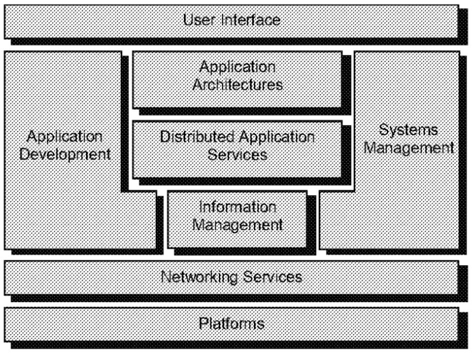

Figure 1.2 - *OPENframework* Information System Elements

- Chapter 5 describes *the Application Architecture.* It is aimed at designers and developers of new business Applications. It discusses the structure and components of the Applications that implement the Horizon business requirements. It describes how they fit into the overall infrastructure and interact with existing Applications. It also discusses the structure of the internal applications used to support the Pathway business requirements. It should be the starting point for any new Application designer, though because the application architecture is heavily influenced by the infrastructure that supports it, there are copious references to other Chapters in the document.
- Chapter 6 describes the *Distributed Application Services* that enable the solution to be spread across a number of hardware platforms. In particular, it covers the facilities of the *Riposte message distribution system*. It also discusses the use of *Remote Procedure Call* facilities, the ways in which distributed database products such as Oracle are structured, and other distributed mechanisms such as shared file stores.
- Chapter 7 discusses the *Information Management* services used. Again, Riposte features prominently in this description, though from the point of view of the way in which it stores data, the uses of this data, and the interfaces presented by Riposte to the application developer. Chapter 7 also discusses the features of the database products used: Oracle, which is used to support the main Host applications and the Management Information System, and Microsoft SQL Server, which is used by internal applications. Chapter 7 concludes with a discussion of the other information management techniques used, in particular the widespread use of Flat Files for passing data to and from PO Ltd and its Clients.
- Chapter 8 describes the *User Interface* that is presented to the users of the system. This focuses on the ways in which Riposte Desktop applications are implemented at the Counter.
- Chapter 9 describes the N*etworking infrastructure and Services* that link all the components of the solution together. It discusses the cabling methods and link level protocols used, and the interconnection services between the Outlets, Campuses, PO Ltd and its Clients, and Pathway's suppliers. It goes on to discuss the interworking

services that are implemented on top of this network, the different types of network connections between the Campus and the Outlets (fixed connection or dial-up connections) and the ways in which fixed connections are maintained and network status information gathered and presented

- Chapter 10 describes the hardware and software *Platforms* used. It groups these together into classes that share a common hardware type or operating system or purpose. Each Platform is described from the point of view of its broad hardware requirements, the operating system that it supports, and the principal Applications or Application components (*Capsules*) that run on it. The need for each of these Capsules is derived elsewhere in the Document.

- Chapter 11 discusses the ways in which *Applications are developed* within the various system layers. It describes the tools and processes used in this, and the ways in which new or changed Applications and infrastructure developments are gathered together and released into the live environment.

- Chapter 12 discusses the *Systems Management* facilities used. It describes how these are implemented, and the services they provide. The major emphasis is on the Tivoli systems management applications. However, Chapter 12 also covers topics such as the organisation of the Horizon Systems Help Desk and the Service Level monitoring.

Finally, Chapters 13 to 17 discuss the solution from the perspective of the five OPEN*framework* "Qualities that any IT system must address.

- Chapter 13 discusses the methods used to ensure the *Availability* of services in the context of the *Service Level Agreements* (SLAs) contained in the Contract. It examines the resilience needed and provided within each Platform or network component, and summarises the failover processes used to provide for resilience in case of failure.

- Chapter 14 discusses *Usability*, and in particular how emphasis on this quality can reduce the training needs for end users and reduce the number and cost of calls to the Help Desks.

- Chapter 15 discusses *Performance,* its impact on the size and capacity of the Platforms and applications that support the system architecture, and the significance of the SLAs in the Pathway Contract. It emphasises the ways in which the agreed business volumes feed through to the size of and number of instances of each Platform type, the ways in which the capacity of the system is monitored and predicted, and the scope for extensions to the solution as more business applications are added to it.

- Chapter 16 summarises the methods used to enforce the *Security* of the system, and looks at the various methods used to support *Authentication*, *Access Control* and *Audit* within the solution. It also examines the use of *Cryptography* to protect the integrity and (where needed) the confidentiality of the data held in the system.

- Chapter 17 discusses the *Potential for Change* to the system in response to revised business or other needs. It looks at the ease with which new Applications can be added to the solution, bearing in mind the architecture discussed in Chapter 5 "Application Architectures". It also examines likely changes to the infrastructure itself, and the impact of these on future Releases.

1.4 DOCUMENT CONVENTIONS

A number of conventions are used in the diagrams contained in this Document. They are illustrated in the following diagram. The colour names given are those in the Microsoft Office 2000 colour palatte.

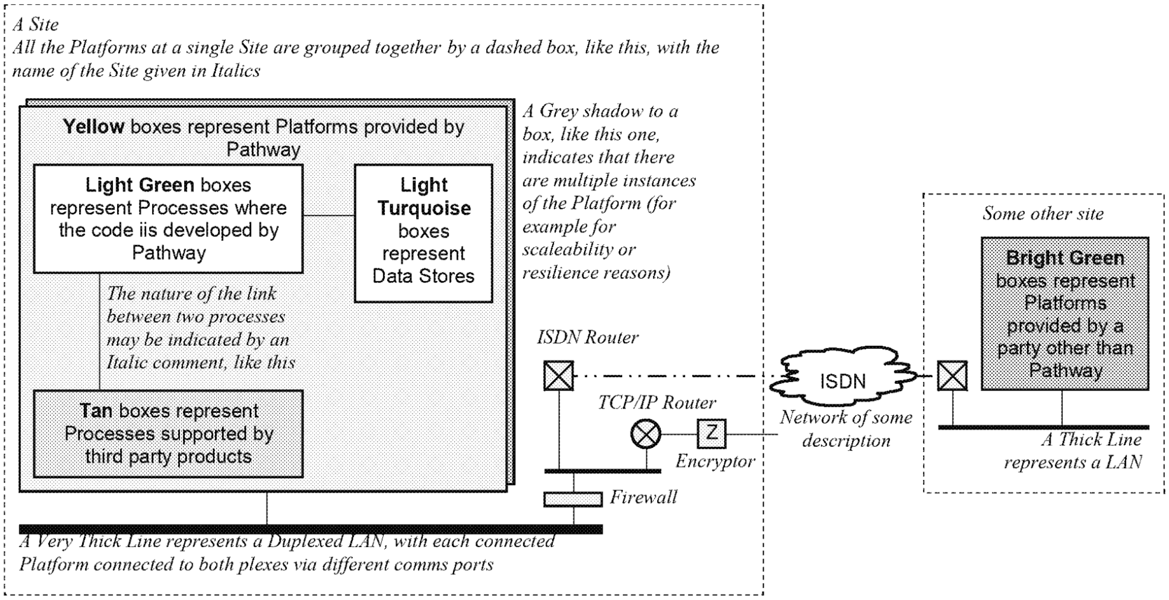
A Site
All the Platforms at a single Site are grouped together by a dashed box, like this, with the name of the Site given in Italics
Yellow boxes represent Platforms provided by Pathway
Light Green boxes represent Processes where the code iis developed by Pathway
Light Turquoise boxes represent Data Stores
The nature of the link between two processes may be indicated by an Italic comment, like this
Tan boxes represent Processes supported by third party products
A Grey shadow to a box, like this one, indicates that there are multiple instances of the Platform (for example for scaleability or resilience reasons)
ISDN Router
TCP/IP Router
Z
Encryptor
Firewall
ISDN
Network of some description
Some other site
Bright Green boxes represent Platforms provided by a party other than Pathway
A Thick Line represents a LAN
A Very Thick Line represents a Duplexed LAN, with each connected Platform connected to both plexes via different comms ports

Figure 1.3 – Diagram Conventions

1.5 FURTHER READING

Ref	Document	Title	Comments
Next	Chapter 2	The Horizon Business Context	Specifies the business context into which the Horizon services are provided by Pathway

Chapter 2 - The Business Context

2.1 SCOPE

This Chapter discusses the business context in which the Pathway provides services to PO Ltd.

2.2 GENERAL

Pathway provides systems that meet PO Ltd's requirements for the automated provision of Counter services in Post Offices. These include the *Electronic Point of Sale Service* (EPOSS) that supports the sale of goods and services at Post Office Counters. It also includes services provided to the DWP Benefits Agency to control the issue and use of benefit Order Books, and the *Network Banking Service* (NBS) that enables Customers to withdraw money from their bank accounts. This application will become more significant as the DWP phases out the provision of Order Books in favour of direct payment of benefits into claimant's bank accounts.

Pathway provides the technical infrastructure and supporting services, as well as the business applications that deliver the contracted services.

The technical architecture defines the ways in which various components are chosen, developed, combined and integrated to deliver the solution required by PO Ltd. These are dictated by technical completeness and the ability to meet these requirements.

2.3 POST OFFICE COUNTERS LTD (PO LTD)

2.3.1 PO Ltd's Business Position

PO Ltd acts as an agent to a number of *Clients* for which it provides counter services in its Post Offices.

The following capitalisation conventions are used throughout this document.

- POCL's Clients are always referred to with a Capitol "C".
- When referring to a client in a client-server sense, we use a small "c".
- The people who use Post Office Outlets are known as C*ustomers*

PO Ltd has a unique position in British life. It is expected to provide a wide range of often low-value services. As PO Ltd gains greater commercial freedom, it needs to bid for, gain and retain a greater degree of high value business. It lives in a business environment where it competes with cherry-picking organisations such as the banks and supermarkets, which covet some of PO Ltd's market share but do not have its special social responsibilities.

Pathway's contribution is twofold. Firstly, it is to provide a system to PO Ltd that makes it cost-effective to support their low-value operations. Secondly, it is to make it relatively simple and inexpensive to add new high-value business. The system needs to ensure an appropriate separation is maintained between PO Ltd and any other Clients for which it carries out business.

The system supports a range of generic functions that can be used to extend the range of business activities supported by PO Ltd. These centre on the following types of business areas.

- *Conveying items* e.g. parcels and letters
- *Paying bills* to BT, utilities, local Government
- *Buying consumer goods and services* - general retail products, registered letter labels, lottery scratch cards
- *Prepayment services* - DVLA savings stamps, gift vouchers and entertainment tickets
- *Acquiring licences* - local Government permits, television, motor vehicle
- *Money management* - banking deposits and cash withdrawals, savings and investments
- *Insurance services* - general, travel
- *Pensions payments* - e.g. for MoD

PO Ltd are looking for a system that displays a number of qualities, including the following.

- High availability
- Style and simplicity of the user interface
- Speedy Counter response times
- Achievement of batch SLAs
- Support which exceeds agreed SLAs
- Low running and development costs
- The capability to move forward as PO Ltd's business needs change

2.3.2 PO Ltd's Requirements

The contractual requirement is for the provision on each Post Office Counter across the UK of a facility to transact most Post Office business, including point of sale services and the payment of Benefits. These transactions are grouped together into *Services*. Each service is treated as separate, except that all transactions from all of these services are also transmitted to PO Ltd for their own subsequent processing. The services provided include the following.

2.3.2.1 Electronic Point of Sale Service (EPOSS)

This provides support for customers purchasing goods or services. It also provides a generic point of sale facility including cash reconciliation and end of day accounting.

2.3.2.2 Automated Payment Service (APS)

This provides support for AP Clients such as the utility companies and others who provide the means for their customers to make incremental payments based on cards and other devices

2.3.2.3 Order Book Control Service (OBCS)

This supports the issue and encashment of Order Books. It takes a data feed from the DSS $OBCS_D$ system. OBCS will continue to be supported until benefit books are completely replaced by automated cash transfers (ACTs).

Note that there are two systems called "OBCS": the Counter application that is part of Horizon, and the DSS feeder system. To avoid confusion, the suffix "D" is used to identify the DSS system.

2.3.2.4 Network Banking Service (NBS)

Starting in April 2003, it is expected that the DWP will begin to phase out payment by Order Book in favour of direct transfer of funds to claimant's bank accounts (*Automated Credit Transfers*, or ACTs).

The NBS service, which is introduced at BI3, enables members of the public to use their bank cards to withdraw funds from their bank account at any Outlet. They can also deposit funds, or carry out a balance enquiry. All NBS transactions are automatically passed to the customer's FI for authorisation.

NBS is supported by the development of a *CardAccount at Post Offices* (CAPO) specifically targeted at those members of the public who are unable to obtain a conventional bank account. Some facilities are provided at Outlets to handle aspects of CAPO accounts, but these are not relevant to Horizon.

2.3.2.5 Debit Card System (DCS)

DCS enables customers to pay for goods and services using *Debit Cards*. A card may be used for some or all of the value of a customer session. The transaction is verified by on-line reference to a *Merchant Acquirer* who either Approves or Declines it.

2.3.2.6 Logistics Feeder Service (LFS)

This is used to ensure that Outlets have up-to-date supplies of stock including cash. It interfaces to PO Ltd's SAPADS stock control system.

2.3.3 Horizon Context Diagram

This shows how the system provides services to PO Ltd and its Clients.

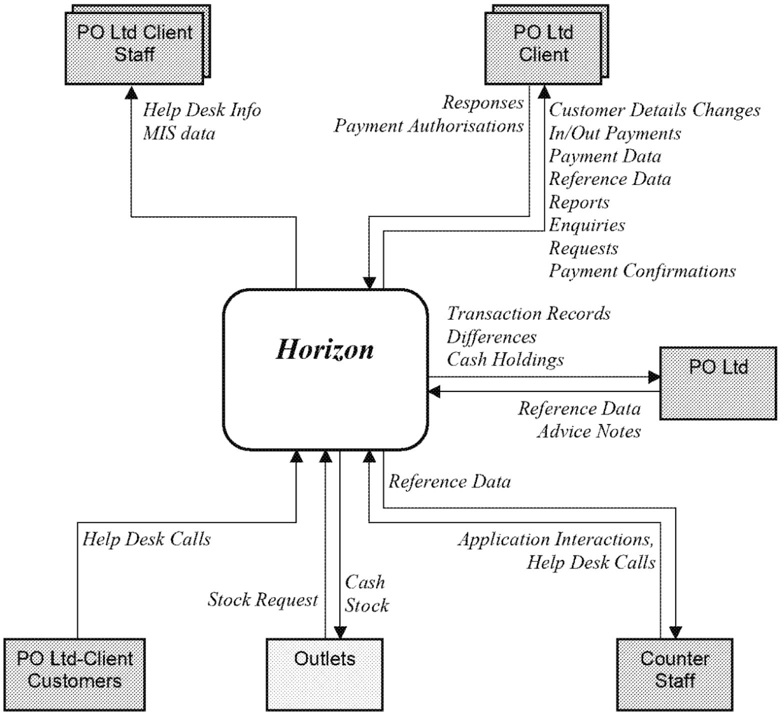

Figure 2.1 - Horizon Context

The round cornered box represents the whole of the Horizon system. The square boxes surrounding it represent external Entities. The lines represent data flows between Pathway and these External Entities. The annotations next to the lines identify the generalised types of data.

2.3.4 PO Ltd's Clients

2.3.4.1 DWP Benefit Agency (BA)

A major Client is the *DWP Benefit Agency* (BA), for which PO Ltd acts as the primary Payment Agent. Payments are made via *Order Books*, each containing a number of Coupons. Each Coupon can be exchanged for cash when it becomes due.

2.3.4.2 Financial Institutions

NBS provides facilities for Customers of selected banks and building societies (those with which PO Ltd has reached an Agency agreement) to withdraw money from and deposit funds into their bank accounts.

2.3.4.3 Merchant Acquirer

DCS provides facilities for Post Office customers to pay for goods or services by means of a *Debit Card*. Any such transaction is authorised, according to standard EFTPoS industry standards, by a *Merchant Acquirer*. PO Ltd have chosen Streamline Merchant Services (SMS) as their MA.

2.3.4.4 Other PO Ltd Clients

There is a range of other Clients such as the utilities and local Councils for which PO Ltd collects payments. Many of these provide *Automated Payment* systems, such as swipe or Smart Cards, with the details of the payments being forwarded to the *AP Client* by Horizon.

2.3.5 Interfaces to Horizon

2.3.5.1 Transaction Information Processing (TIP)

Transaction Information Processing (TIP) is a system used by PO Ltd to collect *transaction records* about all transactions that occur at all Outlets that need to be reconciled with its Clients. Pathway acts as an honest broker for both PO Ltd and its Clients. While Horizon is not an accounting system, the data it passes to PO Ltd and its Clients must be sufficient to enable them to balance their own books and settle accounts between them. The data transmitted to all Authorities must be complete, accurate and timely. Its integrity must be assured throughout the system.

2.3.5.2 Reference Data

Reference Data is a mechanism used by PO Ltd to provide Pathway with data about the services provided, the products available for sale, and the ways in which these are to be offered. It enables much of the operation of the business applications to be "soft centred". It is distributed to the *Counters* and is used by the desktop applications that provide the contracted services.

2.4 PATHWAY

Pathway develops and owns the facilities used to provide the Horizon service to PO Ltd. PO Ltd pays for these services via staged payments, by funding specific developments, and by reimbursing running costs subject to achievement of SLAs. PO Ltd has an option to purchase all the Horizon assets for a nominal sum at the end of the Contract.

2.4.1 Trading Partners

Pathway uses goods and services provided by a number of Trading Partners.

2.4.1.1 Principal Trading Partners

2.4.1.1.1 Escher Group Ltd

Escher are responsible for the Riposte messaging and retail software which forms the core infrastructure of Horizon

2.4.1.1.2 Fujitsu Services Core Services (FSCS)

FSCS (formerly ISD) provide day-to-day operational management of the systems in the Campuses, and of the network that links them. They also provide application support for some of the applications on Host Servers and on the DWP VME mainframe.

FSCS's *Systems Management Group* (SMG) is responsible for the systems management of the platforms in the Campuses and elsewhere, including Software Distribution and event and resource management. FSCS also runs the Horizon Systems Help Desk that manages support calls from Outlet staff

2.4.1.1.3 Celestica

Celestica are responsible for building the Counter PCs that go into Post Office Outlets. They use standard Fujitsu Siemens PCs and a build tape supplied by Pathway.

2.4.1.1.4 IBM

IBM provide the *Network Banking Engine* (NBE) that supports Network Banking applications and hides from Pathway the complexity of the interfaces to the indivual banks. IBM develops the interfaces to the NBE in co-ordination with PO Ltd and Pathway.

2.4.1.1.5 Retail Logic

Retail Logic supply software to the EFTPoS market. Pathway's implementation of EFTPoS (DCS) will use components of Retail Logic's Solve/SE and Solve/PFG software suites.

2.4.1.1.6 NatWest Streamline

Streamline is a *Merchant Acquirer*, chosen by PO Ltd to support DCS transactions in Outlets.

2.4.1.1.7 Energis

Energis provide network facilities, other than that between the Outlet and the local BT *Digital Local Exchange* (DLE).

2.4.1.2 Other Trading Partners

There are many other suppliers of components of the solution or services to it. These include:

Company	Product or Service
British Telecom	ISDN Services
Cherry	Keyboards
Cisco	Routers
Compaq	Windows NT servers and disk arrays
Celestica	Preparation of pre-configured Counter PCs
Delphic	Smart Cards used for Post Master's Memory Cards
Devlin	LIFT Keyboard
Eicon	ISDN cards and driver software
EMC	Disk Arrays
Epson	Printers
Fujitsu Siemens Computers	NT Servers andWorkstations, including Counter PCs
Hewlett Packard	HP OpenView
Hytec	Communications software
Ithaca	Printers used in Outlets
Landys & Gyr	Smart Cards used as Utility Payment Cards
McPerson	Flat screen displays
Microtouch	Touch-sensitive screens
Novacom Microwave Ltd	Time Server
OKI	Printers used in Outlets
Panasonic	Printers used in Outlets
PPC	Printer cables and power supplies
Security Dynamics	SecurID tokens and associated software
Specialix	8-port I/O boards
SUN	UNIX Workstations

Tivoli (now part of IBM)	Systems Management software
Unison (now part of IBM)	Maestro scheduling software
Welch Allen	Bar Code Readers

Table 2.1 - Pathway's Component Suppliers

2.5 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 1	Introduction	Introduction to the Horizon architecture
Next	Chapter 3	IT Perspectives on the Horizon System	Describes the main classes of people concerned with the systems developed by Pathway
SADD	CR/FS/006	Service Architecture Design Document	This specifies the services that are to be provided to PO Ltd and DSS

Chapter 3 - IT Perspectives on the Horizon System

3.1 SCOPE

This Chapter describes the main classes of people, within Pathway and elsewhere, concerned with the development and exploitation of the systems that provide the Horizon solution. This classification is intended to enable Pathway to assess the effectiveness and completeness of these systems.

3.2 THE USERS' PERSPECTIVE

3.2.1 Responsibilities

3.2.1.1 Pathway's Customer's Users

3.2.1.1.1 Post Office Counter Clerks

The Outlet *Counter Clerks* are the main users of Horizon. They have access to a range of desktop applications that include those listed in Chapter 2 "Business Context".

In addition to these desktop applications, Counter staff can also make telephone calls to the *Horizon Systems Help Desk*, which answers technical queries about the operation of the service and the systems installed in Outlets and the Campuses.

Their interest is in ease of use of the delivered systems, an intuitive interface, and speed in carrying out transactions to avoid queues building up in Outlets.

3.2.1.1.2 Post Office Managers

Post Office Managers are responsible for their Outlets. As well as acting as Counter Clerks, they are responsible for the End of Day balance activities. They look for mechanisms that automate these (previously highly labour-intensive) activities and enable them to be completed as speedily as possible.

Post Office Managers are also responsible for booting up the Counter PCs when they are first installed or whenever they have been powered off. They are thus involved in the *Post Office Log On* process that is a means of ensuring the security of the data held in the Counter terminals. They want the process to be simple to use, and simple to restore if something goes wrong (such as they lose their identifying token or *Personal Identification* (PIN) number).

3.2.1.1.3 Post Office Customers

The Customer (the man or woman in the street) makes use of the services provided by PO Ltd's Outlets, and demands that these be provided efficiently, speedily and reliably. They have no direct access to the Counter systems, other than use of a PIN Pad to verify an NBS transaction, and rely upon the skill of the counter staff to carry out transactions on their behalf.

3.2.1.1.4 Horizon Help Desk Staff

Help Desk users respond to telephone calls from Counter Clerks and must provide a speedy and accurate response to their concerns. This is aided by the provision of facilities within the Counters to provide monitoring and support information that may be required by Help Desk staff.

3.2.1.1.5 Financial Institutions

A number of Banks and Building Societies will reach agreement with PO Ltd to enable their Customers to use banking facilities in Outlets. They expect these facilities to be provided in a secure way, in line with normal banking practices and with the provision of significant legislation such as the *Data Protection Act* (DPA).

3.2.1.1.6 Other PO Ltd Clients

Other POCL Clients use the Post Office mainly as a means of collecting payments from their own customers. Horizon notifies these Clients of the payments collected.

3.2.1.1.7 PO Ltd Auditors

PO Ltd auditors examine the accounts kept within the Outlet and ensure that no fraud is being perpetrated there. They need access to a complete and coherent set of records of the transactions carried out at each Counter, as well as the knowledge that these records cannot have been tampered with. Speed is of less concern than completeness of audit information. However, if an Auditor is using a Counter PC, it should be returned to its primary use as soon as possible.

PO Ltd Emergency Managers provide additional powers to the PO Ltd auditors when they are prevented, by the absence of or lack of co-operation from the Post Office Manager, from carrying out their usual functions.

3.2.1.1.8 Client Auditors

Client auditors are concerned with the administration of the services provided to them by the system. They need to verify that these services are carried out in accordance with the Contract or their own agreements with PO Ltd, and with normal fiscal safeguards. Pathway's role is to ensure that they have access to all relevant data. Much of this data is defined in [ATFS].

3.2.1.2 Pathway Users

3.2.1.2.1 Management

Pathway management needs access to a range of applications that enable them to monitor the performance of the business and ensure that SLAs are met.

3.2.1.2.2 Pathway Auditors

These are of two types.

- Internal Auditors who monitor the handling of data belonging to POCL and its Clients, and ensure that Pathway is in a position to invoice accurately for the services it provides

- Security Auditors who are concerned to ensure that the Pathway security policies are adhered to and that all accesses to the system, for whatever reason, are monitored and recorded

3.2.1.3 Support Users

Support of the Pathway systems is provided by the following organisations.

- The *Horizon Systems Helpdesk* (HSHD) provides first-line support to Counter Clerks. It handles application-related incidents (for example OBCS stop list enquiries). It forwards hardware related queries to Sorbus. It forwards system or software incidents to the SMC.
- The *Systems Maintenance Centre* (SMC) provides second level support to incidents reported to it form the HSH.
- The *Systems Support Centre* (SSC) handles third level support to incidents passed to it from the SMC.
- Fourth line support is provided by Pathway's suppliers such as Sequent and Oracle, and the Pathway development units.
- *Support Engineers*, who visit Outlets to replace faulty equipment. Their needs reflect that of the Post Office Manager: to replace failed equipment speedily, and to minimise the time spent in any one Outlet. They have an additional need: there is limited space in their vans, and hence they cannot be expected to carry a large number of different types of spare Counters or other equipment

The need of all support organisations is to identify and fix problems as soon as is reasonably possible. They need speedy access to a wide range of potentially diagnostic information, and this should not be unreasonably withheld from them on, for example, security grounds.

They also need the ability to fix problems when their cause is found, but here there is a need for more care and less speed to ensure that the cure is not worse than the problem.

Support users often have open access to the heart of the organisation's computer systems, so it is important that their actions are fully audited and that the users themselves are not able to delete or modify the audit information.

3.2.1.4 Operational Users

These users provide day-to-day operational management of the systems at the Campuses. Their activities are necessarily routine, and often carried out for a variety of different types of system. Thus information flowing from the system to these users should be:

- *relevant* - don't display it unless the operator should take some action as a result of it or needs it to be on display for information purposes
- *timely* - display it as soon as it becomes relevant
- *identifiable* - the operator must be able to identify easily which system or system component it relates to

3.2.2 Processes

Operational processes are necessary to ensure the smooth running of the operational services. These include predetermined operational schedules, as well as processes which automate the many and varied contingencies which need to be anticipated and planned for.

In addition, well-defined support processes are necessary to handle calls from Outlets and others who are affected by problems with the delivery of the contracted services.

Lastly, where there is a need to call in outside support, careful authentication and monitoring processes are necessary to ensure that the support staff can do their jobs effectively and speedily but without affecting the integrity of the systems or the data for which Pathway has accepted responsibility.

3.3 THE APPLICATION DEVELOPERS' PERSPECTIVE

3.3.1 Responsibilities

The role of the Application Developer is to provide the applications (and, in this context, infrastructure) needed to support the Horizon system's requirements.

They are responsible for identifying and meeting the requirements of the users of these systems, in the most cost effective way. They must provide a system that can be effectively delivered and operated by the service provider and that can respond to changes in the business requirements.

There is a spectrum of application development roles, as shown here.

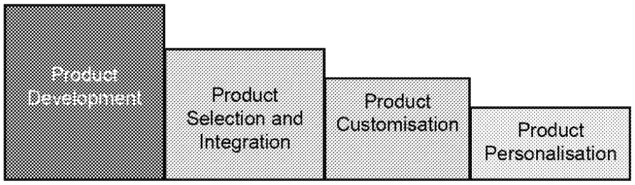

Figure 3.1 - Application Development Roles

- *Product Development* is carried out by skilled application developers who design, code and test the products of an application. Many of the business applications fall into this category.
- *Product Selection and Integration* is also carried out by skilled application developers, who select ready-made products and integrate them so that they conform to the system requirements. Most of the infrastructure has been developed in this way.
- *Product Customisation* involves adapting or configuring products to meet the needs of specific users or Workgroups. Its principal need is in configuring the ready made products to meet the needs of Horizon as a whole. A principal business objective is to provide as much commonality as possible across the systems made available to the end users, and thus there is, for instance, little or none customisation for the needs of individual Post Offices.
- *Product Personalisation* is involved in ensuring that the user interface of the application meets the need of a specific user. There is no requirement for this task within Horizon

3.3.2 Processes

This shows the stages that are involved in any product development.

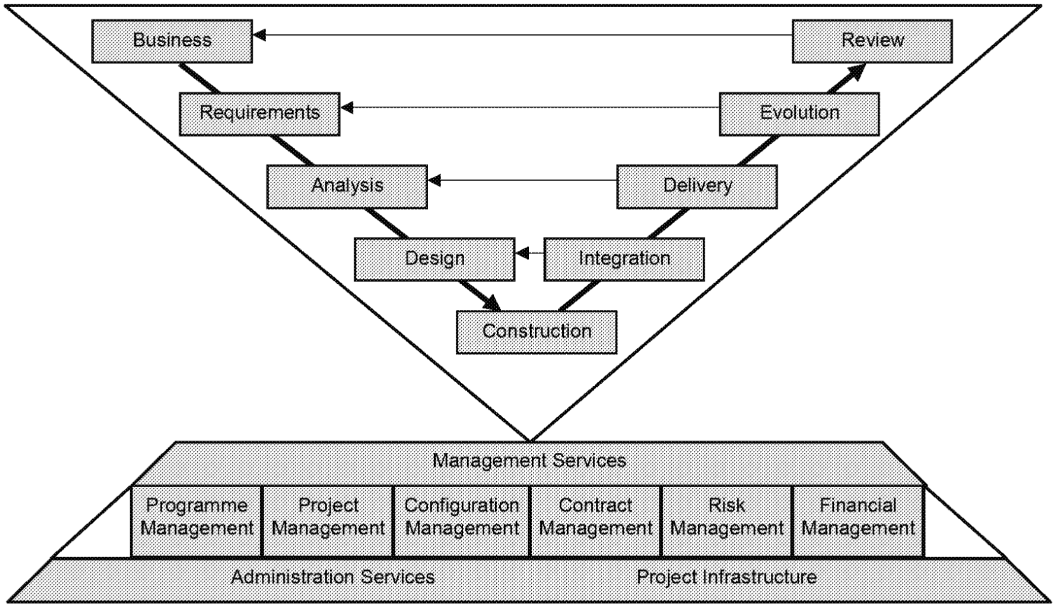

Figure 3.2 - Application Development Processes

There are two classes of process: those involved with the development itself, and those surrounding and supporting it. Both are equally important.

3.3.2.1 Development Processes

A number of processes are defined, and assigned to particular Teams within the Pathway management structure.

3.3.2.1.1 Requirements Team

Most existing *Requirements* are expressed in the Codified Agreement, though many of these originated as "agreements to agree" that needed to be refined and elaborated before application development could begin.

Further requirements are derived from business opportunities identified in discussions with PO Ltd. They are captured in a Pathway-produced *System Requirements Specification* (SRS), which is an agreed statement of what is to be delivered. In the future, it is likely that the SRS will be replaced by a *Business Requirement Specification,* owned by PO Ltd and produced jointly with Pathway.

3.3.2.1.2 Architecture and System Design

New business developments need to be justified against their ability to fit into the existing system structure. This structure is described in the current Document, which is owned by ASD. Any potential change to the system, or any requirement for a new application, will be measured against the existing architecture. This is the responsibility of ASD. Where the business case analysis indicates that the architecture is inadequate to support the new business requirement, then ASD must assess the impact on the current architecture, and make the necessary chages to it. These are documented (usually in retrospect) in the [TED].

ASD's analysis of the requirement leads to the production of *a System Design Specification* (SDS) for the development. This is either developed by, or approved by, ASD. The SDS enables Pathway management to produce a rough outline of its costs and likely timescale. It identifies how the development will be undertaken, and how it fits within the existing architecture (i.e. how it relates to this Document).

3.3.2.1.3 Delivery Unit

This SDS defines the overall structure within which developments take place. The Delivery Unit takes the SDS and produces the high- and low-level designs needed to enable the application and underlying infrastructure to be built.

The Delivery Unit is then responsible for constructing the product and its associated test plans from the design. *Unit Testing* takes place once the product is developed or procured, and ensures that the product conforms to the test plan.

3.3.2.1.4 Pathway Technical Integration

Technical Integration involves testing the product with other products with which it needs to interwork, and (most importantly) verifying that it can be built from information stored within Pathway's Configuration Management database PVCS.

3.3.2.1.5 Pathway Testing Unit (PTU)

The *Pathway Testing Unit* proves that a new Release or Increment, and its components, operates within the system infrastructure. *Acceptance Testing* takes place at the end of the Integration process. It proves to the sponsoring Client that the development meets his functional requirements, and to PO Ltd that it may be brought into use without impacting on the existing solution or other applications.

3.3.2.1.6 Implementation

Delivery of the product involves putting it into use, for example by rolling it out to every Outlet. The time that this takes depends on the type of product. If it can be distributed via the Systems Management Software Distribution facilities, then it can be brought into use very quickly indeed. If it requires a manual visit to every existing Outlet (for example to install a hardware upgrade), then rollout will be extremely slow (not to mention expensive) and may be error-prone to boot.

3.3.2.1.7 Evolution

Evolution of the system means keeping it up to date so that it continues to meet the business needs of both PO Ltd and Pathway. It involves including new functionality and exploiting new technology where it is cost effective to do so.

3.3.2.1.8 Review

Review is a process that is carried out periodically to ensure that the information system continues to meet its business needs. It may lead to changes in the business requirements and to the architecture within which these are developed.

3.3.2.2 Supporting Processes

A number of ancillary functions are involved in the application development process.

3.3.2.2.1 Programme Management

This is necessary because of the wide range of projects involved in Pathway. It involves co-ordinating these programmes and managing the need of each for scarce and competing resources. Programme Management is also involved in the selection of suppliers to carry out these projects.

3.3.2.2.2 Project Management

This is necessary within each development or for each supplier's development to ensure that it is developed to the requirements in the SRS and delivered to agreed timescales and quality criteria.

3.3.2.2.3 Configuration Management

This involves keeping control over the developing components, ensuring that they are brought together at the right time in the right order and comprise the correct parts. It requires extensive use of the Pathway PVCS system from the earliest stage of any development activity.

It is closely involved in the specification of the *Horizon Release Strategy*. It must be closely integrated with supplier's Configuration Management systems.

3.3.2.2.4 Contract Management

This is necessary where some components come from outside Pathway. It involves negotiating an appropriate contract for the supply of the product or development, and ensuring that the terms of the contract are carried out.

3.4 THE SERVICE PROVIDERS' PERSPECTIVE

3.4.1 Responsibilities

Service provision covers the day to day management of the information system. It ensures that the required services are delivered to users in accordance with SLAs.

Pathway's *Customer Services* Directorate is responsible for the management of the services provided to PO Ltd. They sub-contract parts of this responsibility to other organisations such as FSCS.

3.4.2 Processes

This shows the fundamental classes of tasks used by service providers, and the flow of activities between these tasks. The ten parts of the model contribute as follows.

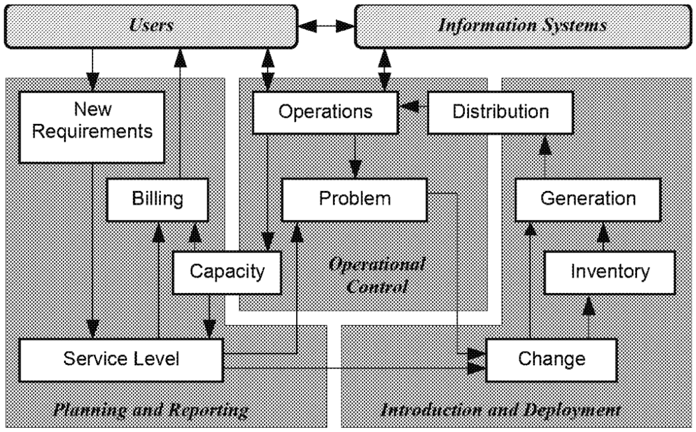

Figure 3.3 - Service Management Services

3.4.3 Operational Control Processes

3.4.3.1 Operations Management

This involves controlling and monitoring the managed resources in the network. They include monitoring the status of managed systems, responding to alerts that they generate, controlling services, and keeping users informed when changes are going to affect them.

This is needed to automate the management of the systems that comprise the Horizon estate, and ensure that they operate in an efficient way with the minimum of unplanned downtime.

3.4.3.2 Problem Management

This involves providing a service to Operations and to other parts of the Systems management process for diagnosing, fixing and preventing the occurrence of problems.

When a problem cannot be handled by automated systems, it should be brought promptly to the attention of a human. This person can manage the impact of the problem, assign it to an appropriate support resource, and track the subsequent processing of the problem. Automated Help Desk facilities are essential to optimise the handling of problems in this way.

Help Desk facilities are needed both for specific applications and for overall system problems.

Infrastructure support is carried out by FSCS using a Help Desk installed in their premises in Stevenage and Manchester. Second line support is handled by the SSC in Bracknell. Third line Support is provided by suppliers including Sequent and Oracle. Where these suppliers need on-line access to the system to enable them to provide speedy support, or carry out detailed investigations of operational systems, this is provided at Pathway premises.

3.4.3.3 Capacity Management

This involves reviewing operational data to assess the availability and performance of the system, and indicating when the service provided is liable to be affected by the capacity of the system components.

Key to this is the ability to detect when particular resources are overloaded or are likely to overload in the near future.

It is carried out by Pathway Management using information gathered by FSCS.

3.4.4 Introduction and Deployment Processes

3.4.4.1 Change Management

This involves providing a mechanism for handling changes to the system, including defining the specification, validation, impact of and authorisation for the change, and the subsequent scheduling and implementation of it.

3.4.4.2 Distribution Management

This provides mechanisms to deliver, install and activate components of the system.

Automated Software Distribution, especially to Counter PCs, can remove the need for human intervention, and enable a greater degree of commonality in the software used than would be possible if users or local administration staff had responsibility for this activity.

Managing Software Distribution is a complex process. It can be simple in operation, but only if every distribution is designed extremely carefully, with an understanding of everything that could go wrong. Distributions need to include a regression process which can “undo” the entire distribution should the software prove flawed in operation.

Software Distribution is carried out jointly by Pathway management and SMG. Software is developed by Pathway, as described above. It is passed to SMG through a process that “seals” the product, to protect its integrity, and is distributed using automated mechanisms.

3.4.4.3 Inventory Management

This involves maintaining up to date records of the total set of applications, hardware and software components and infrastructure that comprise the system.

Pathway maintain an asset register of all systems installed in Post Office premises, and a *Software Inventory* of the software state of all platforms including Counter PCs.

3.4.4.4 Generation Management

This involves ensuring that new or replaced Counter PCs are delivered and installed on time and accurately and configured as members of the Horizon network in an efficient and secure manner.

This is the responsibility of Pathway management using information provided by PO Ltd and Pathway’s. Configuration changes are distributed by FSCS where feasible.

3.4.5 Planning and Reporting Processes

3.4.5.1 Billing Management

In general, PO Ltd pay Pathway at various stages on the achievement of Acceptance of the delivered system.

These payments may be modified should Pathway fail to meet SLAs, most of which relate to response times to various criteria. Pathway needs to gather and store the data necessary to carry out these calculations.

3.4.5.2 Service Level Management

This involves giving a clear statement of what the system has to provide, and reporting on the service levels achieved. It feeds into the Billing process described above. There is a contractual requirement to provide this information as part of its billing process.

3.4.5.3 New Requirements Management

This involves responding to requests for modification to the infrastructure and for the implementation of new applications. It is described further above.

3.5 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 2	The Horizon Business Context	Discusses the business context into which the Horizon services are provided by Pathway
Next	Chapter 4	Overview of the Horizon Architecture	An overview of the technical infrastructure which supports and constrains the applications that provide services to Pathway's customers

Chapter 4 - Overview of the Horizon Architecture

4.1 GENERAL

This Chapter provides an overview of the technical infrastructure that supports and constrains the services provided to PO Ltd and its Clients.

The principal applications, and some aspects of their behaviour, are described in Chapter 2 "Business Context". This Chapter shows how these are implemented. It illustrates the various components of each business application. It discusses the other system components used to support these applications, and the Platforms on which these are located.

4.2 MAJOR ARCHITECTURAL FEATURES

The system's architecture has to cater for the following parameters.

- A very high throughput (up to 1,000 transactions per second at peaks)
- A very high availability, in particular of Counter PCs which must be able to operate autonomously if their communications links fail (at least for those applications that do not require a real-time response)
- No IT support or skills in the Post Office Outlets
- The ability to add new business applications with minimal disruption to existing systems

4.2.1 Major System Components

This shows the major logical components of the system.

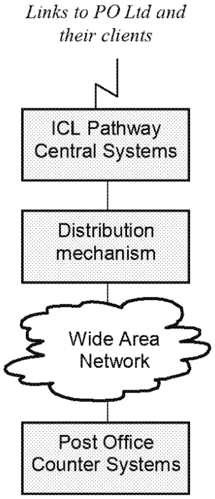
Links to PO Ltd and their clients
ICL Pathway Central Systems
Distribution mechanism
Wide Area Network
Post Office Counter Systems

Figure 4.1 - Major Logical Components

Here and elsewhere in this Document, the logical structure is described "bottom up", starting with the systems installed in Outlets.

4.2.1.1 Counter Systems

4.2.1.1.1 Outlets

Outlet is the generic name used in this Document to cover all Post Offices and Sub-Post Offices, of whatever size, which are provided with Horizon services.

4.2.1.1.2 Purpose of Counter Systems

The Counter Systems provide interactive support for all the staff in every Outlet, and give them access to the Horizon services. The interface presented to the Counter Clerk is specifically designed for retail use. It provides a user interface that requires the minimum of input from the clerk, especially via the keyboard. Many Counter applications are driven by information stored on magnetic cards or other tokens. The appropriate application is entered as soon as the Counter Clerk swipes a card or scans a bar code.

4.2.1.1.3 Availability of Counter Systems

In general, the Counter systems must be capable of operating even if they lose their connection to the Centre. An increasing number of real-time applications require a real-time response from a third party before they can proceed, and obviously these cannot be used if the communications facilities are unavailable, However, other applications should still be usable. An on-screen indication is used to show the Counter Clerk whether the communications link is available, and hence whether real-time applications can be processed.

4.2.1.1.4 Transaction Authorisation

Most of the transactions that occur at the Counter are "unplanned", in that nothing exists to represent an individual transaction until a customer walks up to the Counter and asks for some service or product. Where possible, the transaction should be able to complete without reference to the centre. In some cases, this will not be possible, and the Counter PC will have to contact the centre to seek authorisation to complete the transaction.

4.2.1.2 Wide Area Network

A communications network is used to link the Outlets with the distribution mechanism. This is provided over an ISDN line into each Outlet. The nature of the connection reflects the volumes of business transacted by the Outlet, and for busy Outlets may be a permanent connection for all or part of the day.

4.2.1.3 Distribution Mechanisms

The distribution mechanism is responsible for taking one logical stream of information from the Central Systems and fanning it out to nearly 18,000 Outlets across the UK. It also receives input from these Outlets and merges it into one ore more logical streams.

4.2.1.4 Pathway Central Systems

The central systems comprise substantial computers running large relational databases. These central systems are responsible for the following.

- Receiving information from PO Ltd and its Clients
- Storing incoming information, and in some cases using it to modify existing information
- Transforming it into a format suitable for the Counter applications
- Passing information to the Counter applications via the Distribution Mechanism
- Receiving information back from the Counter applications via the Distribution Mechanism
- Storing returned information
- Passing information back to PO Ltd and its Clients
- Passing requests for information (e.g. authorisations) to third parties in real- time, and returning theresponse to the Counter application
- Summarising information into an appropriate format for Management Information access
- Reconciling transaction flows to different recipients

4.2.1.5 Links to External Systems

The solution requires electronic links to computer systems run by:

- PO Ltd
- Clients of POCL, including the DSS
- Pathway's suppliers and support organisations
- Merchant Acquirers who authorise and process *Debit Card Service* (DCS) transactions
- A *Network Banking Engine* (NBE) that provides access to systems run by the banks and other Financial Institutions

4.2.2 Vertical Application Structure

The system architecture adopted to meet these requirements is not based on conventional client-server models. Nor does it conform to traditional central-system models. It adopts an entirely original and highly innovative four-tier model that effectively merges the qualities of central systems and client server systems.

The business services can be viewed as vertical "stripes" across a number of horizontal layers. The infrastructure supports this structure in a great many ways, as described in Chapter 5 "Application Architectures".

The Distribution mechanism referred to above is called the *Transaction Management System* (TMS) in [SADD] and other contractual documents. Its scope is shown by the dotted outline.

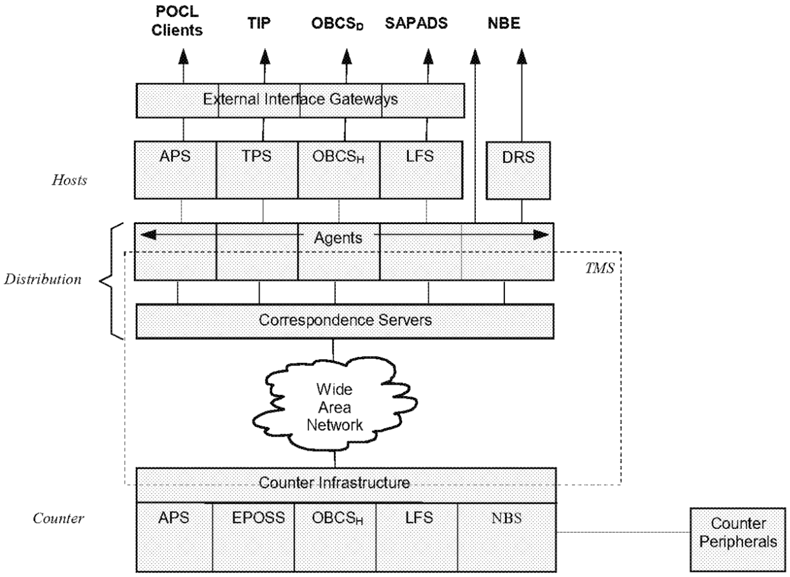

Figure 4.2 - Vertical Services

4.2.2.1 The Counter Layer

A number of applications are implemented at the Counter Layer. These implement the business services required by PO Ltd and its Clients. They use a common *Graphical User Interface* (GUI), provided by Escher, that simplifies the tasks of the Counter Clerk and aims to minimise the time taken by any Counter transaction.

The *Counter Layer* uses a messaging infrastructure provided by a system called WebRiposte. Each transaction executed at the Counter is written to a Riposte Message Store on the Counter as one or more messages. WebRiposte then replicates these messages to all the other Counters in the Outlet, and to a set of Correspondence Servers in the Campuses.

Much of the data required by Counter applications, including much of the way in which they operate, is passed in *Reference Data*, which is distributed via the same WebRiposte messaging mechanisms. Reference data originates with either PO Ltd, the appropriate Client, or within Pathway itself, and is distributed to all relevant Outlets. It enables the construction of "soft centred" applications whose operation can very easily be modified by changes to the Reference Data.

In the future, the use of WebRiposte will enable the development of Web-like applications that are specified in a scripting language with similarities to XML.

4.2.2.2 The Correspondence Layer

This layer provides the Campus end of the message distribution processes. It runs the Riposte Message Service on a set of large Correspondence Servers. It is used to pass data between the Agent Layer and the Counter Layer, and to provide resilience for this data. All messages written to the RMS are archived each day, for audit purposes.

4.2.2.3 The Agent Layer

The distribution mechanism and the Counter systems require data to be passed to them (and returned from them) in *Attribute Grammar* form. This is different from the Host layer's record view of its data. These differences in expectation mean that the data needs to be transformed from one format to another as it passes up and down the vertical stripe. Both transformations are carried out in the *Agent Layer*. Each vertical stripe of applications needs to provide its own Agents.

The Agent Layer is also responsible for obtaining real-time responses from particular Clients for applications such as NBS and DCS, and in the future for other applications such as E-Top Ups (recharging a mobile phone pay-as-you-go card).

4.2.2.4 The Host Layer

The systems at the *Host Layer* can provide permanent storage for information if required by the application's business rules. The Host systems can accept data from external Clients, and translate a file-based view of this information into discrete transactions or "messages". These are then passed to the Counters via the Agent and Correspondence Layers. Similarly, messages received from the Counters are translated back into a file-based view for transmission to the external Clients.

Host systems also implement any Reconciliation made necessary by their own business rules.

Host systems record any transformations they make, for audit purposes.

4.2.2.5 The External Interface Layer

Standardised facilities are provided to transfer bulk information to and from PO Ltd and its Clients. In most cases, this information is passed as "flat files", and a File Transfer Management Service (FTMS) is used to ensure the integrity and timeliness of the data passed across the interface. Information is generated by, or passed to, the Host Layer.

The system maintains an audit log of information flows across this boundary. In most cases, the actual data passed is also retained for audit purposes.

4.2.2.6 Summary of Application Structure

The Correspondence Layer servers and the Counter Infrastructure, which implement the overall WebRiposte service, are transparent to the application's vertical structure (though they provide generic services which are used by both the Agent Layer and the Counter Desktop layer). Thus, each vertical application has four major components within the Horizon domain:

- Counter Applications
- One of more Agents
- A Host System
- An External Interface

The thickness of each horizontal layer within each vertical stripe can vary enormously and in some cases may almost disappear or be merged into another layer. For example, an Agent and a Host may be merged if the Host only supports transient storage of information.

4.3 Logical Architecture

A number of logical components are provided to support the vertical services. These are shown below. They include not only operational components that directly support the provision of the required services to business applications, but also components that support the Pathway business itself.

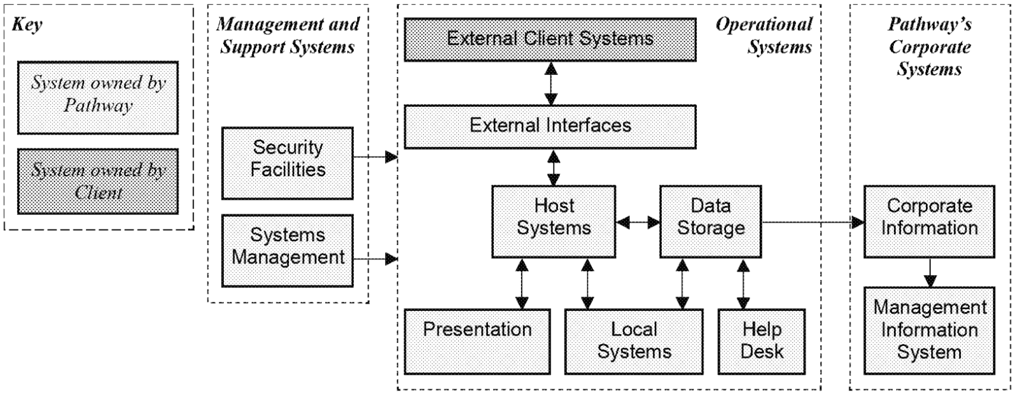

Figure 4.3 - Logical Architecture

4.3.1 Operational Systems

These include the components that support the vertical application structure.

4.3.1.1 Presentation

This mechanism supports the Riposte Desktop interface that handles the operational aspects of the Counter system. It takes information provided by the Host Systems and displays it to the Counter Clerk, and takes information entered by the Counter Clerk and propagates it to the Host Systems. It applies very few business rules, and logically has no persistent data storage apart from Reference Data.

4.3.1.2 Local Systems

Outlets need support for local business processes, such as the following.

- Local user management
- Stock management
- Cash drawer management
- Balancing and reconciliation
- The production of local reports

The local systems access local operational data, and contain sufficient business rules to support local processes. To keep the Counter Clerk's view of the Counter PC consistent and simple, these local applications are implemented as part of the Riposte Desktop. They support the same presentation mechanisms as the main business applications.

4.3.1.3 Host Systems

These Servers run mainly large background batch processes and represent the part of the architecture that is responsible for the following functions.

- Manipulating the information received from the External Client Systems into a form that is appropriate for the presentation mechanism and vice versa
- Applying business rules that are relevant to that information
- Storing non-transient information within the "Data Storage" component. This includes metrics needed for the computation of SLAs that may modify the payments due from PO Ltd for the achievement of key deliverables.
- Manipulating any such stored information

There are a number of Host systems, each aligned with a different business streams. Others will be added as new applications are supported.

4.3.1.4 Data Storage

This represents the base data needed to support the main business applications. It includes their archiving and recovery mechanisms as well as those concerned solely with data storage.

In this logical model, data is considered as a single resource, even though it may be distributed throughout the solution and have different owners. Some of the data has a relatively long life and some is transient. In general, data is structured to optimise the behaviour of the operational systems to which it belongs.

The data held includes metrics that allows measurement of system performance in a number of dimensions that allow calculation of the service levels achieved. This is needed both to meet reporting requirements, and because there are penalties for failure to meet SLAs.

4.3.1.5 External Interfaces

These represent the mechanisms that are used to move information to and from the External Client Systems. They include file level validation and integrity verification mechanisms; audit trailing of file receipt and transmission; data compression if necessary for performance reasons; and recovery/retry mechanisms.

Although shown as one "box", this exists at both ends of the connection. The usual mechanism consists of file transfer operations between an Pathway provided system at the Client's premises, and a similar system at an Pathway Campus.

These interfaces can also be real-time. Interactive messages can be driven either by the Client or by Horizon.

4.3.1.6 External Client Systems

Horizon has to connect to these, and to transfer information to and from them in a secure manner.

There are a large number of sources of external data, or locations to which Horizon must transfer data. An example is the *Automated Payment Service* (APS). Payments are made by customers using magnetic cards or smart cards issued by the Utility companies. Records of these payments are passed to the Utilities via the APS application. The recipient system could be any type of Platform, running any type of industry standard or proprietary operating system and middleware.

The system boundary between Horizon and these external systems varies. In the usual case, the Client transfers the data to a gateway system on their premises provided by Pathway, or takes data from that gateway.

4.3.1.7 Help Desks

4.3.1.7.1 Horizon Systems Help Desk

This is operated by FSCS. Counter Clerks can telephone it when they have a problem with the operation of their equipment or (in certain cases) of the Counter applications.

Telephone calls to the Help Desk use a standard set of “local call” (0845 or 0345) numbers. A Call Managing system is used to route the call to an appropriate operator.

4.3.1.7.2 System Support Centre (SSC)

This is provided by Pathway. It provides a second level support function.

4.3.1.7.3 UK System Service (UKSS)

UKSS provides a hardware support and fix process on behalf of Pathway.

4.3.2 Pathway’s Corporate Systems

These systems support Pathway’s business objectives by gathering, transforming, analysing and presenting the information needed to charge for the services provided.

4.3.2.1 Corporate Information

This is a *Data Warehouse*, separate from the main business data storage. It holds information used to support Pathway’s own management processes, including those contractually necessary to assess conformance to the SLAs, and (from BI3) information needed to provide sales and marketing information to PO Ltd. Data is held in such a way that it can support different types of analysis.

The Data Warehouse runs mainly large batch processes responsible for the following.

- Receiving information from the Input systems, and converting the various source formats into a consistent format suitable for use by all the output components.
- Aggregation of transactional information from the Input systems to summary totals.
- Housekeeping of the information repository to satisfy all archiving, retrieval and recovery requirements.
- Capacity Management activities that are used to ensure the system infrastructure can cope with envisaged changes to the workload.

The following diagram gives a high-level view of the corporate information, and shows the derivation of the data in the system.

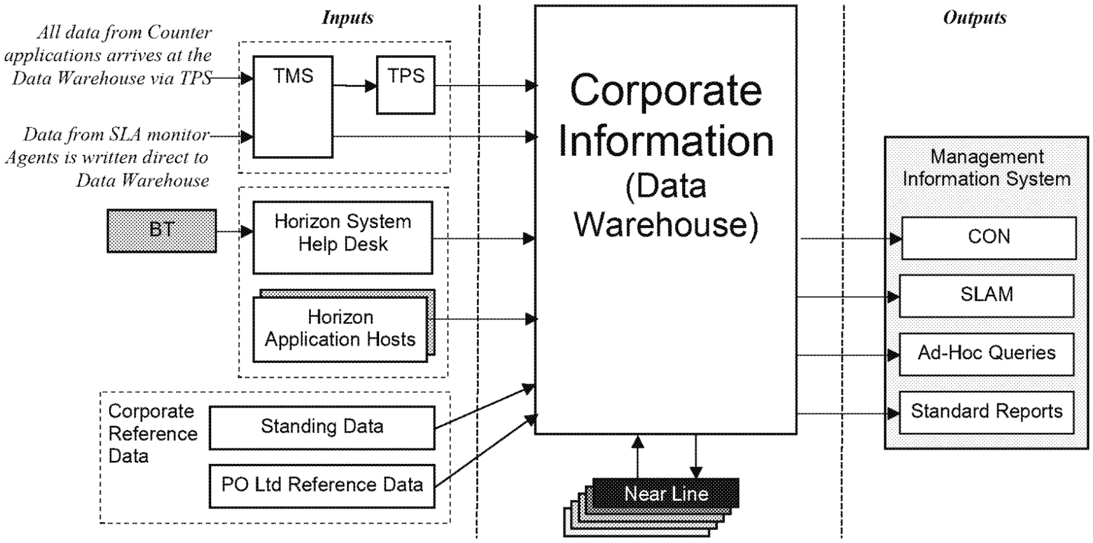
Inputs
Outputs
All data from Counter applications arrives at the Data Warehouse via TPS
Data from SLA monitor Agents is written direct to Data Warehouse
TMS
TPS
BT
Horizon System Help Desk
Horizon Application Hosts
Corporate Reference Data
Standing Data
PO Ltd Reference Data
Corporate Information (Data Warehouse)
Near Line
Management Information System
CON
SLAM
Ad-Hoc Queries
Standard Reports

Figure 4.4 - Corporate Information Flows

Inputs to the Data Warehouse come from the following logical input components:

- Riposte messages comprising all Counter transactions (via the *Transaction Processing System*, TPS)
- Horizon Systems Help Desk and BT for details of calls handled
- Reference Data Database

All information flowing into the Data Warehouse is recorded for audit purposes.

4.3.2.2 Management Information System (MIS)

The Output components represent the *Management Information System* (MIS) applications. This provides a set of analysis tools that can sift and structure the information in the Data Warehouse to support Pathway's management activities. These are mainly enquiry and extract processes, on line and batch, but also include on-line general maintenance functions to record additional information not otherwise provided by the Input system.

4.3.2.2.1 Service Level Contract Administration (SLCA)

SLCA is used, in conjunction with its reporting system Service Level Agreement Monitoring (SLAM), to compare the performance of the Horizon system against a number of measures and formulae established in the Codified Agreement.

4.3.2.2.2 Service Level Agreement Monitor (SLAM)

This is an adjunct to SLCA, and reports on information pertaining to the *Service Level Agreements* (SLAs) between Pathway and PO Ltd, and monitors compliance with these SLAs. It facilitates periodic internal reviews, Pathway/Customer reviews and Pathway/Supplier reviews. It uses timestamps generated by various system components, down to the Outlet level where appropriate, as well as information relating to other activities. This is keyed in manually.

4.3.2.2.3 Other MIS Applications

The information held on the Data Warehouse is also used for other purposes outside of the core Pathway MIS requirements. Typically, aggregated and summary reports are delivered from the Data Warehouse, and exception or transaction level reports are delivered from Host Systems.

In addition, from BI3, information relating to NBS and DCS transactions is provided to PO Ltd in a number of reports that support their business processes.

4.3.2.3 Data Reconciliation Service (DRS)

At BI3, a *Data Reconciliation Service* (DRS) is introduced. This takes information relating to all NBS and DCS transactions, and reconciles the different data flows. It maintains data about transactions until they are reconciled (this may take some days) and for 90 days thereafter.

4.3.3 Management and Support Systems

A range of logical systems is provided to enable Pathway to manage and support the operational systems and corporate applications.

4.3.3.1 Security Systems

Data in Horizon represents large amounts of either PO Ltd's, or PO Ltd Clients' money. Security mechanisms are provided to ensure the integrity of this data. Similar mechanisms are used to protect the confidentiality of personal information.

4.3.3.1.1 Authentication Systems

All users must authenticate themselves before they are permitted to access any Horizon systems. The type of authentication depends on the role and location of the user.

4.3.3.1.1.1 Counter Clerk Authentication

Within Outlets, Counter Clerks, and Post Office Managers are authenticated by the Riposte Desktop. The Post Office Manager specifies to Riposte the Counter Clerks who may use that Outlet's Counters. The Counter Clerks authenticate using a username and password whenever they begin to use a Counter PC.

4.3.3.1.1.2 Counter Authentication at Startup

Post Office Managers are provided with Smart Cards that they must use when switching on or rebooting the Counter PCs. They must follow a Post Office Log On (POLO) dialogue that requires the smart card along with a 14-characyter PIN. The operational information stored on the Counter PCs' disks is encrypted. The decryption key is derived as part of the POLO process.

4.3.3.1.1.3 Customer Authentication

Customers carrying out NBS transactions must verify themselves by typing a PIN into a PIN Pad before the transaction is authorised. The encrypted PIN value is sent to the Customer's FI as part of a Request ([R]) message, and the result of the authorisation (Accept or Decline) is included in the returned Authorisation ([A]) message.

4.3.3.1.1.4 Authentication in Campuses

Users accessing the central systems for operational management or other administrative purposes must authenticate using hand held SecurID Smart Card tokens. These display a randomly changing number. The user authenticates by typing the displayed number and his or her own PIN when prompted to do so.

4.3.3.1.2 Access Control

Access Control entails limiting the access granted to a user following authentication. No access is allowed before a user is authenticated. The access permitted depends upon the Role(s) authorised for each user. Roles are groupings of functions, implemented in various ways by the different Platforms.

4.3.3.1.3 Audit

All successful and unsuccessful authentication attempts, as well as administrative actions to add or delete users, or change their attributes, are recorded for audit purposes. Many other operations are also audited, including all financial transactions.

4.3.3.1.4 Cryptography

Cryptographic techniques are used to protect the integrity of financial and other information within the system, and the confidentiality of personal data stored within the system. The algorithms, encryption devices and techniques used are those approved by HMG's *Communications Electronic Security Group* (CESG).

4.3.3.1.4.1 PIN Encryption

PINs typed by Customers into Outlet-based PIN Pads are encrypted within the PIN Pad and the encrypted value returned to the Counter for transmission to the Campus. The the key used for this encryption is unique to the Outlet. At the Campus, the encrypted PIN block is translated to use a Key that is agreed between Pathway and the NBE.

4.3.3.1.4.2 Link Protection

Hardware and software based encryption technology is used, where appropriate, to provide integrity and confidentiality protection on links between Pathway and its partners. Software encryption is used for all traffic between Outlets and the Campuses. The Key used to encrypt traffic to and from a particular Outlet has the additional benefit of acting as an authentication of the Outlet.

4.3.3.1.4.3 Message Protection

Encryption is also used to "seal" important data items that may be transferred over several links, and where the end-to-end integrity of the data is important. The recipient can then verify the integrity of the sealed data by using an appropriate public key.

⇨ The integrity of Automated Payments, and distribution of updated software modules, is protected using this technique

⇨ The integrity of Request, Authorisation and Confirmation (R, A, C) messages sent to or received from the NBE (for NBS transactions) or MA (for DCS) is protected in a similar way

4.3.3.1.4.4 Filestore Encryption in Outlets

Inf ormation stored on Counter PCs is encrypted and can only be decrypted as part of the Post Office Log On dialogue. This ensures that the data is inaccessible should the terminal be stolen.

4.3.3.1.5 Key Management

A Key Management Application is provided to support the distribution of crypto Keys to relevant platforms to support the encryption facilities, and to revoke these when they expire or are compromised.

4.3.3.2 Systems Management and Support

FSCS, on behalf of Pathway, provides a range of operational management and systems management facilities. These include the following.

- Day to day operation and scheduling of the central systems
- Operation of the Horizon Systems Help Desk, which manages calls from Outlet staff in response to problems with the Outlet equipment
- Monitoring the behaviour of the various components of the system
- Distributing new or amended software to them.

Tivoli Enterprise Management facilities are used for systems management, including event management and Software Distribution. Tivoli interfaces with the native facilities of the remote Platforms, or with other management facilities. Additional facilities are provided by FSCS to monitor and broadcast the status of Outlet systems. This information is held in an *Operational Management Database* (OMDB) and is made available on a Web server that can be accessed by some support staff using Internet Explorer. The OMDB is held within the Campus's EMC disk array. A subset of this information is replicated to a *Service Management Database* (SMDB) where it can be accessed by a rather larger number of support and management staff.

BMC Patrol facilities are used to manage the Sequent Host systems.

HP OpenView is used to manage the network.

All Systems Management processes that cause a persistent change to the nature of the system are recorded for audit purposes.

4.3.3.3 Estate Management

The Horizon system supports up to 38,000 Counter PCs spread over nearly 18,000 Outlets. Managing the ongoing installation and configuration of new Outlets and replacement Counter PCs, and the temporary or permanent removal of Outlets, is a complex and potentially error prone process. A number of steps are taken to simplify it and speed it up.

4.3.3.3.1 Counter PC Replacements

A replacement Counter PC is effectively a "vanilla PC". It has the ability to connect to a dedicated Boot Server within one of the Campuses. This server initiates the Auto Configuration process, which "personalises" the Counter PC and enables it to process transactions. It also brings its software state up to that of the rest of the estate.

4.3.3.3.2 Steady State Outlet Change

Similar mechanisms are used when a new Outlet is opened, or additional Counter PCs are installed in an existing Outlet. These changes are implemented by the *Outlet Change Management System* (OCMS). Input to OCMS is Change Requests received from PO Ltd, for example to open or close Outlets, or vary the number of Counters in an Outlet. OCMS generates data feeds to a number of other systems involved in managing the Outlet estate, including:

- Auto Configuration
- Tivoli
- KMS

4.4 PHYSICAL ARCHITECTURE

This sub-section summarises the physical components that support the logical functions discussed above.

4.4.1 General

4.4.1.1 Campuses

Counter services are supported by a number of Platforms that are in the main located in physically secure Pathway Data Centres. For resilience there are two Data Centres, located at Wigan and Bootle, each called a *Campus*. Each Campus provides fallback for the other.

4.4.1.2 Campus LAN

Each Campus has a set of duplexed central high-speed *Local Area Networks* (LANs). Each server is connected to both plexes of a particular LAN. The LANs are supported by a Cisco Switch that supports “Virtual LANs” (VLANs) spanning both Campuses. This enables simplified failover of certain servers between Campuses.

Each Campus also has a set of WAN and ISDN Routers that form the Pathway end of the connections to external services and to the Outlets, including the FRIACO services introduced at BI3. These are separated from the Campus LAN by a pair of *Logical Campus Routers*. These provide a level of indirection and remove the need for the central servers to know the network addresses of all the sites and Outlets that connect to the system.

4.4.1.3 Platform Classes

There are a number of different classes of Platform, varying widely in their software environments. The following diagram illustrates these classes of Platform types, and shows their locations.

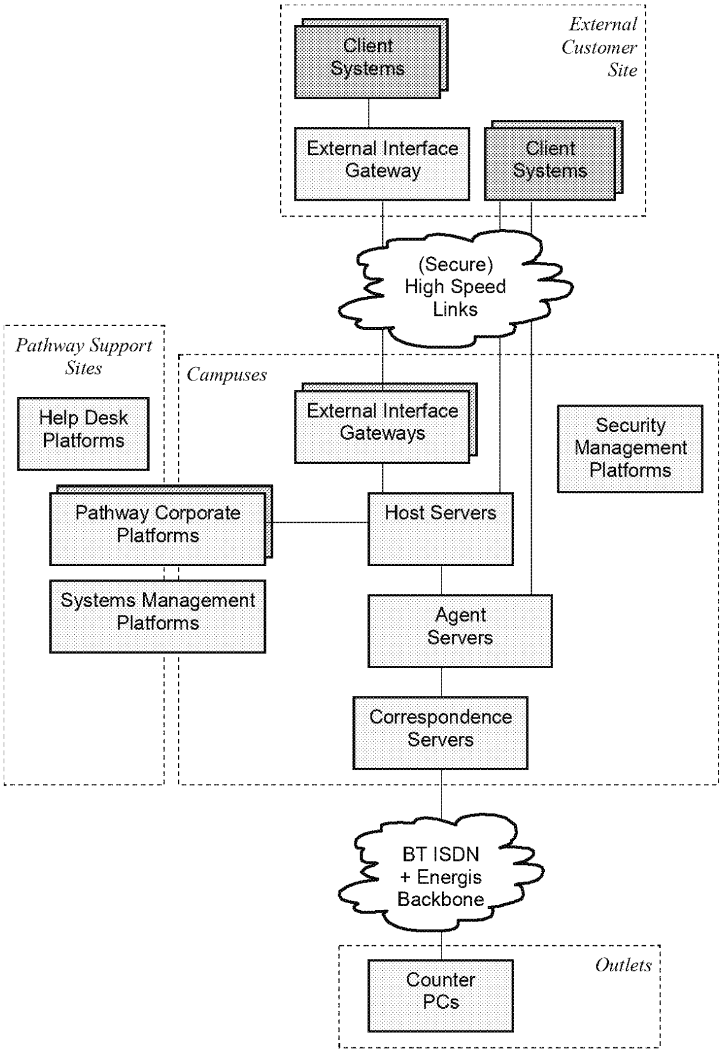
Client Systems
External Customer Site
External Interface Gateway
Client Systems
(Secure) High Speed Links
Pathway Support Sites
Help Desk Platforms
Campuses
External Interface Gateways
Security Management Platforms
Pathway Corporate Platforms
Host Servers
Systems Management Platforms
Agent Servers
Correspondence Servers
BT ISDN + Energis Backbone
Outlets
Counter PCs

Figure 4.5 - Physical Components

4.4.2 Counter PC Platform

4.4.2.1 Counter PC Hardware

Each *Counter PC* is an Intel-based PC with a 400 MHz processor, 128 MB of memory and a 13 GB (or larger) disk. Most Counter PCs occupy fixed positions within an Outlet. A small number of Single Counter PCs are defined as *Mobile Outlets*, and may be moved between different locations. In some Outlets with very limited space, Counters may be held on trolleys.

4.4.2.2 Network Connections

One Counter in each Outlet (the Gateway PC) acts as the connection to the Campuses. Other Counter PCs within the Outlet are linked to the Gateway PC via LAN cards. All traffic across the Outlet LAN is encrypted using VPN facilities.

4.4.2.3 The Gateway PC

The *Gateway PC* is responsible for the communication with the Campus. It supports a mechanism known as a *Virtual Private Network*, or VPN, in which all communication with the Campus is encrypted with a Key that is unique to that Outlet. Thus, as well as protecting the data passed to and from the Outlet, this acts as a form of authentication of the Outlet to the Campus (and vice versa).

Most Outlets communicate with the Correspondence Servers at the Campuses via the BT supplied ISDN network. Connections are passed from BT to the Energis data network and thence to a bank of Campus ISDN Routers. Some Outlets, in areas where ISDN is not available, communicate with the Campuses via satellite links.

To cater for an increasing number of applications that require real-time responses, the network connections in a proportion of Outlets are kept "nailed up" for all or part of the working day.

The Gateway PC also acts as a logical "back office" PC. It supports an A4 printer used to produce reports. In a small office, this is a compact ink-jet printer. In the larger offices, it is a laser printer.

4.4.2.4 Counter PC Software

Each Counter PC runs under the Windows NT Workstation V4.0 operating system, with specific device drivers to support the Counter peripherals. However, the conventional Windows NT desktop is replaced by the Riposte Login screen and Desktop, and the Counter Clerk has no access to standard Windows NT facilities.

4.4.2.5 Counter PC Peripherals

Counter PCs are equipped with a number of peripherals including the following.

- A 10 inch colour *Touch Screen* or 12" flat panel screen
- A specialised financial keyboard with magnetic stripe reader and Smart Card reader
- A hand held Bar Code Reader
- PO Ltd-provided weigh scales that are shared, by networking, between a preconfigured set of Counters. Counter Clerks may press a Menu Button on their screen to read the weight of an object on the scales.
- A tally roll printer including a slip printing facility
- A PIN Pad, on which Customers can enter a multi-digit *Personal Identification Number* (PIN) to verify an NBS transaction

4.4.3 Network Connections

At the Campuses, Outlet connections are supported by banks of ISDN or Frame Relay Routers, or Energis-supplied Routers that support a *Fixed Rate Internet Access Call Origination* (FRIACO) service. These are connected to a duplexed *Access LAN*, which is connected to the (also Duplexed) Server LAN via a set of Routers and a bank of *VPN Servers*. These servers carry out the Campus end of the link encryption process described above, and hence ensure that communication is only from *bona fide* Outlets.

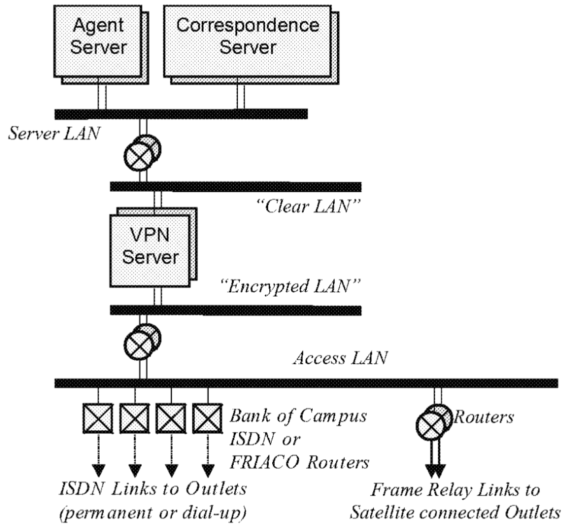
Agent Server
Correspondence Server
Server LAN
"Clear LAN"
VPN Server
"Encrypted LAN"
Access LAN
Bank of Campus ISDN or FRIACO Routers
Routers
ISDN Links to Outlets (permanent or dial-up)
Frame Relay Links to Satellite connected Outlets

Figure 4.6 - Correspondence and Agent Servers

4.4.4 Correspondence Server Platform

There are a number of these in each Campus. Each is a four-processor Compaq DL360 server, with approximately 150 GB of disc storage, running under Windows NT Server V4.0. The main software on the server is the Riposte Message Service. The data in the message store is held on an EMC disk array that provides disk mirroring and backup facilities.

Communication with Agent Servers is via the duplexed Server LAN, as shown above.

4.4.5 Agent Server Platform

These are high performance Compaq DL360 Pentium III PC Servers. They run under Windows NT Server. They support Riposte Client software, and any client software such as Oracle as required. They form the interface between the Host Central Servers and the Correspondence Servers. The Agent applications act as clients to both, by "pulling" information from one and "pushing" it to the other. This occurs in both directions.

The term *Agents* within the Pathway solution always refers explicitly to the interface layer above Riposte.

A set of specialised Agent platforms are provided for NBS and DCS, and manage the real-time interface to the relevant client systems (NBE or MA). These are held within a *De-Militarised Zone* (DMZ) to isolate the Campus LAN from these Client systems.

4.4.6 Host Servers

4.4.6.1 Host Central Server Platform

There is a Host Central Server in each Campus. It is a single Sequent NUMA-Q system, running under Sequent's Dynix version of UNIX, and supporting a number of Oracle databases. Agent applications use Oracle SQL*Net to access data in these databases.

Work is scheduled on each Host Central Server (and on the Agent and some other servers) by the Maestro scheduler. This supports time based scheduling and Job inter-dependencies.

A systems management product, BMC Patrol, monitors the system's behaviour and performance, including that of the Oracle database. It passes events and alerts on to Tivoli.

4.4.6.2 Other Host Server Platforms

A number of non-mainstream applications are hosted on Compaq Windows NT servers running Microsoft SQL Server.

4.4.7 External Interface Gateway Platforms

Much Campus processing involves file transfers to and from external Clients. Apart from OBCS, the strategy for these is to use a pair of PC servers, supplied and managed by Pathway. One is installed in a Campus, the other in the external organisation's premises, along with a Router or other connection to the data network. The Servers run under Windows NT Server. The transfer process is handled by the *File Transfer Management System* (FTMS). This is a generic mechanism that is configured to the particular needs of each interface. It includes a set of functions, such as file compression/decompression or encryption/decryption that can be included or excluded depending on the requirements of the interface. Some or all of these functions are grouped together for each specific use of the FTMS. The Transfer protocol used is the Windows NT file copy process.

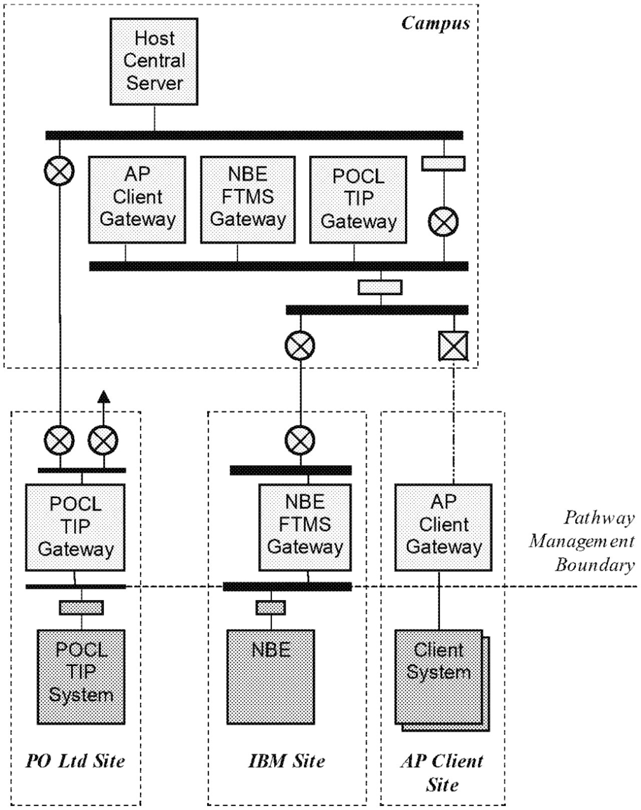

Figure 4.7 - External Interface Gateways

4.4.7.1 AP Client Interface Gateway

Clients communicate with the Horizon system via a direct connection from the Campus AP Client Gateway, via ISDN, to the PO Ltd AP Clients. Each Campus AP Client Gateway is sized to be able to support connections to a considerable number of AP Clients.

4.4.7.2 PO Ltd TIP Interface Gateway

The PO Ltd TIP service is sent records of all transactions that take place at all Outlet Counters. It also provides Pathway with Reference Data. This service runs on a PO Ltd site at Huthwaite, near Chesterfield. A separate FTMS service, running on the same platforms, sends NBS management reports and DRS reconciliation reports to PO Ltd each day.

4.4.7.3 NBE Gateway

The NBE sends files of confirmation messages to Horizon at the close of each day. These are transmitted via FTMS.

4.4.8 Client Systems Platforms

This term includes a variety of platform types. Their exact nature is only of interest in the few cases where information flows directly to and from the Client System, rather than via the External Interface Gateway platforms. These platforms are as follows.

4.4.8.1 DWP OBCS Server

The DWP *Area Computing Centre* (ACC) contains a Fujitsu SX server running under Fujitsu's proprietary operating system VME. This hosts the DSS OBCS System, which is run by EDS. Access to these systems is via a Firewall. Pathway has a partition that is used to exchange data with the DWP. Files are transferred directly between the VME system and the Host Central Server. The overall structure is as follows.

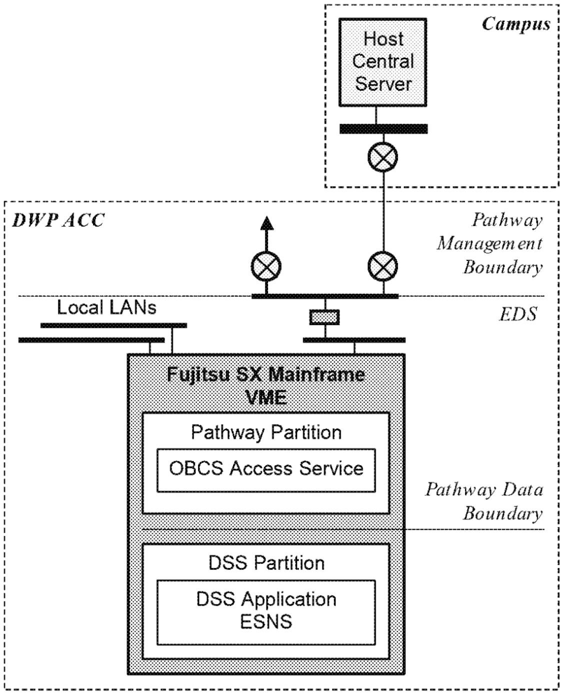

Figure 4.8 - OBCS System Boundaries

There is a two-way batch communication between the OBCS$_D$ service and the OBCS$_H$ service. The physical components are as shown in the diagram above.

4.4.9 Pathway Corporate Platforms

A number of Platforms are used to provide internal Pathway services, including the collection and analysis of data used to support the SLAs negotiated with PO Ltd.

4.4.9.1 Data Warehouse Server

The Data Warehouse Server is located at one of the Campuses and is a single Sequent NUMA-Q machine. Its data is held on an EMC Disk Array. It is used to collect performance data from other systems. This data is retained for up to four months before being archived to tape.

The MIS is a collection of applications that run within the Data Warehouse Server. These include Oracle's *On-Line Analytical Processing* (OLAP) Express packages. OLAP permits its users to generate and subsequently analyse three-dimensional "cubes" containing the data of interest, and subsequently to "drill down" through this to finer and finer levels of detail.

This service runs in a separate NUMA-Q Quad from the Data Warehouse service for two main reasons:

- Oracle Express does not currently operate in client/server mode and the user sessions are particularly processor and memory intensive. Running these sessions on the same processors as the Data Warehouse would require a different configuration that is not conducive to running an efficient enquiry service.
- The OLAP data cubes generated for MIS applications are likely to be quite large.

4.4.9.2 MIS Client PCs

MIS services are accessed via a set of *Client PCs*, standard Windows NT Workstations running client software for one of more of the corporate applications. These Client PCs are based at Feltham and Bracknell. They include the *Business Objects* software that is used to generate database reports.

4.4.10 Security Management Platforms

A number of types of Platform are used to support the security needs of Pathway.

4.4.10.1 Domain Controller

Campus and support centre NT platforms make extensive use of the NT Domain Model. One or more domain controllers are provided in each security Domain. They authenticate users who carry out a direct Windows NT connection (for example to administer or support the Campus servers).

4.4.10.2 SecurID Server

This runs the SecurID service that authenticates any user who is required to use a token as part of this or her authentication process. This authentication is built in to the Windows NT Login processing, and supplements the standard Windows NT authentication carried out by the Domain Controllers.

4.4.10.3 Firewall Management

This is a platform used to manage the Firewalls that are used to restrict access into the Campuses.

4.4.10.4 Network Management Server

This platform runs HP OpenView. It is used to manage the Routers and other network components included in the system.

It also runs the *Terminal Access Controller Access Control System* (TACACS) that authenticates users accessing Horizon services via direct terminal access. New connections of this type are routed to the *Network Management Server* by the WAN Routers.

4.4.10.5 KMA Server and Workstations

The KMA Server supports a range of *Key Management* functions. It generates and stores cryptographic keys, and distributes these to other Platforms such as Post Office Counters and Routers. It uses a Random Number Generator to generate the entropy needed for these Keys.

The KMA Server is managed by a KMA Workstation, and its database is administered by a KMS Admin Workstation. The KMA Workstation operates in conjunction with a CA Workstation that is kept in a secure location and generates Certificates that verify the authenticity of the Keys.

4.4.10.6 One Time Password Workstation

There is a need to generate one-off passwords for authorised visitors to an Outlet, such as auditors or engineers. The freestanding One Time Password Workstation carries out that task. It generates such a password for users who have been verbally authenticated in some way. The password is given verbally over the phone, in clear, to the authorised user.

4.4.11 Systems Management Platforms

A number of Platforms are provided specifically to support the systems management functions needed to ensure the smooth running of the services supported by the other Platform types.

4.4.11.1 Tivoli Management Servers

A central management system and a number of subsidiary servers are used to support the Tivoli Management Environment (TME). The central system supports the principal management functions. They provide a Software Distribution hierarchy, so that the central platform does not have the overhead of managing nearly 18,000 Outlets.

4.4.11.2 Tivoli Inventory Database Servers

These maintain a record of all the managed objects known to Tivoli. They are Windows NT server Platforms. They access an Oracle database (the *Operational Management Database*, OMDB), held on the Campus's EMC disk array, that provides a Web-based interface. This enables a limited set of support units to monitor the status of the systems management functions.

4.4.11.3 Tivoli Event Console Server (TECs)

A number of SUN servers are located at each Campus to manage events generated by the Tivoli client software on each managed node. Each is responsible for a subset of the Outlets, and feeds summarised management information up to the central management system.

4.4.11.4 Service Management Database (SMDB) Server

This is is outside the Campus firewall, and takes a data feed from the Operational Management Database. It provides a similar support facility, though because it is outside the firewall, it can be used by a much wider variety of support units.

4.4.11.5 Audit Server

This is a Windows NT server attached to an EMC Centera system (the Audit Data Repository). This is a high capacity disk array that is optimised for long-term storage of, and easy access to, historical data. It replaces a set of DLT tape drives used prior to BI3, and removes the need for error-prone tape handling processes.

The Audit Server collects audit data originating on other Platforms and writes it to the Centera system.

4.4.11.6 Audit Workstations

A number of workstations are used to extract data from the Audit Server and enable it to be refined in support of audit enquiries.

4.4.12 Estate Management

A number of Platforms are provided specifically to handle the tasks involved in rolling out new Outlets, or installing new Counter PCs in existing Outlets, and in updating the software on these subsequently.

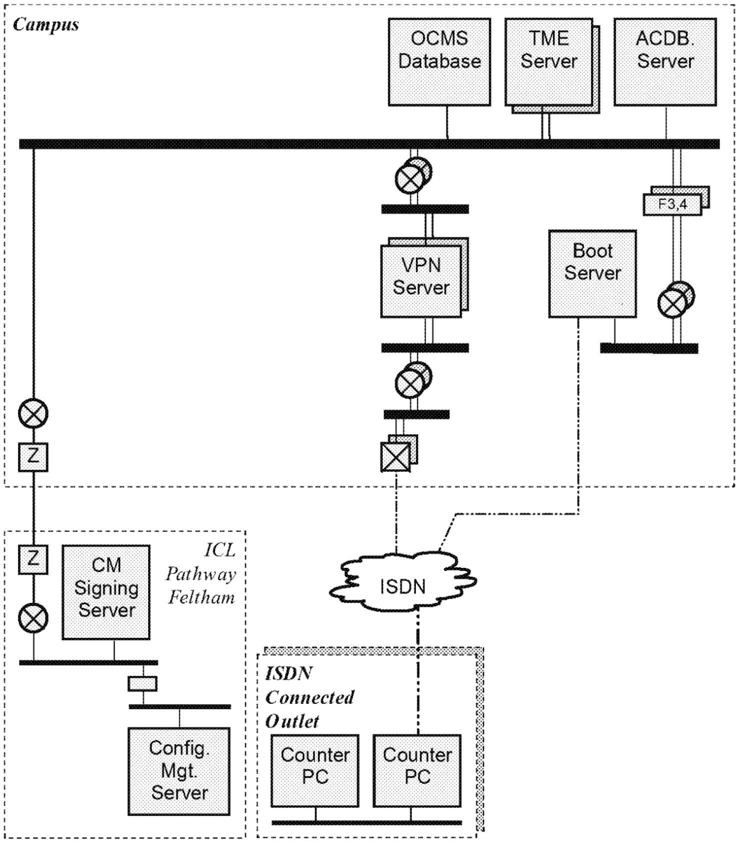

Figure 4.9 – Estate Management

4.4.12.1 ACDB Server

This server hold information that defines the "personality" of each installed Counter, and those that are expected to be installed in the near future. It was populated initially from the Roll-out Database during the Horizon rollout, and is now updated as part of the *Operational Business Change* (OBC) process with information from the TME Management Servers and the OCMS Server. These provide it with details of Counters due to be installed in the near future. It feeds some of this information to the Boot Server. The rest, in the form of the ACF, is used to configure the Counter PC, according to its location and role, when it first connects into Horizon.

The ACDB Server also provides a data feed to the Tivoli management platforms.

4.4.12.2 Boot Server

When a Counter PC is installed, and boots up for the first time, it connects to the Boot Server. This server contains the data that the Counter PCs need to configure themselves. It downloads a basic configuration file to the Gateway PC, and this provides enough information to enable the Counter to connect to the appropriate TME Server. This then "personalises" it with information in the ACF sent from the Auto-configuration Database.

The Boot server is a Windows NT platform. It is connected to both the ISDN and Frame Relay networks, and is isolated from the main Campus LAN by a Firewall.

4.4.12.3 CM Signing Server

This server is used to add a cryptographic seal to any software released from Pathway in Feltham for distribution via the Software Distribution facilities.

4.4.12.4 OCMS Server

The *Operational Change Management Service* (OCMS) is used to manage the installation or removal of Outlets, and changes to the number of Counters in an Outlet.

4.4.13 Reference Data Management

A number of platforms are provided to handle the receipt, validation, manipulation and distribution of Reference Data received from PO Ltd, or its Clients, or generated within Pathway.

4.4.13.1 Reference Data Management Centre

This is an application that runs on the Host Central Server.

4.4.13.2 RDMC Administration Workstation

The RDMC Administration Workstation is used for data entry and Reference Data release authorisation. It also provides a facility for Pathway Customer Services to send messages, of up to a single A4 page, to some or all installed Outlets.

It is a standard networked PC using Windows NT 4 Workstation. It runs a bespoke application on top of Microsoft Access that then links to the *Reference Data Management Centre (*RDMC) Oracle database using ODBC over SQL*Net.

4.4.14 Printing

4.4.14.1 Central Printing

There are no central printers used for operational purposes. Neither are there any support staff to distribute printout if it were generated at the centre. Consequently, any printing required from the central systems is routed to a LAN connected printer at Feltham.

4.4.14.2 Outlet Counter Printing

Each Outlet Counter has a combined slip and receipt printer. It is driven directly by Riposte's *Peripheral Broker*. It is used for receipts and for local reports.

4.4.14.3 Outlet "Back Office" Printing

Two styles of back office printer are available and are selected based on the size of the Outlet. This printer is connected to one of the Counter position machines and is shared across the local network by the other Outlet machines, as required.

There is an Inkjet printer for smaller offices and a laser printer for larger office.

These printers are used for producing office level reports. They use normal Windows printing mechanisms.

4.5 PLATFORM LOCATIONS

The following diagram shows the physical location of the Platforms used, and of the external systems that require access to Horizon.

This diagram shows one of the Campuses in detail. The other is broadly identical. In reality, some of the Platforms are installed in either one or the other, though most are at both. There is no architectural significance as to which is installed where, and this decision is usually made for reasons of space in the Computer suite or to balance the network load between the two Campuses. In addition, in many respects each Campus acts as a fallback for the other.

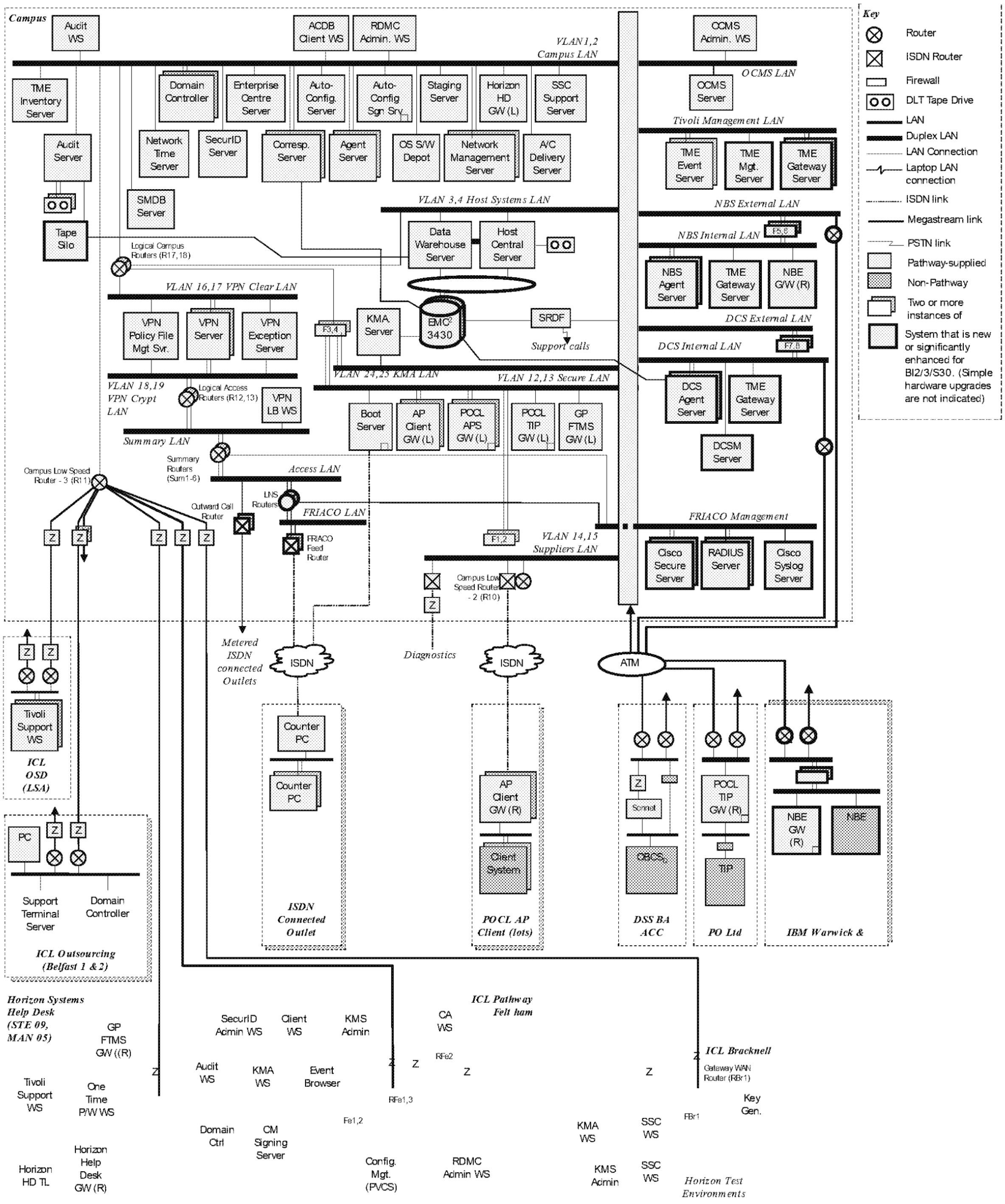

Figure 4.10 - Platform Locations

4.5.1 Platform Changes Since CSR+

This diagram shows the situation at S30. Changes from CSR+ (CI4) include the following.

4.5.1.1 Platform Changes Following Rollout of CSR+

The **POLO Recovery Code Workstation** and **POLO Recovery Server** have been removed following the completion of the Counter migration to CSR+.

4.5.1.2 Platform Changes Following Rollout of all ECCO Outlets

Once the rollout to ECCO-equiped Outlets was complete, the following platforms were removed.

- Migration Agent Server
- ECCO Migration Laptop

4.5.1.3 Platform Changes Following Completion of National Rollout

Once the National Rollout was complete, the following platforms were removed.

- Rollout Database Server
- Rollout Database Client

4.5.1.4 Platform Changes to Support FRIACO Network Services

- Introduction of FRIACO Feed Router to replace many existing Campus ISDN Routers
- Introduction of RADIUS Server
- Introduction of Cisco Syslog Server
- Introduction of Cisco Secure Server
- Introduction of LNS Server
- Introduction of Outward Call Router for continuing outward connections to Outlets

4.5.1.5 Platform Changes to support NBS

- Introduction of NBS Agent Servers
- Introduction of NBS Gateway Servers (both Remote and Local)
- Introduction of HSM Key Generation Workstation
- Introduction of PIN Pad Key Generation Workstation
- Introduction of links to a *Network Banking Engine* (NBE) to support the NBS application

4.5.1.6 Platform Changes to support DCS

- Introduction of DCS Agent Servers
- Introduction of DCSM Server

4.5.1.7 Systems Management Changes

Introduction of a *TME Gateway Server* to support an upgrade in the Tivoli software level.

4.5.1.8 Other Platform Changes

- Satellite access to Outlets that are not contactable by ISDN. These will communicate with a ground station that is then linked via the Energis network to the Campuses.
- Introduction of Mobile Counters
- Introduction of a *Service Management Database* (SMDB) that provides support services to CS and others, using information derived from the FSCS *Operational Management Database* (OMDB)

Check that all of these appear in the diagram.

4.6 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 3	IT Perspectives on the Horizon System	Describes the main classes of people concerned with the systems developed by Pathway.
Next	Chapter 5	Application Architectures	Describes in detail the ways in which applications are constructed to exploit the architecture. It describes the various types of Agent., the construction of Host applications, and the use of Reference Data
Chapter 2		The Horizon Business Context	Describes the principal applications supported.
Chapter 6		Distributed Application Services	Describes the message passing facilities of Riposte
Chapter 7		Information Management	Describes the data handling mechanisms of Riposte and Oracle, and the structure and use of Reference Data
Chapter 8		User Interface	Describes the User Interface presented by the Riposte Desktop applications
Chapter 9		Networking Services	Describes the mechanisms which support the Wide Area Network linking Outlets and other sites to the Campuses
Chapter 10		Platforms	Describes the various platforms used to support the Horizon services
Chapter 12		Systems Management	Describes the Tivoli facilities used to handle Software Distribution

Chapter 5 - Application Architecture

5.1 SCOPE

This Chapter discusses the *Application Architecture* that applies to applications within Horizon. These applications deliver the Pathway and PO Ltd business objectives.

Applications or application components are developed by:

- *Suppliers* who supply generic applications such as database products
- *Third parties* who supply applications or application components to meet Pathway requirements
- *Internal developers* who develop applications to meet specific business or strategy goals.

The key need is that any applications from any of these sources should be capable of integration with other applications, whatever their source.

[GENAPI] describes in detail how an application should be prepared for integration into the Horizon system.

5.2 HORIZON SERVICES

This sub-section describes the architecture of the services that are provided to Counter Clerks, and to PO Ltd and its Clients.

5.2.1 Application Structure Overview

All of these services are implemented as vertical stripes across the horizontal enabling layers. They are supported by discrete applications as shown for example in the diagram below (copied from Chapter 4). This Chapter shows how it is possible to add a new Counter application to the existing system by providing the relevant vertical components. It identifies these components, and defines the constraints that are imposed on their design and implementation.

Each vertical stripe is ideally totally independent of the others, and should have no inherent knowledge of the other's implementation. Where some form of integration or provision of service is required from another stripe, the mechanisms used vary between the layers.

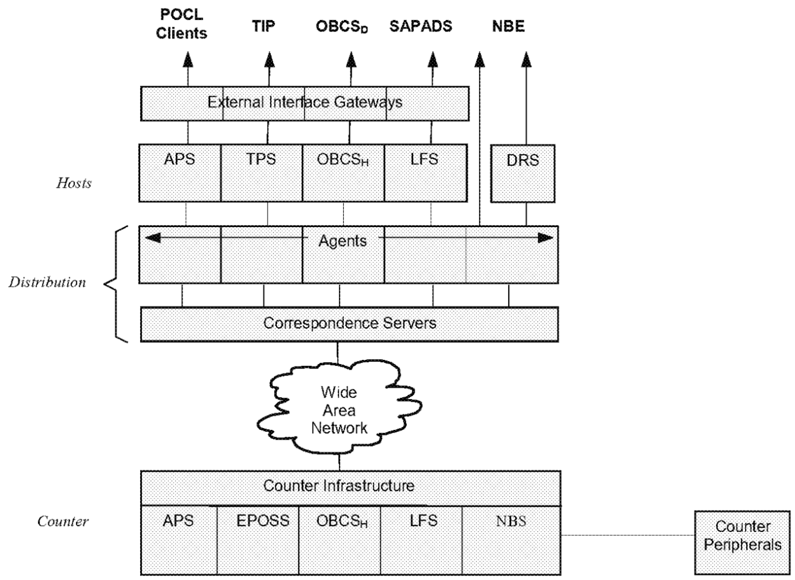

Figure 5.1 - Vertical Applications

As well as the major application components shown, applications should include some other components.

- Information about all transactions carried out at the Counter is passed to the PO Ltd TIP service by TPS, as well as to the relevant Client.
- Information about all transactions, and their service-related details, is also fed into the Data Warehouse.
- Counter applications may be responsible for the data flows to and from their Clients, but they may also be subject to, configured by or impacted by Reference Data passed via the RDMS. This may include data from PO Ltd, from the relevant Client, as well as Reference Data generated by Pathway.
- MIS facilities are needed to enable management to understand the behaviour of the application based upon information held in the Data Warehouse

This shows the overall application structure extended to include these components.

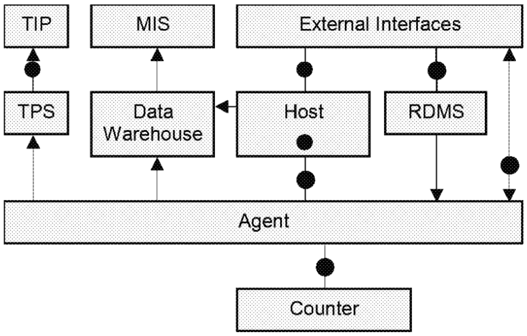

Figure 5.2 - Application Components

This diagram excludes infrastructure components such as the Correspondence Layer and Network. It indicates, by "blobs", the points at which ownership of data conceptually changes and hence at which audit information is generated.

In practice, each of these components can be quite complex. The following diagram illustrates all the potential components of an application that supports this structure.

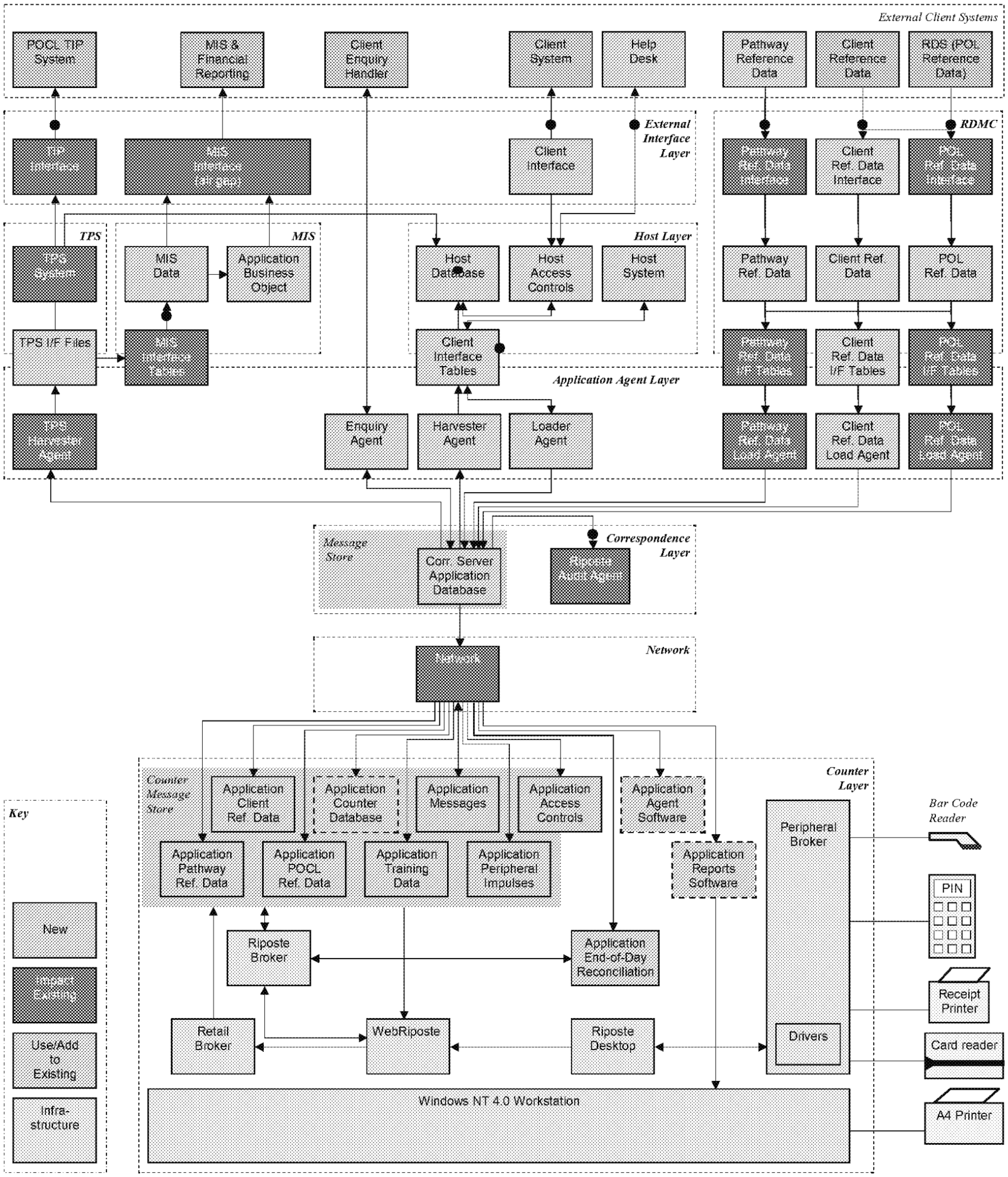

Figure 5.3 - Application Component Checklist

Shading is used in this diagram as follows.

- In most cases a new application requires a new instance of one of the components shown (*Create New*) – shown as Gold
- In some other cases, the application can use an existing component, or add to its functionality (*Impact Existing*) – shown as Turquoise
- In yet other cases, all that is necessary is to review the impact of adding the application to the size, performance or functionality of an existing component (*Use/Add to Existing*) – shown as Brown
- Infrastructure components available to all applications are shown in Tan, though here, too, it may be necessary to assess the impact of adding a new application.

The interfaces between each component are well defined, and determined by the position of the component in the overall architecture. For example, the interface between the Agent Layer and Counter Layer is the Riposte Message Service (RMS). This is described in more detail in Chapter 6 "Distributed Application Services". The interface between the Host System and the External Interface is usually the UNIX *Networked File System* (NFS).

The "blobs" in this Diagram indicate the points at which Audit information is gathered.

5.2.2 Counter Layer

5.2.2.1 General

The two main purposes of the *Counter layer* are as follows.

- To provide a user interface for the Counter Clerk to conduct transactions with the customer
- To record the result of those transactions and pass them back to the Host Layer.

5.2.2.1.1 Soft-Centred Applications

Riposte enables Counter applications to be developed in a flexible (or "soft") manner, where the application is configured from data stored within the RMS. Applications that use this mechanism are easy to modify in the future. New applications will use Reference Data where appropriate to define their structure, menus, persistent data and any other appropriate features.

⇨ EPOSS and APS make heavy use of this facility. Some older applications such as OBCS do not and hence are relatively less amenable to change

This should not be taken to extremes. Reference Data should not be used for what are in reality code functions, such as report structures. These should be distributed via Tivoli Software Distribution, as described in Chapter 12 "Systems Management".

5.2.2.2 Riposte Counter Infrastructure

Each Counter PC runs a set of independent user applications that sit "on top of" Riposte. These applications run within the Riposte environment on the Counter, shown here.

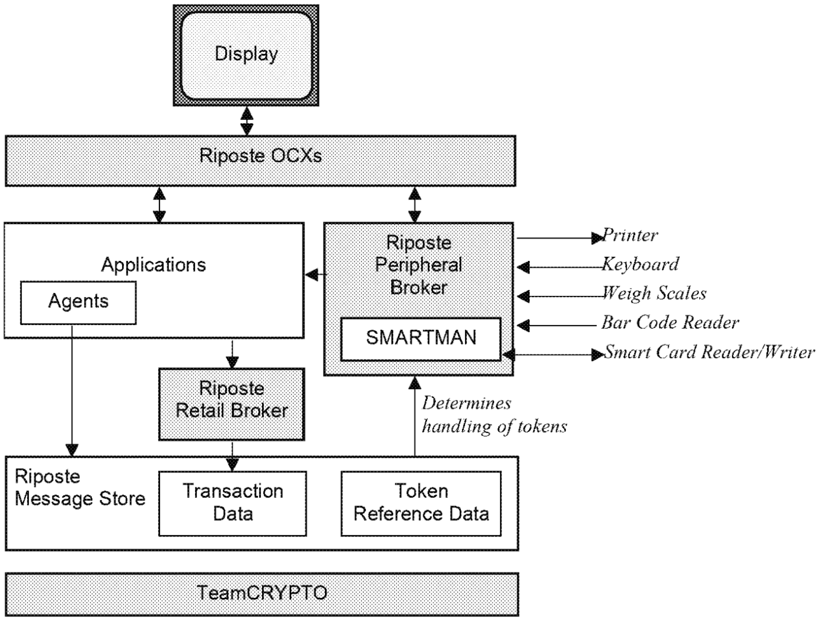

Figure 5.4 - Counter Applications Environment

5.2.2.2.1 Riposte Retail Broker

This co-ordinates the various applications in terms of a customer session, and adds contextual information to message (for example stock unit names). It provides APIs that an application may use to place items on the stack.

5.2.2.2.2 Riposte Peripheral Broker

This is described in Chapter 7 "Information Management". It provides the interface to all the peripherals apart from the display and back office printer. It supports the sharing of peripherals between Counter positions. The back office printer is driven conventionally using the normal Windows NT printing interface. It be shared by any of the Counter PCs using Windows printer sharing.

5.2.2.2.3 SMARTMAN

This is a plug-in component within Peripheral Manager that is specific to the handling of a particular type of Smart Card.

5.2.2.2.4 Riposte OCXs

A set of Riposte OCXs (ActiveX Control Modules) provides a consistent set of controls for interacting with the end user via the Display.

It is feasible to integrate existing counter-type applications with Riposte, as long as they are implemented as OCX modules and support a sensible API that can be invoked from Riposte modules

The end users are constrained to the above set of applications. They are not given access to "raw" Windows NT, and are therefore unable to run any other applications or services.

5.2.2.3 WebRiposte

WebRiposte is introduced into the Counter infrastructure at BI3, and provides an enhanced set of desktop support and message server facilities, in particular oriented towards the development of web-based Counter applications. Its structure is shown here.

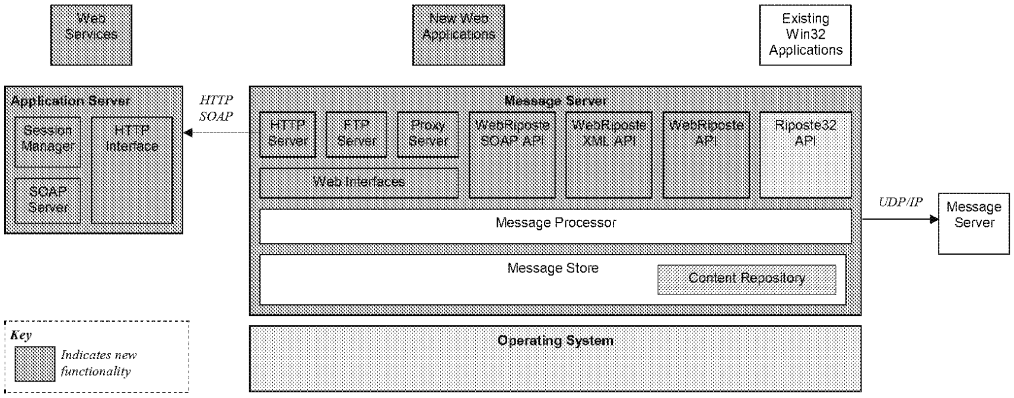

Figure 5 – Components of WebRiposte

It supports both "traditional" VB-based Counter applications, and (via the Financial Transactions Framework) applications whose structure is defined in XML. Note that Pathway has chosen not to exploit the Framework in BI3, and discussions with Escher are continuing with the objective of making the Framework more usable, and in particular to improve its choice of applications scripting language.

WebRiposte provides APIs for use by Web based applications, and Web Services to support web applications (for example by providing access to Reference Data).

5.2.2.3.1 WebRiposte Components

5.2.2.3.1.1 WebRiposte API

This provides support for Web applications.

5.2.2.3.1.2 WebRiposte XML API

This allows data to be transferred to and from Riposte as XML documents rather than as Attribute Grammar.

5.2.2.3.1.3 WebRiposte SOAP API

This supports the standard *Simple Object Access Protocol* (SOAP). Among other things, this allows access to *Common Object Model* (COM) objects from *Hyper Text Transfer Protocol* (HTTP) and XML.

5.2.2.3.1.4 HTTP Server

The HTTP Server runs within the Message Server and acts as a "proxy" for the calls from the Client Application to the various Riposte brokers. It supports the HTTP 1.1 protocol, and enables applications to use HTTP commands to invoke COM objects such as the Riposte Broker and Retail Broker APIs. Its primary function is to interpret *Uniform Resource Locators* (URLs) and satisfy them within the WebRiposte *Content Repository* (see below). Each URL should map onto a single WebRiposte Object. These WebRiposte Objects are predistributed, thus enabling executables to be pre-validated.

The HTTP Server can "pass on" non-local URLs to an appropriate web server. This is achieved by encapsulating the request and reply within Riposte messages that pass between the local message server and the Correspondence Server. A central Agent called the *HTTP Proxy*, conceptually running on the Correspondence Server, handles the communication with any other web servers.

⇨ This facility could be used to support access to YG-type forms

5.2.2.3.1.5 *Proxy Server*

This supports standard HTTP facilities to intercept URLs and map them onto a local *Content Repository*, held in the local Message Store. It may also be used in controlled conditions to obtain Web content from a third party server.

5.2.2.3.1.6 *FTP Server*

This supports standard *File Transfer Protocol* (FTP) facilities. It can be used by Client applications to store data in and/or retrieve data from the Message Store.

5.2.2.3.1.7 *Web Interfaces*

This provides support functions for the HTTP, FTP and Proxy Servers and maps their requirements onto the local Message Store

5.2.2.3.1.8 *Content Repository*

This consists of a set of WebRiposte Objects held within the local Message Store.

WebRiposte Objects are a new type of entity introduced by WebRiposte.

Like Persistent Objects, WebRiposte Objects are not automatically removed from the message store, but can be replaced by newer versions or they can be implicitly or explicitly removed. Unlike Persistent Objects, WebRiposte Objects can be contained within one another and so a hierarchy of such objects can be defined, similar to a hierarchy of folders and files within filestore.

5.2.2.3.2 Application Server and Web Services

These components provide services to Web applications in a way that constrains their access to the full set of HTTP constructs. Examples are XML-RPC or CGI requests from Web Browser Clients, which can be used to call COM application objects that have been defined to service requests of that type. These services can reside either within the local platform, or on a remote server.

5.2.2.3.2.1 *HTTP Interface*

This supports HTTP 1.1 commands and maps them on to the remainder of the Web Services set.

5.2.2.3.2.2 *Session Manager*

This is responsible for establishing the user session. It is of use only where WebRiposte is the only component of the Desktop. Horizon will continue to manage user sessions through the Riposte Desktop. Session Manager is also used to provide for the storage of data between stateless Web Services, and in this respect will be used by NBS.

5.2.2.3.2.3 *SOAP Server*

This supports a SOAP interface and enables Web applications to access information such as Reference Data.

5.2.2.3.3 The Framework

The Financial Transaction Framework is structured as shown here. Note that this may change as a result of ongoing discussions between Pathway and Escher, and designers should refer to the latest Framework definition from Escher before making any design assumptions about new applications.

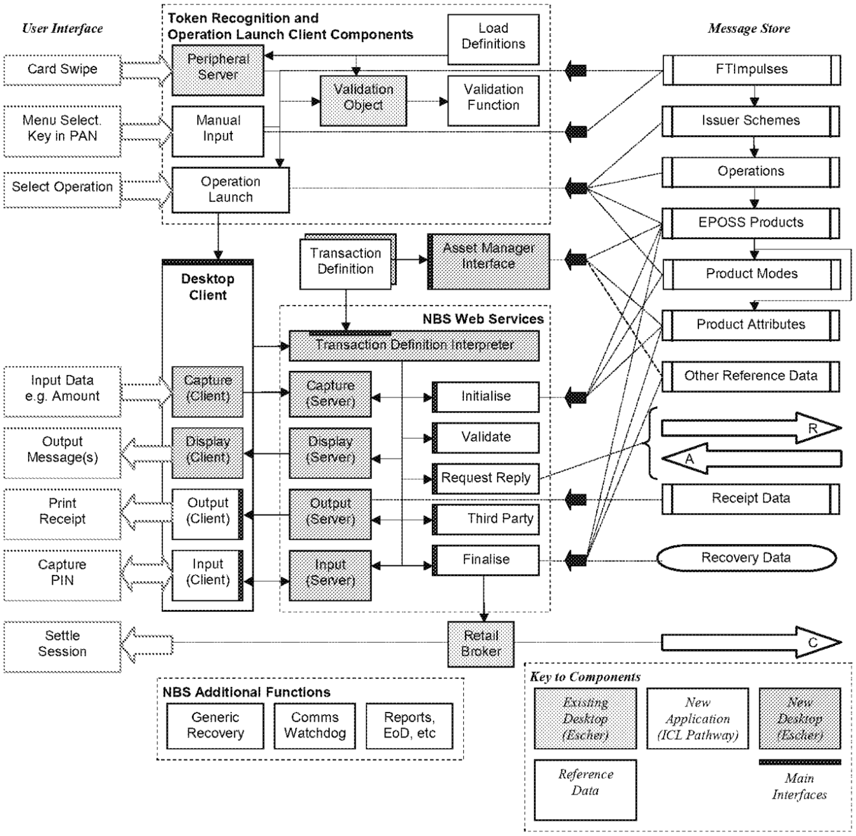

Figure 5.6 – Web Services Framework – Software components

The following sub-sections describe each component in turn.

5.2.2.3.3.1 *Token Recognition and Operation Launch*

This stage of the application is responsible for capturing data about a magnetic token that is used to initiate a transaction. The data can be captured either via a card swipe or manually. It establishes the identity of the token (e.g. its IIN), and uses Reference Data to relate this to the appropriate Issuer Scheme (i.e. FI) and the permitted Operations for that scheme. Finally, it is responsible for requesting the Clerk to select the required Operation.

5.2.2.3.3.2 Load Definitions

This component is used at Desktop initialisation to load from Reference Data the definitions of the tokens to be supported, for subsequent use by Peripheral Server and the Validation Object.

The Impulse definitions will be held as Temporal Persistent Objects (as opposed to Web Objects) in given Collection. Such Temporal Persistent Objects should be accessible in a Subscription Group.

5.2.2.3.4 Peripheral Server

This is the existing Peripheral Server functionality. It detects a token being presented at the Counter and reads the relevant data from it.

Impulses are generated when the Counter Clerk carries out some action using a Counter PC peripheral, such as swiping a card through a magnetic card reader. Data held in Reference Data indicates the action to be taken when each Impulse is received.

Peripheral Server reads the contents of Tracks 1 & 2 on a magnetic swipe card. These contents are passed to a *Validation Object* that determines (for example from the IIN) which application is to process the impulse.

Peripheral Server will be pre-configured with details of expected tokens, and will match the token that has been presented against these expected impulses using the *Validation Object*. Details of these impulses will be passed to Peripheral Server by the *Load Definitions* component on desktop initialisation.

In particular, the Impulse definition will describe the exact layout of the data being read and the mapping of this onto logical fields that can be used by the application.

5.2.2.3.5 Validation Object

The standard Riposte Desktop includes a *Validation Object* that supports a general-purpose validation facility for token impulse checking, together with the concept of user-defined *Validation Functions* that can be invoked from the Validation Object as COM objects. The Counter Application would use the basic validation matching criteria, and also provide an application specific *Validation Functions* to be invoked as part of the analysis of each token.

5.2.2.3.6 Validation Function

This validation function will handle the initial validation of the token, and provide any necessary differentiation between the use of the same token by different applications.

⇨ For example, this function would distinguish between a bank card used by NBS and by DCS, depending on the point in the customer session at which it was swiped.

If the validation function successfully matches a token against a defined impulse definition, then Peripheral Server will invoke the appropriate application (as defined in the Impulse definition), which in this case will be the *Operation Launch* application. It will then pass it the Impulse definition filled out with details of the impulse. This Impulse definition will also identify the "Issuer Scheme" associated with the token.

A *Magnetic Card Token Validation Function* will be developed by Pathway using existing standard Riposte interfaces.

5.2.2.3.6.1 Manual Input

Should the token fail to be read, or if the token peripheral is out of action, then an alternative of manual entry may be required.

This component represents the dialogue required to capture token information manually.

This will be done by displaying a dialogue to capture the token identity, and then passing this as an impulse to the Validation Object. This allows reuse of the logic to be used for a swiped input to identify the Issuer Scheme (as described above).

Having done this, Reference Data can be used to identify whether or not manual entry is supported for this token, and if so, what additional data is to be captured. If it is supported, an appropriate script is launched to request this information from the Counter Clerk. If manual entry is not supported for the token, then the Counter Clerk will be informed and the transaction ended.

Having assembled the equivalent of the swiped information, an Impulse can then be constructed and passed to the *Operation Launch* component as if it had come directly from a card (but with an additional attribute identifying the impulse as being "manually input").

5.2.2.3.6.2 Operation Launch

This component receives details of the token (either from a swipe or manual input as described above) and the identity of the Issuer Scheme as identified by the *Validation Object* (using the NBS specific *Validation Function*).

It then uses Reference Data to navigate to the Operations associated with the Issuer Scheme, and for each such operation checks to see if it is currently allowed.

There are two classes of checks.

- *Global Checks*. These are primarily to do with whether or not NBS is currently available in the Outlet, i.e. whether the Counter is likely to be successful in communicating with the Campus. The requirement is for the ability to invoke a function to carry out such detailed checks.
- *Per operation Checks*. These are required on each configured Operation to decide whether or not it should be presented at this time. Examples are:
  - The *EPOSSProduct* associated with the Operation is currently available for sale in this Outlet
  - The Operation is currently available in the current transaction mode
  - That the operation is allowed for the current Method of Entry (i.e. swiped or manual)
  - That the operation is allowed in the local configuration

From the above checks, a number of Operations will be identified as appropriate to the Token. These are presented to the Counter Clerk to select, and the identifier of the selected Operation is passed to the Counter application.

Note that if there are no suitable operations, then the Clerk needs to be informed of this.

5.2.2.4 Counter Application Structure

5.2.2.4.1 Scope

Ideally, the only business rules that are implemented within the Counter application components are those that control the user interface. Any other rules, for example, that perform data manipulation should be carried out elsewhere, normally within the Host Layer.

In practice, the split of application processing between Host, Agent and Counter layers can be more complex and should be determined by a number of factors including the following.

- Some business rules logically need to be carried out on the Counter
- Some business rules are already implemented in third-party applications and so their position is determined by the position of that third party code
- It may be sensible to provide immediate feedback in response to certain situations, and this is best done at the Counter
- Opening the communications link to the Campus costs money and leads to response time delays so is best avoided.

These constraints apply regardless of the mode of application development ("traditional" VB or web-based).

5.2.2.4.2 Data Management

To perform a particular function the Counter application may need to refer to existing information held within the desktop machine. This information is always held within Riposte.

It can take the form of standing (or reference) data, which is constant for some time. Riposte provides a feature called Persistent Objects specifically to handle long term information requirements. Examples include: the price of a first class stamp; the value of postal orders; or the cost of Driver and Vehicle Licensing Agency (DVLA) licences for different classes of vehicles. However, in general these facilities are used to pass long-term data from PO Ltd to the Counters. They should not be used by Counter applications to store data for their own internal use, as this is replicated to the Outlets and can have a major impact on the size of the Correspondence Server message stores. Alternative facilities exist to generate "Local Persistent Objects" that are *not* replicated to the Campuses.

Applications can call on a Riposte API that returns the value of any particular instance of Reference Data.

It can also take the form of data that is specific to a particular Client and is used to validate or otherwise control the behaviour of the transaction for that specific Client over a more limited period. This class of data is also held within Riposte messages, but not as Persistent Objects.

⇨ An example of this is the use of Stop Lists by OBCS.

5.2.2.4.3 Transaction Sessions

Normal transactions at the Counter take place within a customer session. Each physical transaction with the customer (e.g., stamp sale, benefit book encashment, postal order sale) results in the creation of one or more messages depending on the complexity of the transaction. For example, a stamp sale has one message, and a postal order results in two messages (one for the fee). None of these messages is normally written to the message store until the customer "settles" the session. This results in an additional transaction for each *Method of Payment* (MoP) used.

Applications must themselves determine the point at which a transaction is "settled", based on their own business rules. However, once a transaction is settled it cannot be cancelled. It may be reversed (i.e. create a new and opposite transaction) if that is permitted by the business rules.

Each message written contains either a credit or a debit. The total session (and the sum of all the credits and debits) has a net value of zero.

5.2.2.4.4 Distributed Application Services

The vertical stripes that represent the applications should have no inherent knowledge of each other's implementation. They do not need to interfere with each other's operation. This applies at all levels. However, at each level there may be a need for specific inter-application communication. At the Counter level, there is a need for visible integration between the various application components so that the user is presented with a seamless and consistent interface.

This integration is achieved in two ways.

- By Riposte which provides a consistent integrated Desktop, transaction manager and peripheral manager
- By use of a consistent object model within the transactions. This is the same as the early strategies that caused integrated database systems to be developed in the early 1970s. They hit problems because of schema management. Riposte uses attribute grammar to overcome that problem.

There are no direct calls between the application components.

5.2.2.4.5 Independent Working

A fundamental feature of the architecture is the ability of the Desktop applications to normally work independently of any connection to the Campus. This is essential to reduce the load on the Campus systems, which would otherwise be unable to cope with the load, and as a resilience feature should the communications facilities fail. In addition, it minimises the need for the Host systems to run 24 hours a day.

Information flows to and from the centre are normally batches of Riposte messages that are transmitted asynchronously from the original transactions that generated them.

However, there are a number of application areas where a Counter application requires on-line information from another system, or a Host requires confirmation that data has reached the Counter.

5.2.2.4.5.1 Direct Counter Communication with Another System

This other system may be part of the Central Systems or may belong to an external body that is either part of PO Ltd or one of their Clients. There are several cases of this, including the following.

⇨ OBCS needs to refer to the Campus whenever an Order Book is presented at an Outlet by a person for whom no record is held locally. If the line is down, the Counter Clerk looks it up on paper.

⇨ NBS needs to refer to the Network Banking Engine (NBE) whenever a customer wishes to carry out a Network Banking transaction.

⇨ DCS needs to get authorisation from the Campus whenever debit card is used a Method of Payment. The Campus, in turn, requests authorisation from the Merchant Acquirer. If the telephone line to the Campus is down, the transaction is Declined

These applications all operate in a similar way, using the standard Outlet communication links and an appropriate Enquiry Agent. The application generates a Priority Message or Real Time Message, that causes a connection to the Campus to be made immediately if needed. The application captures its Message ID. It then creates a message port waiting for a response to the enquiry or update. This response will be keyed on the Message ID of the enquiry or update. The message port should be set to time out after a configurable interval defined in a Persistent Object.

Once the link to the Campus is open, the message is then sent. In the case of a Priority message, it is preceded by all others that have been waiting to be transmitted. The line is kept open until a response is received, or the message times out. The response has the ability to say "keep the line open for at least another zero seconds", thus allowing it to be closed as soon as the reply is received

An Enquiry agent running at the Campus will listen for enquiries or update messages, and will process them as they arrive. The reply (or time-out information) is returned to the Counter Application. The Counter Application receives the response and processes the information within it accordingly. Alternatively the message port will time-out, in which case the application behaves according to rules defined within its requirement.

5.2.2.4.5.2 *Direct Host Communication with Counter*

In certain circumstances, an application may need confirmation that a message has reached the Counter. A similar mechanism is used. A Priority Message is generated by the Application Agent, and passed to the Counter. A Counter Agent (see below) must respond to it with another Priority Message that is passed straight back to the Host via an Interactive Agent.

This mechanism is used to generate *Acknowledgements* for SLA Calculation purposes.

5.2.2.4.6 Modes

The Riposte Desktop supports the concept of *Modes*. An example of a mode is "Serve Customer" or "Transfer Stock In". Modes are selected by the Counter applications as they see fit, using APIs and Persistent Objects exposed by Riposte. The current Mode is indicated at the bottom of the Desktop screen.

It is possible to prevent certain functions being used in particular modes. This results in the associated Menu Button for the function being disabled. An example is that Logout is prevented by the Serve Customer Mode. The user has to settle the current session before he or she can log out.

5.2.2.5 Counter Application Components

Each Counter application may include an instance of the following.

5.2.2.5.1 Application Database

This comprises the Persistent Objects and WebRiposte Objects used by the Application. Each Collection (see Chapter 7 “Information Management”) must be owned by a specific application, and the application must ensure that it uniquely identifies the contents of its own Collection.

> *There are no mechanisms in place to enforce this, or to police the choice of Collection names by applications. Note that some applications have several different “applications” within them, each with its own Collections.*

The major purpose of this Database is to exploit the affinity between customers and Outlets. Members of the public who are customers of PO Ltd tend to use only a small number of Outlets (most commonly only one, their local Post Office) and only change when they move house or jobs.

Applications can exploit this by distributing, in advance, relevant information about those customers from the Host to the Outlets that they visit. This distribution is virtually free as it can happen at low priority and at the same time as other information is flowing to the Outlet.

This technique avoids an on-line connection being made for every instance of certain classes of transaction, but at the cost of using up additional disc space at the Counters. It reduces the mean response time for the transaction class. It can be used by any application that has a need to make a connection between customers and the Outlets that they use. The application's design should identify the impact on the Counter disk storage, and the impact on the Outlet ISDN connection rate, and make an appropriate tradeoff. (The application should never make the assumption that customers will *only* use the same set of Outlets as they have done previously. This is an optimisation, not a design principle.)

⇨ OBCS uses this mechanism for distributing benefit book information. On the first use of a book at an Outlet, an on-line connection is made to determine the validity of the book. This is remembered by the system and any future updates to that book (such as stops) are transmitted to all Outlets at which the book has previously been used.

5.2.2.5.2 Counter Reference Data

Counter Applications must use Reference Data wherever practical to define their function and for long-term data storage. As discussed below, Reference Data variants may exist for:

- Pathway (used to configure the applications)
- Client
- PO Ltd

Separate Collections are defined for each of these that an application needs. The use of Collections in this way establishes boundaries between the Reference Data used by different applications.

5.2.2.5.3 Application Messages

All communication between the Counter and the Agent Layer is carried out using Riposte messages. In addition, the RMS provides a “working area” which applications can use by generating, and then re-reading, transient messages. The nature and structure of Riposte

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

messages are described in Chapter 7 “Information Management”. The RMS includes messages belonging to each application within Riposte. Each application must define the structure and Attribute Grammar of the messages it needs, and ensure that these do not conflict with any other messages belonging to other applications.

5.2.2.5.4 Application Training Data

Each application must make provision for training Counter staff. As described in Chapter 14 “Usability”, this is done via a Training Database, which must be populated with new data appropriate to the new application.

> *Previous applications have populated this Training Database directly. This is not acceptable. The Training Database data for a new application must be populated via the Reference Data Management System.*

5.2.2.5.5 Application Peripheral Impulses

Impulses are generated when the Counter Clerk carries out some action using a Counter PC peripheral, such as swiping a card through a magnetic card reader or placing an item on the weigh scales. Some Impulses are associated with particular applications and invoke those applications directly (for example swiping a magnetic card will invoke the application to handle the particular type of card, as defined by the first six digits of its PAN). Some Impulses may be of interest to a number of different applications, and are processed by whichever is current at the time.

In general, the rules for determining which application handles any particular Impulse are defined by Reference Data.

A particular instance of Impulse processing is the use of the Touch Screen to select a Menu item. There is a complex hierarchy of Menus and sub-menus, and each is associated with a particular application. Applications need to give careful attention to their position within the hierarchy. They need to know whether this position applies to all Outlets, or to a subset of them. This is discussed in Chapter 8 “User Interface”.

5.2.2.5.6 Application Access Controls

Part of the data held within Riposte Reference Data defines the mappings from Buttons or Impulses to Applications and to Counter users. It also determines which component of the Application handles the Button or Impulse. Not all applications (and their associated Buttons and Impulses) are available to all Outlet users. Some are reserved to the Post Office Manager and others to Auditor Roles. The *Access Controls* must be defined and set up as part of the application design. They include the user-to-application privileges associated with Counter Clerks, Post Office Managers, Auditors and so on. New applications need to define their own controls.

> *There are no facilities in Riposte at present to control access to Impulses.*

Applications must always check their Access Control values. User data may be incomplete or corrupt.

In addition, some messages (or parts of messages) need to be signed. The Access Controls define which these are, and also allow the application to verify the signature on signed messages that it receives.

5.2.2.5.7 Application Software

This implements the Counter logic of the application. Use of the Counter peripherals must conform to the Pathway Counters Style Guide (see [STYLE]). This defines the ways in which Buttons, menus and other screen and keyboard components are used.

Applications drive peripherals via the Riposte Peripheral Broker, the screen via Riposte OCXs, and the Riposte Message Store via the Retail Broker.

5.2.2.5.8 Application Agent Software

Agents at the Counter are used to provide a measure of flow control. They run in the Gateway PC, and thus the application developer can guarantee that there is only one instance of an Agent running within an Outlet at one time. Any task which must be single streamed is invoked by the application writing a Riposte message which is picked up and executed by an Agent.

Any new application must consider whether it needs to provide any Counter Agents. Examples of the functions that they can carry out include the following.

- Sometimes messages arrive at the wrong place. A generic Redirector Agent can recognise this and send them on to the new Outlet
- Maintenance of the Application Database, or of the Persistent Objects which it contains
- Tidying up the Counter Database

5.2.2.5.9 Application Reports Software

If the application has the ability to generate reports, such as records of transactions that it has handled, then new code is required to implement this and to define the structure of the reports.

Report layouts are held as part of a single Windows NT file that is included in standard Counter PC Builds. It is indexed by an *ObjectName* attribute in the Report's Reference Data.

5.2.2.5.10 Application End of Day Software

Applications must take account of the fact that they may need to handle End of Day activities such as cash control. If so, they need to provide close-of-day procedures. A generic Counter Scheduler is provided, driven by Reference Data that determines the processes to be invoked at predetermined events such as End of Day.

The operation here is driven by the requirement that data is not sent to TIP unless the Outlet involved has closed for the day. This is indicated by the arrival of an *End of* Day (EoD) marker for that Outlet. A Generic Harvester reads these EoD markers. For each one that it receives, it updates a Persistent Object in a Virtual Group that is used to delineate which Outlets may be harvested for the day.

All other Harvesters only harvest messages from Outlets that are recorded within the Virtual Group.

The EoD marker is written to the mainstream message store, rather than to the "active" message store (which may be the training one).

5.2.2.6 Generic Application Functions

As well as the applications that support the vertical services, each Outlet also contains various "local management" processes that interface with the vertical services. These processes are invoked from the Riposte Desktop. They revolve around the administration, balancing and reconciliation of the "sales" activity. They are conceptually provided as part of the EPOSS application, but have a wider significance.

5.2.2.6.1 Stock Units

There are functions that manage stock: movement of stock into or out of the Outlet (remittance), and transfer of stock between stock-units. This all has to be tracked to enable subsequent balancing and auditing. There are also a significant number of local reports to be produced.

Within an Outlet, there will normally be a number of stock units. These are allocated by the Post Office Manager, on a medium term basis, to individual Counter Clerks. The Counter Clerk is then responsible for ensuring that the stock unit balances at the end of the Cash Account Period, or whenever the stock-unit is de-allocated from him.

The Outlet, itself, also balances all current stock at the end of the *Cash Account Period* (CAP). The Outlet stock is the sum of all the stock units at the point that they individually rolled over into the next CAP.

From these transactions, the current position can be deduced by working forward from the previous balance position. At the end of each Cash Account Period, after a balance has been achieved for each stock unit, a virtual "line" is drawn across the Riposte journal for each stock unit. A set of messages is stored that represent a clean start with the brought forward balances.

All the information to support these applications is stored within Riposte as transactions that caused the status quo to change.

There are recovery issues with single Counter Outlets if the Counter PC fails and is physically replaced before it has replicated to the Correspondence Server. The end of day process may have to be re-run after the machine is repaired.

There are further issues with regard to Outlets that are closed temporarily. The Riposte messages that represent its stock units will be expunged at the end of their expiry periods, unles they are periodically refreshed.

5.2.2.6.2 Session Mobility

Session Mobility is a feature of the Riposte Desktop that allows a Counter Clerk to logon to a different Counter, resulting in the transfer of the current Customer Session to that new Counter and the automatic logout on the original Counter. The ability to swap between two sessions on a single desktop is also closely related to this.

However, there are circumstances under which it is undesirable to transfer or swap a session, and so the Riposte Desktop also provides facilities to inhibit Session Mobility.

⇨ For example, it is necessary to inhibit Session Mobility in an NBS transaction between the sending of the [R] message and receipt of the [A] message, since otherwise there is a danger that the [A] will be missed whilst the session is transferring.

5.2.2.7 Session Timeout

Another feature of the standard Riposte Desktop is that of Session Timeout. There are two aspects to this:

- *Counter Locked.* If a terminal is inactive for more than a given period (configured to 15 minutes for Horizon), the Counter is locked. In order to unlock the Counter, the Counter Clerk is required to re-input his or her password before being able to continue. Alternatively, a manager can force a logout at that point (for example if the Counter Clerk has gone home having forgotten to logout). Such a forced logout will be handled as described below.
- *Forced Counter Logout.* If a Counter is inactive for a longer period (configured to 60 minutes for Horizon), it is automatically logged out. Such a forced logout is reported by the Riposte Desktop to any applications running under its control, thus enabling them to tidy up. In particular, EPOSS will automatically commit any outstanding Customer Session to the stack with a transaction assuming it to be settled for cash.

However, the mechanism used to implement session timeouts is only active when session mobility is active. This means that if session mobility is inhibited by a particular application, then this has the side effect of inhibiting Session Timeout.

5.2.2.7.1 Counter Recovery Application

There are transaction types for which, once an initial action has taken place, it is important that a full transaction history is written to the message store.

⇨ An example is NBS, where during normal operation every Transaction will have both an [R] and a [C] (most will also have an [A]).

If the Counter is switched off or fails at any stage during the processing of the transaction, part of the transaction record (including its eventual outcome) will be missing from the message store. The application thus needs to provide a *Message Recovery* component that can examine the message store, and where there is any doubt ask the Counter Clerk for the outcome of any indeterminate transaction.

These cases can be determined as the Message Store will not contain a logout at the end of the Clerk session. This can be detected when the Clerk next logs on to the Counter.

5.2.2.7.2 Counter Call Scheduler (CCS)

This is an Agent that runs on the Gateway PC and has responsibility for managing Riposte connections to the Campus Correspondence Server at regular intervals, depending on the number and size of waiting Riposte messages. Any priority message forces Riposte to make an immediate connection. Initiating a Riposte connection will result in an underlying network connection being made with the Campus, and consequently a dial up connection in the case of ISDN connection Outlets.

5.2.2.7.3 EPOSS Watchdog

The EPOSS Watchdog is a Desktop application that monitors connectivity of a Counter and in the event of a problem alerts the Clerk. It ensures that critical activities are not carried out in an “unsafe” environment.

This component maintains a *Network Status Indicator* on the desktop, which provides a visual indication to the Clerk as to whether or not the Network is currently available. The

Network Status Indicator will be set to show that the Network is unavailable in any of the following circumstances:

- The Counter is a slave Counter and is unable to communicate with the Gateway PC
- The on-line service Persistent Object indicates that the network is unavailable.

5.2.3 Network

There are no application components *per se* at the network layer. However, the introduction of a new application may well increase or modify the network traffic, and may change the traffic profile. Hence, it is essential that the data traffic is assessed in the application design, in good time for the cost of any network enhancements to be included in the Business Case for the application. Chapter 15 "Performance" indicates the types of calculation required.

5.2.4 Correspondence Layer

Applications *per se* do not include a component at the *Correspondence Layer*, though some application Agent functions run at this layer for performance reasons. It is important for applications to understand the architecture of this layer, and the services that it provides to the Agent layer.

5.2.4.1 Correspondence Server Application Database

The Correspondence Layer and Counter Layer share the use of the Riposte Message Server (RMS). This supports a shared, distributed message store to ensure that information generated at the Counter PC is replicated in the Campuses and vice versa. These Riposte mechanisms interact directly with the Agent Layer. As shown in the diagrams above, Agents invoke the RMS by an RPC interface. This is used to transmit messages to the Counter PC, or to listen for and read messages transmitted by the Counter PC. Riposte ensures that these messages are transmitted to their destinations with integrity and in a secure and resilient manner.

Messages are formatted in an extensible style known as "Attribute Grammar", which is described in more detail in Chapter 7 "Information Management". Each new application must define the Attribute Grammar constructs that it requires, and ensure that these do not conflict with the needs of other applications. There is a manually managed "data dictionary" which helps in this.

5.2.4.2 Correspondence Server Application Agents

Some Agent code runs, for performance reasons, in the Correspondence Servers. The only example at BI3 is the TMSDistrib Agent

Applications wishing to locate Agent processes on the Correspondence Server must gain the agreement of the Chief Architect.

Correspondence Server Agents are supported by the same set of libraries as Agents (see Figure 5.15 above), though they do not invoke the Oracle Client. The Multi-Riposte library provides a Redirector function that ensures that messages go to the appropriate Cluster. This may not be the Cluster within which the calling Correspondence Server is located.

5.2.4.3 Riposte Archiver

The RMS constitutes a point at which ownership of data changes from Client to Pathway, or vice versa, and hence transfers across this boundary need to be recorded for audit purposes. A specialised Riposte Archive Agent, running on one of the Correspondence Servers in each Cluster, listens on a dedicated Riposte Real-Time Message Port and receives each message written to the RMS. It writes this to serial files. At intervals, it closes the current file and passes it to the Archive Service to be written to bulk storage media. Each time it closes a file it generates a Riposte Checkpoint.

5.2.5 Agent Layer

5.2.5.1 Purpose

A new application is likely to need to provide new *Agent* components.

The *Agent Layer* is responsible for transforming the message-based view that is appropriate for the Counter application into a file (or set) view of the Host Layer. It provides facilities to pass data in both directions: from the Host layer to the Counter, and vice versa. It also provides facilities to pass messages direct to third party Clients, and to return the Client response to the Counter.

5.2.5.1.1 Host-Based Agents

It creates Riposte messages from one or more records placed into the Client Interface Table*s* by the Host Layer. It also transforms Riposte messages from the Desktop into records in the Client Interface table. An Agent behaves as a client to both the Host Layer and the Distribution layer. It "pulls" data from one and "pushes" it to the other.

Two transformations are required:

- Records held within the Host Layer tend to be normalised, particularly if they are held in a database. A message to or from the Counter needs to contain all the information for a single transaction at the Desktop. This will typically contain unnormalised information (e.g. pick lists). The normalisation or de-normalisation process is carried out by the Agent.
- Conversion between the flat record structure of the Host Layer and the attribute grammar that is appropriate for Riposte and the Counter application.

Agent processing takes place either in bulk or on individual messages. Different approaches are required for each of these. Whichever type is used, the Agent is unique to the application and does not interact with other applications' Agents or provide any services to other applications. (There are some common services used by all Agents.)

For some classes of messages, the Agent has to digitally sign each message (or part of the message), by adding an extra attribute that contains the signature, or to check a received signed message. This is defined by the business rules for the application.

There may be cases where two (or more Agents) require access to the same set of transactions within Riposte. Subjectively, from a performance perspective it may seem attractive to retrieve them only once. However, this contravenes the principal of Vertical Application separation, and must be avoided.

It is permissible for data to be harvested twice within the same application.

All Agents must be designed with an *Application Interface Specification* (AIS) which defines the nature of their interfaces.

5.2.5.1.2 Other Agents

These operate at the *message level,* passing individual Riposte messages from the Counter to the third party and returning the response to the Counter.

5.2.5.2 Types of Agent

There are five principal classes of Agent:

- Host to Counter - bulk
- Host to Counter - interactive
- Counter to Host - bulk
- Counter to Host - interactive
- Enquiry Agents (interactive)

A new application may require instances of any or all of these.

5.2.5.2.1 Loader Agents vs. Harvester Agents

Agents that pass data from the Host Layer to the Counter Layer are called Loader Agents. Those that pass data from the Counter to the Host are called Harvester Agents. A particular application may include one or more of each type of Agent. Agents that are invoked by a Counter application, and acquire and pass back data to that application, are called Enquiry Agents. They may communicate via a Host, or direct to the third party Client.

Some hybrid Agents operate as both Loaders and Harvesters.

5.2.5.2.2 Bulk Agents vs. Interactive Agents

Bulk Agents operate on all messages of a particular type already held within Riposte. *Interactive Agents* react to the appearance of a particular message type.

5.2.5.2.3 Generic Agents

The TPS Harvester Agent, harvests *all* transactions for input to TIP and the Data Warehouse.

This could be impacted by the development of a new application if that application added a new attribute to the relevant message types.

A specialised Riposte Archiver, running on the Correspondence Servers, is used to ensure that all Riposte messages are written to tape for audit purposes.

5.2.5.3 Loader Agents

5.2.5.3.1 Interactive Loader Agents

The overall architecture for these depends on the capabilities of the Host application, and its infrastructure.

Where the Host supports RPC or an equivalent interface such as Sockets, it makes a direct call to the Agent as shown here. Note that in these diagrams, data transfers are shown by broken arrows. Calls are indicated by continuous arrows.

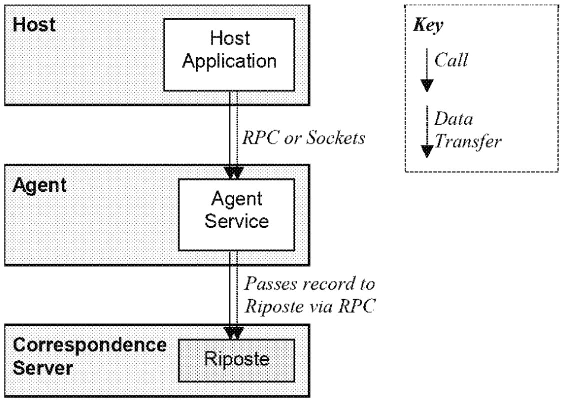

Figure 5.7 - RPC Driven Loader Agents

Where the Host application is implemented on an Oracle database, and the triggering event is the application writing a record to the database, a different mechanism is used. This is shown here.

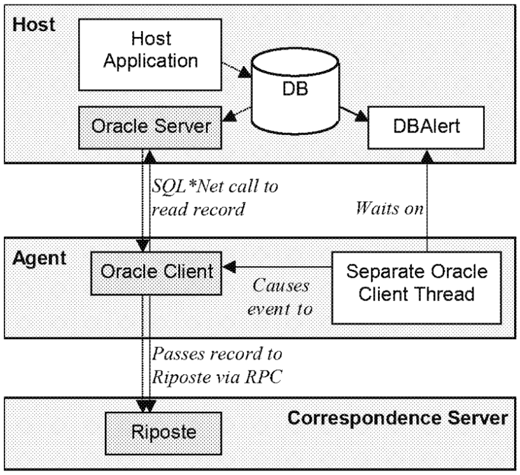

Figure 5.8 - Oracle Driven Interactive Loader Agents

The Oracle DBAlert daemon is associated with a particular Table in the Host application's database, and is invoked when the application writes a record to that Table. A separate Oracle Client thread in the Agent waits on this DBAlert. When it receives one, it causes an Event to the Oracle Client, in a separate thread. This causes the client to read the record from the Oracle Server. The Interactive Agent thus calls the Oracle SQL client to read the record, and then process it as required, including passing it to the RMS using the Riposte *Application Programming Interface* (API) over RPC.

Alerts may be "lost" occasionally. To ensure that it doesn't miss any records, the Oracle Client also reads the table on a timed basis.

5.2.5.3.2 Bulk Loader Agents

The structure of these depends on the complexity of the Host application, and whether or not it uses an Oracle database.

5.2.5.3.2.1 Oracle Based Bulk Loader Agents

In the case of simple Oracle based Host applications, the structure is the same as for Interactive loaders, and is shown in Figure 5.7. The Host passes one or more records via RPC or an equivalent interface such as Sockets to the Agent, which passes them to the RMS by RPC.

This is the structure of a Bulk Loader Agent where the Host uses an Oracle database. The Reference Data loader, discussed below, is an instance.

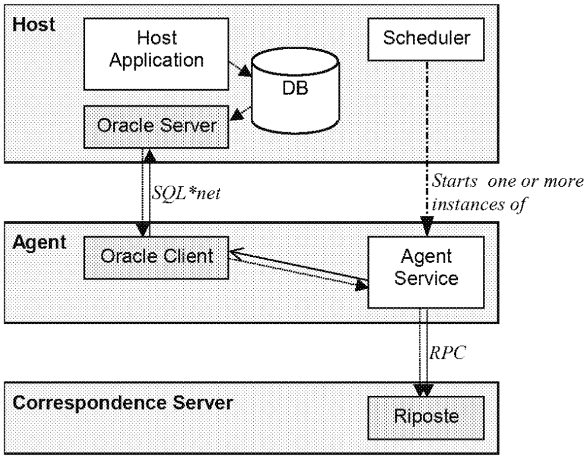

Figure 5.9 - Structure of a Bulk Loader Agent for an Oracle Host

The Host System sets up in its Client Interface Table the records to be loaded. When this is complete, a scheduling process is invoked to start a number of Agents in parallel. Each is given a defined set of “work chunks”, defined by data held in the Client Interface Table. Each Agent starts up, and selects and processes one of these work chunks. After each, it checks to see if there are any further work chunks to select. If so it processes them, if not it exits.

Bulk Agents run continuously. Maestro starts and reschedule them as required, and restarts them if they fail.

Work chunks are designed to take a similar amount of processing. Each will usually involve reading a series of *fetch units* from the Client Interface Tables in the Oracle database (using the Oracle Client-server interface), and updating the Correspondence Server’s RMS journal. Progress with processing Oracle records may be managed either by marking individual (or groups) of rows as “processed” in the Client Interface Tables, or by maintaining a “progress marker” in separate control tables depending upon the performance requirements. Such progress information needs to be updated prior to issuing a *Commit*. Any Riposte transactions must also be completed before a *Commit* to Oracle. There is no need to co-ordinate Oracle *Commits* with fetch units, and it may be appropriate to *Commit* during a fetch unit (for example when the Outlet changes). The maximum size of the fetch unit will depend on the optimum number of records that can be retrieved in an SQL*Net call, and the associated memory available in the Agent server. These parameters, and other features of the interface, must be defined in the application’s AIS. Work chunks are also used to enable another Agent to recover the work being processed at the time an Agent fails.

When all Agents have completed, a check process is run to ensure that all work is finished. This means that all the records in the Client Interface Table have been successfully input into the RMS.

5.2.5.3.2.2 *Flat File Based Bulk Loader Agents*

Where the Host application handles Flat Files, these are passed to the Agent, which then reads records from them serially and passes them by RPC call to Riposte. The Agent may also generate Checkpoints, for example after every file, to aid its recovery. Agent recovery should be linked to Host database recovery, for example by the Host holding the checkpoint name in the database.

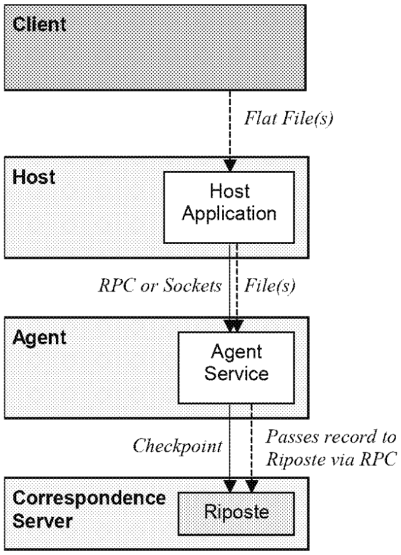

Figure 5.10 - Flat File Loader Agents

5.2.5.4 Harvester Agents

5.2.5.4.1 Interactive Harvester Agents

The structure of these depends on whether the Host Application uses an Oracle Database.

5.2.5.4.1.1 *Oracle Based Interactive Harvesters*

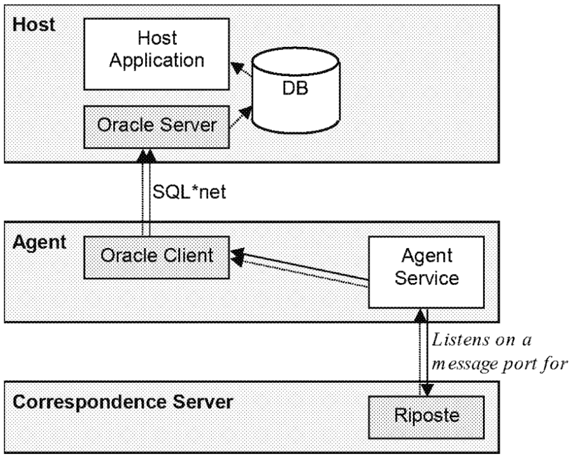

Figure 5.11 - Structure of an Interactive Harvester Agent

This harvester runs at designated times during the working day, listening for the arrival of Riposte messages of the type that it is designed to harvest. When such a message arrives it is processed and the results are written to the Oracle database's Client Interface Table by a direct call on the Oracle Client.

5.2.5.4.1.2 *Non Oracle Interactive Harvester*

Where the Host supports RPC or an equivalent interface such as Sockets, the Agent makes direct calls to it.

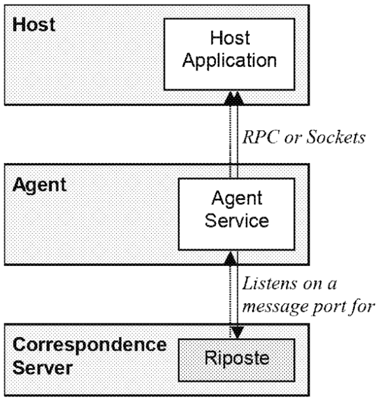

Figure 5.12 - Non-Oracle Interactive Harvester Agents

Normally only one instance of an Interactive Harvester Agent can run at once within a Cluster, otherwise duplicate processing can occur. However, as Clusters are essentially discrete message stores, it is usual to run one Harvester per Cluster for improved throughput.

5.2.5.4.2 Bulk Harvester Agents

The structure of these is similar to the equivalent type of Interactive Harvester Agent. The difference is that records to be harvested build up in the RMS journal on the Correspondence Server, rather than being harvested as soon as they appear. At an appropriate time, the scheduler starts up one or more harvesters to harvest the records from RMS. The Agent obtains the messages by reading serially through the RMS message store rather than by waiting on a message port.

5.2.5.4.2.1 *Oracle Based Bulk Harvesters*

This is the structure for Oracle-based Bulk Harvester Agents.

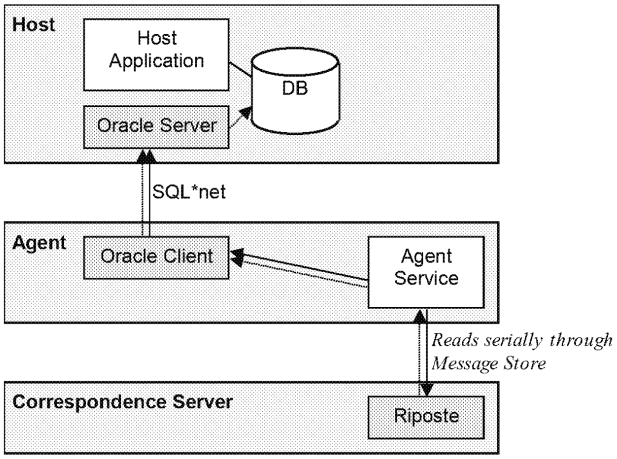

Figure 5.13 - Structure of a Bulk Harvester Agent

Each instance processes a subset of the outstanding messages, typically, on an Outlet by Outlet basis. The Client Interface Table in the Oracle database is used to store markers (relating to the Riposte journal), identifying which records have been harvested. This enables success units to be defined appropriate to the particular harvester.

Chapter 7 "Information Management" discusses success units in more detail.

The harvested records are re-formatted into the form that the Host wants them. They are added to the Client Interface Table using Oracle's client-server functionality.

When all Outlets have been harvested, the harvester exits.

Many Bulk Harvesters need to be triggered by an Outlet closing for the day. This is indicated by an End of Day Marker being written to the Riposte journal by the appropriate Application. A separate bulk harvester is used to detect the End of Day Marker. When it detects such a Marker, it writes a control record to the Oracle database indicating that the Outlet is ready to be harvested. The writing of this record triggers Maestro to initiate a Bulk Harvester to process that Outlet.

5.2.5.4.2.2 *Flat File Bulk Harvesters*

Certain Harvesters generate a set of Flat Files from the Agent Service. This service can run either within an Agent Service or directly within the Correspondence Server if performance reasons dictate.

Harvested records are passed to the Host in a Flat File. The Agent should operate between Markers written to the Riposte journal. While it may need to generate more than one Flat File to encompass all the Riposte records between the Markers, it should not include records either side of the Marker in one interface file.

The Host application may either manipulate the Flat Files directly (for example sorting, merging and splitting them to create the data sent to the Client). Alternatively, it may bulk load them into a database for manipulation, for example using the Oracle flat file load facility.

The structure is as shown here.

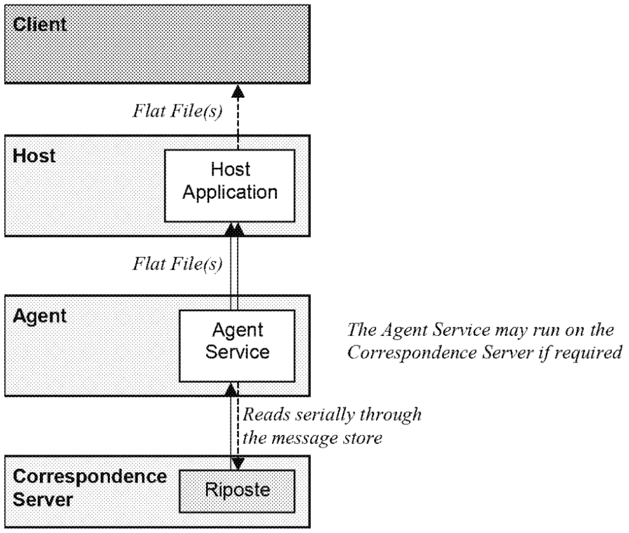
Client
Flat File(s)
Host
Host Application
Flat File(s)
Agent
Agent Service
The Agent Service may run on the Correspondence Server if required
Reads serially through the message store
Correspondence Server
Riposte

Figure 5.14 - Flat File Bulk Harvester Agents

Some Bulk Harvesters need to run continuously or periodically throughout the day. This can reduce the amount of work required at the end of the day, or to provide a more immediate response time without the performance overheads and single-streaming constrains of Interactive Harvesters. These are scheduled automatically by Maestro. They will use their own control mechanisms, based on work chunks, to identify the Outlets to be harvested.

5.2.5.4.3 Checkpoints

A “checkpoint” is a form of Marker (see Chapter 7 “Information Management”) over the whole message store. Checkpoint Messages are replicated across all Correspondence Servers in the Cluster. This makes it possible to guarantee the harvesting of all messages of the type being listened for without having to re-process all messages in the message store following a failure. Tivoli will detect a failed Agent and restart it. The Agent will restart from the latest message store Checkpoint and this will ensure that all relevant messages are processed.

5.2.5.5 Enquiry Agents

Enquiry Agents handle cases where a Counter application wishes to obtain some data from a Host System or external source.

5.2.5.5.1 Priority Messages

The Counter application can create a Riposte *Priority Message* that contains the enquiry or the update and captures its message-id. It then creates a message port waiting for a response to the enquiry or update. This response will be keyed on the message-id of the enquiry or update. The message port should be set to time out after a time specified by a configuration parameter set in a Persistent Object.

Note that a Priority Message merely attempts to trigger the raising of the communications line. If it succeeds, all waiting messages from the Outlet are transmitted to the Campus, finishing with the Priority Message that triggered the call. This makes it difficult to predict response times to Priority Messages.

5.2.5.5.2 Real Time Message Ports

Riposte supports *Real Time Message Ports*. These ensure that Priority Messages can be processed immediately by the message port, without waiting for the message to arrive in sequence, as is the situation with Priority Messages. This provides the ability to reduce certain response times by several seconds. Note that delivery through a Real Time Message Port is *not* guaranteed, and duplicates may also arise under certain recovery scenarios. Agents using this facility will need to be designed around these features.

⇨ Real Time Message Ports are used for OBCS "Foreign" transactions and for NBS and DCS Agents

5.2.5.5.3 Functions of Enquiry Agents

The Enquiry Agent listens for enquiries or update messages of a particular message type. When the Agent receives a message it makes the appropriate enquiry or update. The architecture beyond the Agent depends on the service being accessed.

Where the Enquiry Agent needs to go to an external source to answer the enquiry, it should set a time-out period that is just greater than the SLA agreed with the service provider. It should then wait for the response from the service provider. (It may start another thread to do this.) The time-out period should be significantly less than the time-out set at the Counter (which is there to deal with line failures).

After receiving a response from the service provider, the Agent creates a Priority Message with a key of the original enquiry or update, and returns it to the Counter application. This message can indicate to the Counter that it need no longer keep the link to the Campus open. Attributes within the message will provide the information required by the Counter application. Alternatively, after a time-out the Agent needs to indicate this fact to the Counter application.

In general, an enquiry should be treated as such, with the implication that the underlying transaction may not proceed depending on the outcome of the enquiry. The Host application component, if any, must not assume that it will complete. Ideally, neither the Host application nor the external system should make any changes to its own data because of an enquiry. There may be cases where this is unavoidable, because the external system is provided by a third party over which Pathway has no control. In this case, the Host application must understand and record any data changes made by the external application. In this exceptional case, the Host needs to provide a mechanism to reverse the change should the transaction not complete. This may require, for example, some End of Day processing to sweep up and reverse changes made by enquiries from transactions that were subsequently cancelled.

⇨ NBS provides an example of this. The [A] response to an [R] message is treated as a committal of the relevant funds. If the transaction is subsequently abandoned by the Customer, then the application must generate a "reversing" message that undoes its impact at the NBE or beyond

5.2.5.5.4 On-Line Access from Horizon to Merchant Acquirers

⇨ DCS transactions require the merchant (in this case PO Ltd, or Pathway on its behalf) to be able to obtain on-line authorisation of transactions which exceed the merchant's *floor limit*. PO Ltd have chosen NatWest Streamline (now part of the RBS Group) as their Merchant Acquirer, and are in the process of negotiating an appropriate Contract. They will use a floor limit of zero, thus forcing an on-line authorisation for all DCS transactions. Such authorisations are generated by standard code. They use a standard known as APACS 29 over an X.25 interface. Horizon will send the card details and transaction amount, and receive in return an authorisation (including an authorisation code) or a refusal code. The reply must be passed back to the Counter application.

5.2.5.6 Managing Message Recovery

Agents are responsible for managing recovery and message re-synchronisation between the Host Layer and the Counter Layer following a failure.

Riposte contains transaction features that allow multiple messages to be committed as one atomic unit. These ensure that messages are replicated as a unit, and another processor cannot read one message in the message run until all the messages in it have been replicated to that processor.

Equivalent facilities are available at the Host Layer within Oracle, and should be designed into other application types as appropriate.

Bulk Agents mark their work chunks as "in progress" as soon as they start to process them. If the Agent fails, this is detected by a Bulk Monitor running on the Host Central Server. This initiates a recovery process that will recover the failed work chunks.

Enquiry Agents and Interactive Agents run as Windows NT Services. Failure of one of these is detected by Tivoli, which then restarts the Agent.

The general strategy towards message recovery is:

- Applications should be able to detect duplicated messages and ignore the duplicate
- Agents must guarantee not to lose messages, though they can duplicate them.

As the traffic between the Agent Layer and the Host Layer is one-way, this avoids the need for a sophisticated two-phase commit protocol.

5.2.5.7 Agent Structure

The following table shows the functions that logically belong at the Agent layer, though as can be seen, some of them are located on other Platforms.

Component	Platforms
Agent Control Product (DW)	Data Warehouse Server
Agent Counter Common	Counter PC
Agent Management Utilities	Correspondence Server
Agent Performance Monitor Libraries	Agent Server Correspondence Server DCS Agent Server DCS Management Server
Agent Performance Monitor Libraries	NBS Agent Server
Audit Data Retrieval Agent	Audit Server Audit Workstation
Cluster Lookup Service (LUC)	Agent Server Audit Server Audit Workstation

	Correspondence Server DCS Agent Server DCS Management Server NBS Agent Server
Correspondence Agents Common Counter Configuration Administration Counter Monitoring Agent Counter Shutdown Monitor General Agents	Correspondence Server Counter PC Agent Server Counter PC Agent Server DCS Agent Server NBS Agent Server
Host Agent Control Multiple Riposte Library	Host Central Server Agent Server DCS Agent Server DCS Management Server NBS Agent Server
NT Agent Control TMS Distrib TMS Library	KMA Server Correspondence Server Agent Server Correspondence Server
TMS Outlet Monitor Agents	Agent Server Agent Server Correspondence Server
TMS PostOfficeRedirector - Agent TMS PostOfficeWait - Agent User Lock Request Library	Counter PC Counter PC Agent Server Counter PC DCS Agent Server NBS Agent Server PIN Pad Key Generation Workstation

A number of standard libraries are used to simplify the task of the Agent developer. Any particular Agent may not need to use services from all the functions indicated on this diagram.

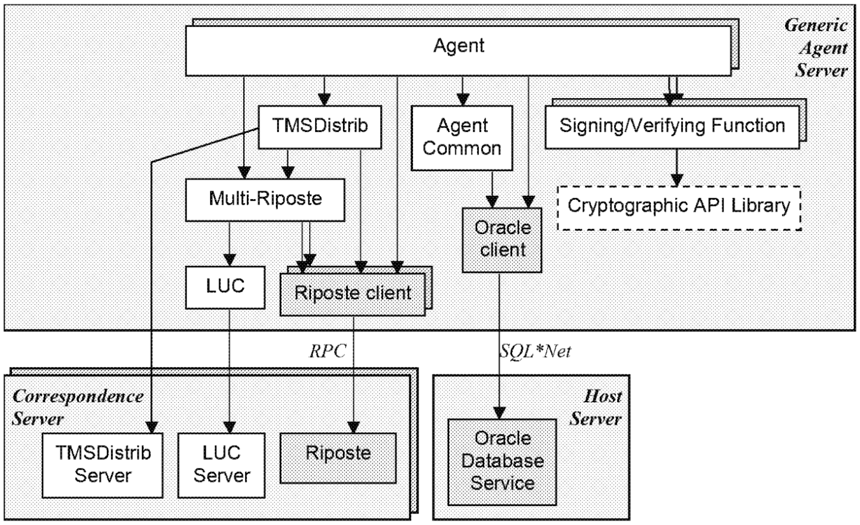

Figure 5.15 - Agent Structure

Agents are largely configured by information held in the Windows NT Registry. More verbose configuration information is held in serial files that are pointed to by Registry entries.

5.2.5.7.1 General Agents

This provides a range of general-purpose Agents including:

- "Ping" agent used by Tivoli to check that an Outlet can be accessed via ISDN
- EoD Harvester Agent that checks for End of Day markers from Outlets
- Central Acknowledgement Agent that harvests Acknowledgement messages generated by Counters when requested following receipt of a set of Reference Data
- Message Submission Loader Agent that passes message broadcasts from CS staff to Outlets

5.2.5.7.2 TMSDistrib

This is an instance of a case where applications provide specific code to interface to Riposte. This instance invokes a remote service to provide locking and co-ordination services across a number of Agents, and allows certain functions (primarily change of nominated office) to be isolated from other functions. It effectively forces the Agent to be single threaded.

5.2.5.7.3 Multi-Riposte Library

This is used to handle multiple Correspondence Server Clusters, and removes the need for an Agent to know in which Cluster a particular Outlet is located. It calls LUC to identify the Cluster to receive a message intended for a particular Outlet, and then invokes multiple Riposte Clients to access those Clusters. It is described in Chapter 6 "Distributed Application Services".

5.2.5.7.4 Look-Up Cluster Agent (LUC)

This calls the *LUC Server* to read Riposte data held in the Windows NT Registry to build up and store a list of Riposte services. It then calls Riposte to identify which Groups (Outlets) are handled by which Clusters. LUC services run on each Agent server and Correspondence Server, for resilience and performance reasons.

5.2.5.7.5 Counter Monitoring Agent

This is introduced at Release S06 and monitors the time that each Outlet last communicated with the Campus.

5.2.5.7.6 Oracle client

This is a standard Oracle Client that interfaces via SQL*Net to the Host Central Server at the Campus.

5.2.5.7.7 Message Signing and Verifying

Agents are responsible for "signing" (adding digital signatures) messages passed back to PO Ltd Clients. If an application needs to perform signing functions, it must provide its own signing code, annotated *Signing Functions* in the diagram.

⇨ *APS signs messages transferred to AP Clients. NBS adds a Message Authentication Code (MAC) which provides many of the same benefits, to messages transmitted to the NBE*

Signing is done by the Cryptographic Functions API Library.

Agents may also need to verify signatures that have been added at the Counter or by a third party. Again, the Cryptographic Functions API Library is used.

⇨ *APS and NBS signatures are verified by Agents.*

Other Cryptographic API functions permit Agents to "translate" security information from one protection domain to another without the relevant data being available in plain text other than within a *Hardware Security Module* (HSM)

⇨ This is used by NBS, which translates encrypted PIN values from the Key used by the Counter to that used by the NBE

5.2.6 Host Layer

5.2.6.1 General

The *Host Layer* applies any business rules to the information being received from or sent to the External Client System. It may also provide persistent storage of information on behalf of the external system.

The Host layer can be substantial, as is the case for TPS. It can also be so thin that it can, in theory, be absorbed within the Agent layer. An example is where there are few business rules and no persistent storage requirement. It may make sense to locate the Host and Agent components on the same server. However, the two application components must be clearly separated and only communicate via standardised mechanisms which apply whether they are co-located or not.

One essential task that can only be carried out at the Host layer is reconciliation. The Host is the only system component that can detect discrepancies between the transactions carried out at the Counter (and hence reported back to PO Ltd via TPS), and those that were authorised or expected. It should be in a position to send reconciliation reports back to its Client. These enable the discrepancy with the TPS records to be identified and resolved.

5.2.6.2 Application Integration

Each Host applications is independent of the others. They have no knowledge of how the others are implemented. They have independent databases, and do not directly share data. Host data processing requirements are covered in Chapter 7 "Information Management".

Host applications need to communicate with an Agent layer, and may need to interface to external interfaces. This communication can be achieved in several ways.

5.2.6.2.1 Batch Interface to External Bodies

Flat Files may be passed to and from external bodies using the FTMS or some other means.

5.2.6.2.2 On-Line Access by External Bodies

In exceptional circumstances, external Clients may need on-line access to the Host's data. This is provided via SQL*Net calls.

5.2.6.2.3 Communication with Agents

Agents communicate with Oracle-based Hosts using SQL*Net. Data to be passed to or received from Agents must be limited to Client Interface tables specifically designed for this purpose, as described below.

There are some exceptions to this. Some Agents read lookup data from Hosts. Architecturally, they should obtain this from Riposte instead.

Applications that do not need an Oracle based Host may pass Flat Files between the Host and Agents.

5.2.6.2.4 Communication With Other Hosts

In certain circumstances, Host applications may need to communicate with each other. Such communication is covered in Chapter 7 "“Information Management” and uses object-oriented methods which make no assumptions about the physical location of the other service.

5.2.6.3 Types of Host Application

Host applications fall into one of three classes.

- Complex applications that require a large amount of persistent storage, with high volumes and/or high transaction rates. These require the use of a sophisticated database system such as Oracle. These are located on one of the Host Central Servers.
- Less complex applications, with little persistent storage requirement. These may run on the Host Central Server, but any new applications of this type should consider the use of a Host Ancillary Server, an Intel Platform running under Windows NT Server. Oracle or Microsoft SQL Server can be used to provide the database functionality and storage mechanisms. Database backup and restore facilities are provided, but there is in general no failover facility in the event of loss of a Campus.
- Simple applications that have no requirement for a persistent database should, again, be implemented on a dedicated Intel-based Host Ancillary Server running under Windows NT server. Typically these generate or process Flat Files.

The *System Design Specification* (SDS) for a new application will determine into which type it falls.

5.2.6.4 Host System Components

Each application may include any of the following in its Host layer.

5.2.6.4.1 Host System

This is the actual application and the Platform on which it runs. Most existing Host applications are implemented as Oracle databases and associated applications. New applications may be implemented as new databases on Sequent or Windows NT Platforms, unless for the reasons given above it is decided to co-locate them with an existing database on the Host Central Servers.

5.2.6.4.2 Host Database

This is either a new Oracle database, a new schema and set of tables in an existing database, or a discrete SQL Server database. (At BI3, each application uses its own discrete database.) Guidelines are given in Chapter 7 “Information Management”. Whichever approach is used, its storage and other requirements need to be identified as these may impact on the performance of existing applications. Its capacity requirements should be lodged in Chapter 15 “Performance”.

Hosts should generate audit information representing any changes they make to their persistent data, using the mechanisms outlined in Chapter 7 “Information Management”.

5.2.6.4.3 Host Access Controls

Access Control processes manage the receipt of, and distribution of data to, external bodies.

The rules should reflect the [ACP] and Chapter 16 "Security". Pathway has a contractual obligation to protect the confidentiality of data belonging to PO Ltd and its Clients. Any potential conflict of interest between different Clients is best resolved by using different databases for their data.

5.2.6.4.4 Application Business Objects

Component	Platforms
Business Objects - Designer Bundle	MIS Support Workstation
Business Objects - End User Bundle	MIS Client Workstation MIS Support Workstation
Business Objects - End User Bundle	OCMS Client

Business Objects is a user-friendly definition of the information required to feed into the Data Warehouse. It is compatible with both Oracle databases and Flat Files. It is used, for example, to generate capacity planning information.

The *Designer Bundle* is used by authorised staff to construct Business Objects models for use on MIS Client PCs.

5.2.6.4.5 Client Interface Tables

Each application Oracle Database must include Tables that form the specific interface to the Agent layer.

- Loader Agents (see below) will read these Tables, or listen on them to pick up new or changed Records
- Harvester Agents will write information from the Counters *only* into these Tables.

Hosts must make these tables available to the Audit Service for writing to bulk storage media.

> *There are some feeds from the Host Databases directly into the Data Warehouse, bypassing both the Client Interface Tables and the MIS Interface Tables (see below). This should be reconsidered at an appropriate point.*

Non-Oracle applications must provide similar mechanisms to isolate the data available to the Host from that made available to the Agents. This can be Flat Files, or another structured database such as Microsoft Access or SQL Server.

5.2.6.5 Reconciliation

Each application needs to consider the following.

- How can it verify the integrity of the information that it passes back to its Client?
- How can it guarantee the internal consistency of this information with any data received from the Client?
- How can it guarantee that information passed by Reference Data is picked up by it and used in an appropriate way?
- How can it guarantee that its transaction information passed back to TIP is the same as the information that it passed back to its own Client?

5.2.6.5.1 Intra-Application Reconciliation

Where the application needs to carry out a reconciliation process over information which it passes back to its Client, or between this data and data which it receives from its Client, it should do so in its Host component. There are two reasons for this.

- Architecturally, the Host is the point at which significant business processing should be carried out
- Reconciliation is likely to involve the storage of information for at least a short time (days) and the Host database is the architectural point at which application persistent storage is implemented.

5.2.6.5.1.1 Database Applications

Where the application uses an Oracle database for persistent storage, it needs to carry out any necessary reconciliation using this and in accordance with the principles in [HADDIS].

⇨ An example is the *Data Reconciliation Service* (DRS) used by NBS and DCS

5.2.6.5.1.2 Flat Files

Whether or not the application uses a relational database, data passed back to the Client is transferred as Flat Files via the FTMS. These files should follow normal batch processing disciplines, and include volume and value totals for inclusion in trailer records.

5.2.6.5.2 Inter-Application Reconciliation

Reconciliation cannot be considered in isolation on an application by application basis. While each application may have its own internal reconciliation requirements, there are cases with every application where it is necessary to verify its data against that belonging to TPS, at the least, and sometimes to other applications. This is discussed below.

5.2.6.6 Data Reconciliation Service (DRS)

This is introduced at BI3 to support reconciliation of the many data flows introduced with NBS and DCS. It is described in Chapter 7

5.2.7 Help Desk Applications

Where a Help Desk application is provided to support telephone calls from Counter staff, it should provide a similar interface to that provided in the Outlets. This is provided by a pseudo-Counter PC providing access to the Correspondence Server message store (or a copy of it), though with perhaps a wider range of access rights than Outlet based Counter staff.

> *Earlier Help Desks can work from a copy of the Host data. The OBCS Stops Help Desk is an example. In these, data needed to populate the Help Desk is generated by the Host Application on a regular basis and copied (for example by FTMS) to the Help Desk system.*

5.2.8 External Interface Layer

This layer is responsible for retrieving or accepting information from, or sending it to, a Client System. It removes the complexity of handling these external interfaces from the Host layer of the application.

An application may contain either batch or real-time interactions, or both. Each may be initiated from either end.

5.2.8.1 File Transfer Managed Service (FTMS)

This is a generic file transfer interface mechanism that provides a secure and reliable mechanism for transferring files between Pathway and customers or suppliers.

5.2.8.1.1 FTMS Structure

Component	Platforms
FTMS Core Application	AP Client Gateway - Local AP Client Gateway - Remote Audit Server Capacity Management Server DCS Management Server General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote
FTMS Core Application for Unix	Host Central Server
FTMS General Purpose Local Configurations	General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote
FTMS General Purpose Remote Configurations	General Purpose FTMS Gateway - Remote

5.2.8.1.2 Use of FTMS

Pathway provides a Windows NT based Server within the Campus. It interworks with a similar Server installed by Pathway on the Client's premises. The overall structure of the FTMS is shown here. It is described in more detail in [FTMS].

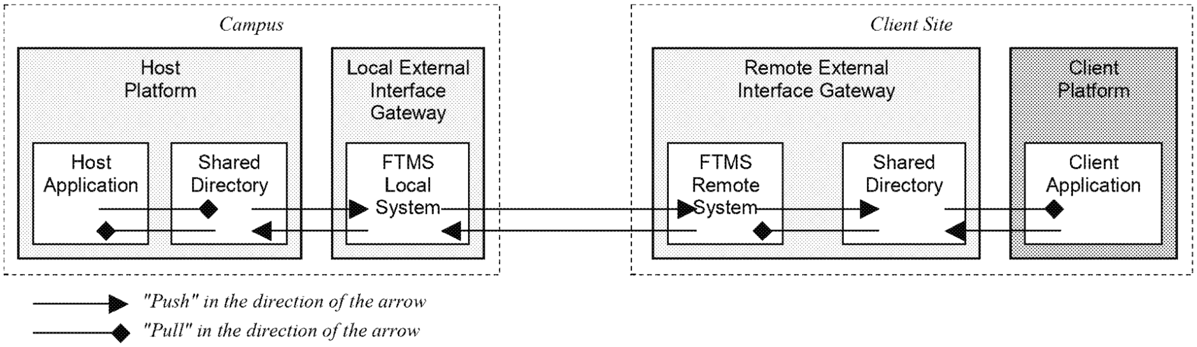

Figure 5.16 - File Transfer Managed Service

5.2.8.1.3 FTMS Core Application

The components of this model are responsible for a number of functions, as shown here. The type of function depends on the direction of the transfer. Versions are provided for both NT and UNIX.

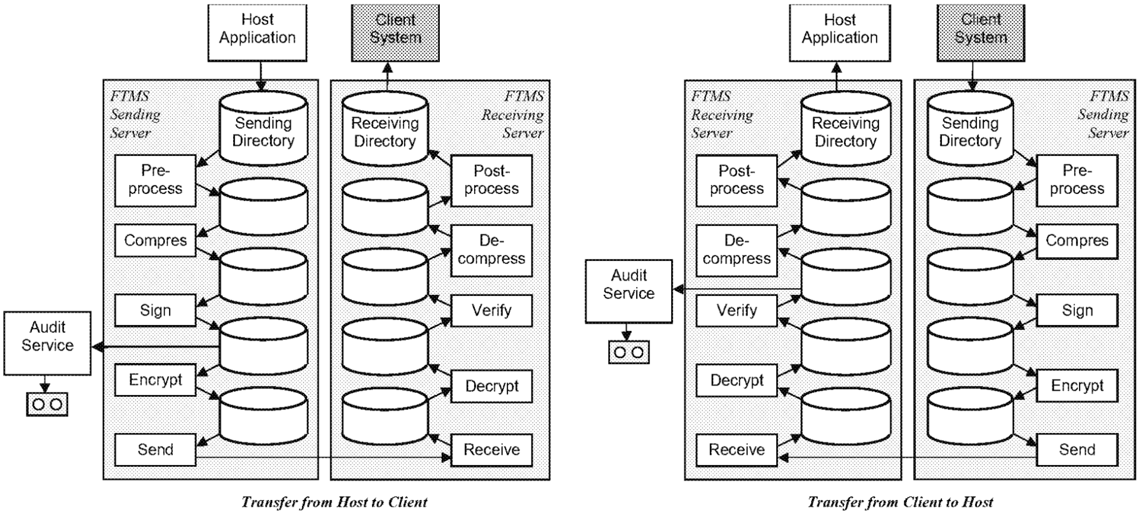

Figure 5.17 - FTMS Functions

FTMS runs as a series of inter-related Windows NT services, each triggered by the appearance of a file with an appropriate name in a designated directory. Each terminates by creating an output file in a (different) designated directory. The processes that may be carried out by any particular instance of the FTMS are driven by its configuration information, which is specified by the application designer, and may include the following.

- Pre- or post-process the file in any application specific way
- Compress the file to save on transfer time, and decompress on receipt
- Sign the file with a digital signature, and verify it when received
- Encrypt the file using software encryption, and decrypt on receipt (not needed where hardware encryption is available on the link)
- Copy the file to the receiving Platform
- Copy the file's control file, and if required the file itself, to the Archive Service.

Regardless of the direction of the transfer, the Campus end of the link is responsible for passing a control file, identifying the transfer, to the Archive Service. If required it also makes the transferred file available to the Archive Service.

5.2.8.1.4 UNIX Host File Transfers

Where the Host application runs on a UNIX server, the External Interface Gateways use NFS to extract data from or feed it into the Host System.

- On the local FTMS Gateway platform, this is provided by Hummingbird Maestro Solo
- On the Host platform, it is provided by the native Dynix NFS daemon

5.2.8.1.5 Windows NT Host File Transfers

Where the Host application runs on a Windows NT server, the communication method is distributed file sharing. The same mechanism is used between the two External Interface Gateway platforms.

5.2.8.1.6 Transfers at the Client Side

The preferred method of file extraction and delivery at the remote site with TCP/IP is FTP, using the standard Windows NT mechanisms.

Where the remote system is also a Windows NT platform, NT file sharing can be used.

Where there is no network connection to the Client system, a diskette drive or Iomega zip drive is used.

Remote FTMS Gateway services include a “user hook” from which a Client-specific transfer package can be invoked.

5.2.8.1.7 FTMS Configuration Files

For each instance of an FTMS service, the Application provides up to four Configuration files.

- One at the Local (Campus) end to transfer files from Pathway to the Client
- One at the Local end to transfer files from the Client to Pathway
- One at the Remote end to transfer files from Pathway to the Client
- One at the Remote (Client) end to transfer files from the Client to Pathway.

5.2.8.2 Batch Interface to OBCS

⇨ For historical reasons, a different approach is taken to data passed to Pathway from the OBCS systems. Files are transferred directly from the Benefit Agency's VME system to the Host Central Server, without the intervention of External Interface Gateways or the use of FTMS. The transfer mechanism is FTF using software provided by Hytec.

5.2.8.3 Interactive Client Interface

There is no generic model for this type of interface.

5.2.8.3.1 Interactive Access From Client

In some instances, on-line access is required from other suppliers to or Clients of PO Ltd to Horizon.

This is an exceptional requirement. It should only be implemented where there is no practical alternative. Approval is needed from the Chief Architect before an application may introduce a mechanism of this type. Any such mechanism should include full consideration of qualities such as Security.

5.2.8.3.2 Interactive Access To Client

In some cases, the Counter transaction needs to make an on-line enquiry to an application run by the Client. The rules in this case are set by the Client and agreed with Pathway and PO Ltd. Horizon's task is to understand the nature of this interface, and define appropriate SLAs to monitor its use.

In most cases, this access occurs at the Agent Layer rather than via the Host.

⇨ NBS and DCS both provide examples of this type of working

5.2.8.4 Supplier Interface

An application may need to pass data to, or receive it from, an external supplier. Applications need to consider providing new code to handle this interface.

Similar mechanisms are used to the generic Client Batch Interface paradigm. Pathway provides External Interface Gateway PCs that carry out a file transfer between the Supplier and the Campuses. Data is transferred as Flat Files, and controlled by FTMS.

The files transferred are generated by or received by the Host Component of the application.

5.3 ANCILLARY APPLICATIONS

5.3.1 Transaction Processing System (TPS)

This mechanism is used to harvest information about all transactions carried out in the Outlets, and feed it back to the PO Ltd TIP system.

5.3.1.1 Structure

Component	Platforms
Database Links	Host Central Server
FTMS TIP to TPS Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS TIP to TPS Remote Connection Configuration	POCL Standby Gateway - Remote
	POCL TIP Gateway Server - Remote
FTMS TPS to TIP Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS TPS to TIP Remote Connection Configuration	POCL Standby Gateway - Remote
	POCL TIP Gateway Server - Remote
TPS Database	Host Central Server
TPS Host Application	Host Central Server

5.3.1.2 TPS Counter

There is no TPS Counter component *per se*. TPS is sent information about *all* transactions carried out on the Counter, by whatever application.

5.3.1.3 TPS - Agent

Transactions are gathered in the first instance by the *TPS Harvester Agent*. This is a standard Bulk Harvesting Agent running within the Agent Layer. It collects all messages that result from Counter transactions, stock unit balancing and Outlet cash accounting, and feeds them into the TPS database, from whence they are fed to TIP. New applications need to log a particular message type that is harvested by this Agent, and to ensure that this message type is not shared with any other application.

5.3.1.4 TPS Database

This is an Oracle database running on a Host Central Server.

5.3.1.5 TPS Host Application

This Host application stores, manipulates and processes the TPS data ready for submission to TIP.

5.3.1.6 TIP Interface

This is a standard File Transfer gateway that passes TPS information back to PO Ltd's TIP service, and receives acknowledgements from PO Ltd. The time taken to transfer the data may be impacted by the introduction of a new application.

5.3.1.7 Application Reconciliation with TPS

TPS harvests all messages relating to transactions carried out at the Counters and transmits them, in a series of Flat Files, to PO Ltd.

There must be at least one point in the day when the transactions sent to PO Ltd are in step with those sent to each Client.

Harvesting is triggered by the Outlet writing an End of Day Marker to the Riposte journal. Thus, this requirement will be met by using the End of Day Markers to delimit both sets of transactions.

Conceptually, the data transmitted to TPS is the sum of the transaction data harvested by all other applications. However, it could vary from this for a number of reasons, including the following.

- An Outlet's End of Day Marker may arrive after the TPS Harvesting completes but before the application's Harvester (or vice versa), and thus its transactions appear in different "days" so far as the two applications are concerned
- Applications harvest messages from some different end-point than the Outlet's End of Day Marker
- The Application Harvester misses some messages which it should have read, and which were in fact read by the TPS Harvester
- Messages are harvested by both applications but differ in their details
- One or other Agent failed and during its recovery some messages were lost (not likely) or were harvested twice (the preferred recovery strategy)

5.3.1.7.1 Messages Harvested in Different Days

To avoid differences caused by messages being processed in different days, End of Day Marker are detected by one Harvester that then updates an Outlet-specific persistent object to indicate that the Outlet has completed its End of Day activities. All other Harvesters work from this set of Persistent Objects, and not from the EoD markers themselves.

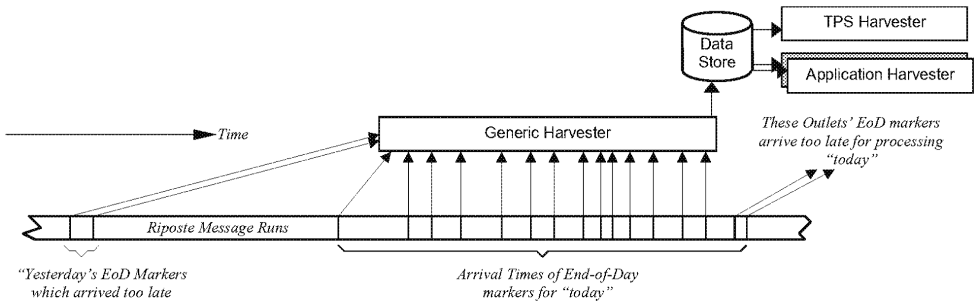
Data Store
TPS Harvester
Application Harvester
Time
Generic Harvester
These Outlets' EoD markers arrive too late for processing "today"
Riposte Message Runs
"Yesterday's EoD Markers which arrived too late
Arrival Times of End-of-Day markers for "today"

Figure 5.18 - Common Harvesting Datastore

5.3.1.7.2 Different End Points

Problems will arise where application harvesters use something other than the Outlet's End of Day Marker to delimit the messages they harvest.

5.3.2 Management Information System (MIS)

As well as feeding details of all transactions to PO Ltd, there is a need to feed similar information into the Data Warehouse for use by the MIS applications. This is carried out by the TPS Harvester.

5.3.2.1 Structure

Component	Platforms
Ad Hoc Reporting Universe	MIS Client Workstation MIS Support Workstation
Data Warehouse Agents	Agent Server
Database Links	Host Central Server
MIS Application	Data Warehouse Server
MIS Business Development Reporting	MIS Client Workstation MIS Support Workstation
MIS Business Objects	MIS Client Workstation MIS Support Workstation
MIS Business Objects APR	MIS Client Workstation MIS Support Workstation
MIS Business Objects Customer Service Reporting	MIS Client Workstation MIS Support Workstation
MIS Business Objects Universe	MIS Client Workstation MIS Support Workstation
MIS Common Software	MIS Client Workstation MIS Support Workstation
MIS Contract Administration	MIS Client Workstation MIS Support Workstation
MIS Datawarehouse Archiving	Data Warehouse Server
MIS Datawarehouse Backup & Recovery	Data Warehouse Server
MIS Datawarehouse Build	Data Warehouse Server
MIS Datawarehouse Processing	Data Warehouse Server
MIS Datawarehouse Reference Data	Data Warehouse Server
MIS Datawarehouse Restore	Data Warehouse Server
MIS Datawarehouse Scheduling	Data Warehouse Server
MIS Datawarehouse Setaside Tablespaces	Data Warehouse Server
MIS Datawarehouse Tablespaces	Data Warehouse Server
MIS Datawarehouse TPS	Data Warehouse Server
MIS Reference Data Maintenance	MIS Client Workstation MIS Support Workstation

5.3.2.2 MIS Harvester

At a later Release, a separate MIS Harvester will be introduced. It will harvest all message types that need to be fed into the Data Warehouse.

5.3.2.3 MIS Interface Tables

The Data Warehouse is an Oracle database running on a separate Sequent server from the Host Central Servers.

Data is fed into it from Flat Files generated by the TPS Harvester. The database contains *MIS Interface Tables* that are populated by the MIS Harvester as the first stage of populating the MIS with this data. These will be used in the same way as an application's Client Interface Table. The size of the table may be impacted by the introduction of a new application.

5.3.2.4 Application MIS Data

This is data held in the Data Warehouse that is specific to a particular application. It may be necessary to define new Tables as part of the design of a new application.

Data is maintained for the following applications:

- Reference Data (RDMS)
- Service Level Agreement Monitor (SLAM)
- Transaction Processing Service (TPS)

5.3.2.5 Application MIS Business Objects

Business Objects provide a user-friendly view of the data in a database, and this mechanism permits Pathway management to view the Data Warehouse data generated by a particular application. Universes are provided for:

- APR
- Business Development

The Ad-hoc Reporting universe provides generalised access to data in the MIS. It is used for Capacity Management.

5.3.2.6 MIS System

This constitutes the set of applications that provide the MIS functionality. Any of these applications could be impacted by the addition of a new business application.

5.3.2.7 Specific MIS Applications

The following applications are provided, as described in Chapter 4 "Overview".

- Business Development
- Service Level Agreement Monitor

5.3.3 Reference Data Management Centre

Riposte makes it relatively simple to configure a new Counter Application by the use of Reference Data. This makes the application "soft centred" and hence easy to modify in response to changing user requirements. The structure and use of this data is described in Chapter 7 "Information Management".

Any new application thus needs to provide for the handling of the Reference Data it needs. Overall, Reference Data is fed to Pathway via the RDMC. Each application may need to make its own contributions to the RDMC system.

Reference Data has two aims. One is to provide the standing data at the Counter that is used to populate the transaction as it is assembled by the Counter Clerk. The second is to enable operational changes to be implemented at a system level, without the need for code changes. This aim supports a number of business processes such as those involved with the creation of a new service, or a new Outlet, or deletion or closure of the same. These processes involve:

- validation and error correction
- ensuring the security and integrity of Reference Data
- the transformation and distribution of Reference Data to the target applications at appropriate times
- provision of Reference Data to Pathway development for test purposes

These incur consequential processes for ensuring data integrity, such as referring back to the Reference Data provider any errors found during any kind of validation (including site surveys), and managing errors due to transformation.

5.3.3.1 Types of Reference Data

Reference Data is of four types covering three classes of data.

- Type A Reference Data
- Type B Reference Data
- Type C Reference Data
- Type D Reference Data

5.3.3.1.1 Type A Reference Data

This defines business rules. It is supplied by PO Ltd across the Reference data Interface as Type A or Type B data. It is Temporal data transmitted electronically over an automated interface from the PO Ltd RDS system, and loaded automatically into the RDMS. It includes product specification data, data that configures the Counter application to support various classes of external Clients. Type A Reference Data is not configured by Pathway. Examples include:

- Outlet-related data, indexed by FAD Code, e.g. address, type of Outlet, opening times, number of Counters
- Product-related data e.g. Product Code, Name, Price, Outlets at which the product is available
- Cash Account mapping data for each transaction type

⇨ It also includes application-specific data such as the types of card supported by NBS or DCS, and the rules relating to each type of card

5.3.3.1.2 Type B Reference Data

This is temporal data transmitted electronically over a non-automated interface from PO Ltd RDS to the RDMS, and enriched by data loaded manually by Pathway. Scales data is an example of this type of data; Pathway enriches the data provided by PO Ltd with Scale Service product numbers.

5.3.3.1.3 Type C Reference Data

This is Temporal data prepared by Pathway in response to PO Ltd requests or as a result of system changes, loaded by manual processes into RDMC. It includes Menu Button Definitions and Primary Mappings, and is enhanced with the additional products that represent the NBS transactions. Type C Reference Data is also used to configure the EPOSS and LFS Counter products.

Examples are:

- Button positions on screen
- Print positions on menus
- Layout of data on magnetic stripe cards

5.3.3.1.4 Type D Reference Data

This is data prepared by Pathway, mainly non-temporal build dependent definitions. It is not loaded into RDMC. Type D data is used to define Counter applications (such as Operation Launch). It is also used to define application- or desktop-specific data such as messages to the clerk and implementation parameters.

5.3.3.1.5 Type X Reference Data

This is defined for future use, and will comprise Counter applications delivered as scripts (for example in XML).

5.3.3.2 RDMC Structure

Component	Platforms
Counter Reference Data	Counter PC
FTMS RDB to RDMC Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS RDB to RDMC Remote Connection Configuration	POCL Standby Gateway - Remote POCL TIP Gateway Server - Remote
FTMS RDB to RDT Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS RDB to RDT Remote Connection Configuration	POCL TIP Gateway Server - Remote
FTMS RDMC to RDB Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS RDMC to RDB Remote Connection Configuration	POCL Standby Gateway - Remote POCL TIP Gateway Server - Remote
FTMS RDMC to UKSS Local Connection Configuration	General Purpose FTMS Gateway - Local
FTMS RDMC to UKSS Remote Connection Configuration	General Purpose FTMS Gateway - Remote
FTMS RDT to RDB Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS RDT to RDB Remote Connection Configuration	POCL TIP Gateway Server - Remote
Message Submission Application	RDMC Administrator Workstation
RDDS Database	Host Central Server
RDDS Host Application	Host Central Server
RDMC - Change Control Application	RDMC Administrator Workstation
RDMC Access Control	RDMC Administrator Workstation
RDMC Administration Application	RDMC Administrator Workstation
RDMC Database	Host Central Server
RDMC Host Application	Host Central Server
RDMC Interactive Data Loader	RDMC Administrator Workstation
RDMC Release Manager	RDMC Administrator Workstation
RDMC Reports	RDMC Administrator Workstation
RDMC Send	RDMC Administrator Workstation
Reference Data Agents	Agent Server

The RDMC broadly follows the overall application structure, but has some significant differences.

The RDMC in fact consists of two Oracle databases:

- The *Reference Data Management System* (RDMS), that contains the Reference Data itself.
- The *Reference Data Distribution System* (RDDS). This holds Reference Data released for use in a particular environment. The principal RDDS is used to distribute Reference Data to the live environment. There may be other RDDS instances, accessing the RDMC, that feed data to various test environments.

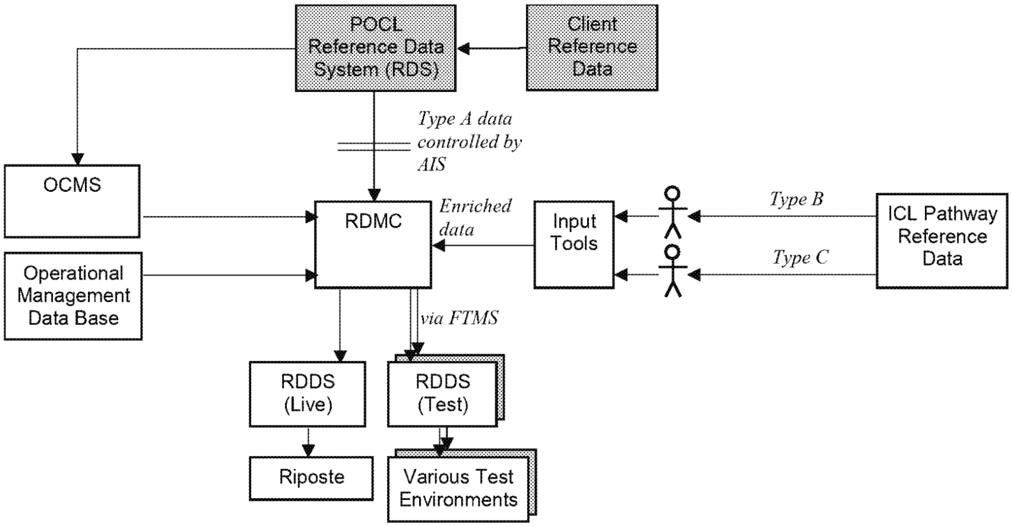
POCL Reference Data System (RDS)
Client Reference Data
Type A data controlled by AIS
OCMS
RDMC
Enriched data
Input Tools
Type B
Type C
ICL Pathway Reference Data
Operational Management Data Base
via FTMS
RDDS (Live)
RDDS (Test)
Riposte
Various Test Environments

Figure 5.19 - RDMC Structure and Data Feeds

There are data feeds into the RDMS as follows.

- The *Operational Management* Database (OMDB) provides a feed of how many Counters are active in each open Outlet.
- The *Outlet Change Management Service* (OCMS)
- Pathway Reference Data is input manually and enriched by appropriate input tools.

5.3.3.3 Reference Data processing Threads

Separate but parallel facilities, and data handling threads, are used for each of these three types of Reference Data, though any particular application may not include data or the associated processing threads for all three types. A new application may thus need additional PO Ltd, Pathway or Client Reference Data, plus appropriate RDMS functionality to handle it. This functionality follows the standard threads (External Interface, Host and Agent) through the Application Architecture.

In most cases, this functionality is provided within the core RDMC system. However, where there is a close interaction between the nature of the Reference Data and the operation of the application, Reference Data processing may be a part of the application itself. This is the case for APS, for example.

The components of each processing thread are described below. While there may be interactions between the threads for any particular application, there must be no interaction between the Reference Data belonging to one application and that for another.

5.3.3.4 Reference Data Interface

For each of the three types of Reference Data, an application needs to consider the provision of a separate *Reference Data Interface* facility. Each such type forms a discrete Collection.

Interface mechanisms already exist for defining Pathway Reference Data and PO Ltd Reference Data. Where the application is developed in response to the need to support a new Client, the application will need to ensure that a Client Interface is provided. This may use the same mechanisms as are used for Client Interface, or the Client may pass their Reference Data to Pathway via PO Ltd as shown in the diagram above.

Reference Data is received from these sources, normally via FTMS, as as text files with *Comma Separated Values* (CSVs). The structure of Reference Data input files for a particular type of data is defined by an AIS. This may change (usually at a new Horizon Release) but will always have a defined version at any point in time.

All Reference Data from whatever source must be verified before it is implemented. Formats of files and records are validated against the AIS in force at the time

The degree of further verification depends on the *Change Classification* of the data, as follows.

- Class 1 data types are those which have no impact on the system or the service, and can be passed through to the Counters without change control
- Class 2 data could impact just the service. An example would be a change to the number of receipts to be printed for a session. Reference Data would allow up to 99. This could impact the service response times at the Counters
- Class 3 data involve logistical changes. An example is a change to an Outlet requiring rewiring and/or reinstallation of Pathway equipment. Change to a FAD Code is another example
- Class 4 data involve changes to Reference Data in order to effect the change. Introducing a new item/product could require a new or changed Button on the screen, or a change to menu hierarchies. These changes need to be managed and tested before releasing to the Counters, and some training could be involved as well
- Class 5 data requires a code change, and would be subject to the software Release process

5.3.3.5 Application Reference Data

5.3.3.5.1 Business Reference Data

PO Ltd Reference Data needed by an application is loaded into the *Reference Data Management System* (RDMS) Oracle database which is located on a Host Central Server. RDMS is a standard application (at least at the External Interface, Host and Agent Layers).

Pathway Reference Data is input manually or from a development database by the developers of each Pathway Counter System, and conforms to an AIS comprising a documented screen layout with validation and loading rules. The data in question are, typically, Screen and print formatting data, error messages, etc. The RDMC validates that the data are what they are meant to be. They are distributed to a test system before being released to the Counters.

The resulting data set represents an enrichment of the Reference Data as received.

It is a key requirement of PO Ltd, that changes to be implemented via Reference Data will be implemented completely and reliably by Pathway. This is a major quality issue, and requires that an audit trail of changes is maintained by the RDMC. (A corollary is that there is no way to modify the data received from PO Ltd, even if it contains errors. All that is possible is to report these errors back to PO Ltd in the expectation that they will be corrected in a new Release of Reference Data.)

To enable Pathway to carry out this responsibility, PO Ltd will always identify the data items that enable an "atomic" change to be implemented completely and reliably. The unit of change of the Reference Data is the Record. Thus to change a data item requires a re-issue of the entire record which contains it.

5.3.3.5.2 Client Reference Data

Where the application design requires that data is transmitted from the Client directly to Pathway, then an application component must be created to receive, manipulate and distribute it. This can be modelled on the RDMS structure, as is the case with APS.

5.3.3.6 Manipulating Reference Data

There is a need to input or manipulate Reference Data manually in some circumstances. This is entered into the RDMC database tables using a Microsoft Access data entry application. The data entry application runs on a Windows NT workstation (the RDMC Administration Workstation) PC and calls PL/SQL packages in the RDMC.

5.3.3.7 Reference Data Distribution Service

Enriched Reference Data intended for Counter PCs is loaded into application-specific Interface Tables for transfer to the application. This is carried out by the *Reference Data Distribution Service* (RDDS), which is invoked by Pathway Customer Services. The Interface Tables correspond to those used by standard applications. The RDDS is invoked when a set of Reference Data is ready for release. This will reflect or precede the introduction into service of an application or of changes to it, and will follow detailed testing of the application or its upgrade away from the Campuses.

Multiple instances of this Agent run in parallel.

Some Reference Data is packaged into files and delivered to Counter PCs via Tivoli.

5.3.3.8 Reference Data Loader Agents

A Bulk Loader Agent is used to organise the distribution of the Reference Data to the correct Outlet. It takes data from the Reference Data Interface tables, converts it to Attribute Grammar and feeds it into the RMS. Target Outlets are identified by in the change data by their FAD Codes.

A Reference Data Scavenger Agent runs nightly to delete obsolete Core Reference Data. This will help to reduce the size of the Reference Data at both Campuses and Outlets.

A large proportion of Reference Data (especially that originating with Pathway) is applicable to all Outlets. These will have a GroupID of Null. Messages with this GroupId are written to a "dummy Group" (e.g. 999997). A Reference Data Replicator Agent then replicates this data to all currently active Outlets. This mechanism ensures that new Outlets get the latest Reference Data. Facilities are provided to limit the overnight window within which Reference Data is distributed to Outlets.

Facilities are provided to "scavenge" obsolete reference data, and avoid the size of the message store growing in an uncontrolled way.

Other "dummy Groups" include the RDMC Replicator dummy office. These *must* be different, otherwise Virtual Office data gets replicated to all offices.

Classes of Outlet may include:

- Northern Ireland vs. non-Northern Ireland (or, in more general terms, the Region)
- LF S Outlets with "stringent SLAs" vs. those with "less stringent SLAs
- Crown Post Offices vs. Sub-Post Offices

Riposte includes a facility to define "Global Persistent Objects", and code to exploit these facilities will be in place at BI3. A Group (Outlet) may be assigned to one or more *Subscription Groups*. Any messages sent to a Subscription Group are automatically replicated to all Outlets that are members of the group, but only need to be held once in the Correspondence Server message store. This facility also enables Reference Data to be targeted at different types of Outlet without the originator needing to know from day to day which Outlets are in which class.

This feature should be used only for static data. It must not be used for data that changes rapidly, for example those Outlets that have been upgraded from one Release to the next.

5.3.3.9 Application Reference Data Users

The principal recipients of Reference Data are the Counter Applications whose structure is described in detail above. However, there are some other Recipients of Reference Data, including the following.

- TIP. This is fed by the TPS Harvester, and hence contains records of all Counter transactions. These may include information based on Reference Data (though no Reference Data *per se* is passed to TPS).
- The Data Warehouse. This is fed by the MIS Harvester. Data in the Data Warehouse is accessed by the MIS applications. The key input here is the transactions executed and their response times. Transaction information may be aggregated.
- The Horizon Systems Help Desk

Other recipients include the following.

5.3.3.9.1 Roll-Out Database

This is passed details of Outlets pending their installation. Data is passed to the Roll-Out Database via FTMS.

5.3.3.9.2 Test Users

Reference Data received from PO Ltd is passed to a number of test environments in Bracknell, via FTMS.

5.3.3.10 Monitoring Receipt of Reference Data

A number of Contract clauses require Pathway to monitor and report on the time at which certain Reference Data changes are received by the Outlets. The Loader Agents can append an acknowledgement request to a sequence of Reference Data. This request is actioned by each Counter PC when it reads it, and as the messages are processed in sequence, indicates that all preceding messages have been received up to that point.

An Acknowledgement Agent running in the Campuses reads these acknowledgements and is able to calculate the adherence to Reference Data SLAs.

5.3.3.11 Message Broadcast

RDMS provides a facility for CS staff to broadcast messages to all or a subset of the live Counters.

5.3.3.11.1 Message Submission Application

This runs on the RDMC Administration Workstation, and provides facilities to format a message and to specify the set of Outlets that it will be sent to. The message is written to the RDMS Database on the Host Central Server, and then inserted into the Correspondence Server message store by the Reference Data Agents. It is distributed to each Counter the next time that replication occurs to that Outlet.

At the Counter, the message is displayed by the Counter Clerk using the *Memo View* facility of Riposte. An icon is displayed on the desktop when there is an unread message.

See [MBS].

5.4 CONFORMING APPLICATIONS

This Sub-section lists the business applications that conform to the above model.

5.4.1 Automated Payment System (APS)

APS is described in detail in [APSHLD].

5.4.1.1 Structure

Component	Platforms
APR Application	Host Central Server
APS Agents	Agent Server
APS Counter Application	Counter PC
APS Database	Host Central Server
APS Host Application	Host Central Server
APS SCCache	Counter PC
APS User Maintenance	RDMC Administrator Workstation
Database Links	Host Central Server
FTMS AP Client Local Connection Configuration	AP Client Gateway - Local
FTMS AP Client Remote Connection Configuration	AP Client Gateway - Remote

5.4.1.2 Functions

APS supports payments by customers to Utilities and other Clients of PO Ltd using magnetic swipe cards or smart cards.

- For payments using a magnetic swipe card, the card indicates the customer's "account number" with the Client, and the amount paid is credited to that account.
- For payments using a smart card, the value of the transaction may be written as credit to the card. This is then used to transfer the credit to a meter in the customer's house. Because the card thus represents a monetary value, there are increased security constraints surrounding its use.

Details of all APS transactions are gathered by the APS Host application. This transfers files of transactions direct to the relevant Client.

5.4.1.2.1 APS Counter Application

This handles tokens presented to the Counter Clerk. Functions include token validation (format, checksum, valid Client etc) against information held in APS Reference Data.

"Reversals" are permitted, but only in the Outlet where the original transaction took place, and subject to business rules that depend on the token type.

All smart card tokens are handled by procedures that are specific to the type of card.

Receipts are generated for completed transactions.

See [APSCHLD].

5.4.1.2.2 APS Agents

APS Harvester Agents collect APS transactions from the Riposte Message Store and write them to the APS Database.

APS Loader Agents take Client Data from the APS Database and distribute it to Outlets.

5.4.1.2.3 APS Host Application

This generates a data file for each Client, containing records of all transactions carried out on behalf of that Client, and arranges for the transfer to the Client.

5.4.1.2.4 APS Reconciliation

APS transactions are harvested by both the TPS and APS Agents. APS Reconciliation verifies consistency between the records harvested at various points within Horizon.

5.4.1.2.5 APS Database

This Oracle database holds details of APS transactions *en route* to the Client, or APS-relevant information destined for the Counter.

5.4.1.2.6 APS Reference Data

APS uses Reference Data to define the following classes of data.

- *AP token types and data*, defining the format and content of APS tokens
- *AP product data*, including business rules such as which tokens are supported at which Outlets. It also includes presentation data such as menu hierarchies, Icons and validation rules, receipts and report formats.
- *AP Client data*, describing the Client and account against which transactions are charged

In addition to this, Clients may define Client data that contains information about the customers of the Client, such as authorisation codes, stop lists, tariff data and others.

5.4.1.2.7 APS SCCache

This "caches" APS smart card token information within the Counter in a secure manner.

5.4.2 Order Book Control Service (OBCS)

5.4.2.1 Structure

Component	Platforms
Database Links	Host Central Server
FTMS OBCS to UKSS Local Connection Configuration	General Purpose FTMS Gateway - Local
FTMS OBCS to UKSS Remote Connection Configuration	General Purpose FTMS Gateway - Remote
OBCS Agents	Agent Server
OBCS Counter Application	Counter PC
OBCS Database	Host Central Server
OBCS Host Application	Host Central Server
OBCS Stop List Enquiries	Horizon Help Desk Terminal

5.4.2.2 General

OBCS provides facilities to monitor the issue of DSS payment *Order Books*, which are presented by customers in Outlets to claim benefit. Usually, one page (or "foil") is detached by the Counter Clerk for each payment due. The book itself is bar-coded.

OBCS maintains a record of the Outlets that a Customer has used a particular Order Book in, and should a *Control Notice* be issued against the Order Book (invalidating or restricting the use of the book), this is copied to every relevant Outlet.

If a Customer uses an Order Book in an Outlet for the first time, a check is made against the central OBCS Database that the book is valid and that there is no outstanding Control Notice against it.

See [OBCS].

5.4.2.3 OBCS Counter Application

This carries out the Counter part of the OBCS application, including validation of Order Books via their bar codes. It includes an Outlet-specific list of Order Books that have been previously used in that Outlet, together with Stop information that may be used to refuse payment. If the Outlet has no record of the Order Book, a Riposte Priority Message is generated to request details of the book (including any Control Notices) from the OBCS Host Application.

See [OBCSCNTR].

5.4.2.4 OBCS Stop List Enquiries

This is an application running on the Horizon Help Desk terminal. If the Counter Clerk cannot validate a new Order Book (for example because the network to the Campus is unavailable) the Counter Clerk phones the HSHD. Staff there have access to a complete set of Control Notices and can rule on whether to permit the payment.

5.4.2.5 OBCS Agents

These Agents provide two functions.

- They pass details of all OBCS transactions carried out in Outlets back to the OBCS Host Application and thence to the DWP
- They pass Control Notices to Outlets at which an Order Book has been used
- They handle enquiries when an Order Book is used fro the first time at a new Outlet

5.4.2.6 OBCS Database

This holds details of OBCS encashments, as well as details of Outlets that an Order Book has been used in, and any Control Notices that have been notified by the DWP.

5.4.2.7 OBCS Host Application

This provides the following facilities.

- Respond to queries from Outlets when an Order Book is used for the first time at the Outlet
- Receive encashment data from Outlets, batch this up and transmit it to the BA ENCS
- Receive CNs from the BA and pass this to relevant Outlets

5.4.3 Electronic Point of Sale Service (EPOSS)

5.4.3.1 General

EPOSS is a Counter-only application that provides three major functions.

- Point of sale support for retail processes
- End of Day processing
- Manual migration

5.4.3.2 Structure

Component	Platforms
EPOSS Counter Application	Counter PC
HTML	Counter PC
MiMAN	Counter PC

5.4.3.3 EPOSS on Counter

This provides point of sale support. All transactions are recorded as Riposte messages that are subsequently harvested by TPS and transmitted to TIP. Product information is provided by Reference Data.

5.4.3.4 Counter End of Day

End of Day runs at (typically) 17:00 each working day and handles the end of day reconciliation process. It scans through the messages generated in the Outlet that day, and balances the cash account and stock levels. It generates an End of Day marker that, when it arrives at the Campus, initiates the harvesting process for that Outlet.

5.4.3.5 MiMAN

Manual Migration is a set of facilities for the manual “remming in” of stock and cash levels at Outlet migration or re-installation after a temporary closure.

5.4.4 Logistics Feeder Service (LFS)

Component	Platforms
FTMS LFS to SAPADS Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS LFS to SAPADS Remote Connection Configuration	POCL TIP Gateway Server - Remote
FTMS SAPADS to LFS Local Connection Configuration	POCL TIP Gateway Server - Local
FTMS SAPADS to LFS Remote Connection Configuration	POCL TIP Gateway Server - Remote
LFS Agent	Agent Server
LFS Counter Application	Counter PC
LFS Database	Host Central Server
LFS Host Application	Host Central Server

5.4.4.1 General

LFS is the Pathway component of PO Ltd's *Automated Distribution System*. The PO Ltd central element is SAPADS. ADS handles the management and distribution of cash and value stock, principally to minimise cash held overnight in Outlets and Outlets' value stock holdings generally.

LFS provides for notification:

- From SAPADS of planned orders and stock advice notices
- To SAPADS of cash held at Outlets
- To SAPADS of stock held at Outlets
- To SAPADS of pouches received at Outlets
- To SAPADS of pouches dispatched from Outlets

See [LFS]

5.4.4.2 LFS Counter Application

LFS provides a set of "back office" functions that include the ability to record receipt of pouches from PO Ltd's Couriers. It also interfaces to various EPOSS components, using data provided by the *Overnight Cash Holding* (ONCH) function, the stock balancing and office rollover functions. It uses the Peripheral Server, with appropriate Token definitions, to facilitate, and validate, the scanning of the delivery and collection pouch barcodes.

5.4.4.3 LFS Agent

An LFS Bulk Loader is used for the distribution of Planned Orders and Advice Notices.

A single Interactive Harvester captures all LFS messages that are required by SAPADS. LFS reuses the Reference Data Agent Replicator to distribute Advice Notices that must be sent to all Outlets.

5.4.4.4 LFS Host Application

This receives information from SAPADS and forwards it to the relevant Outlets. It also gathers SLA information from Counters and transmits it to the MIS.

5.4.4.5 LFS Database

This is a standard Oracle database. It has a "view" of the RDMC Database so that it has access to an up-to-date list of Outlets.

5.4.4.6 LFS External Interface

This uses FTMS over the communications links provided for TIP.

5.4.5 Network Banking Service (NBS)

5.4.5.1 Structure

Component	Platforms
Data Reconciliation Service (DRS) Host Application	Host Central Server
Database Links	Host Central Server

DRS Database	Host Central Server
DRS Workstation Application	MIS Client Workstation MIS Support Workstation
FTMS NWB Local Configurations	Network Banking FTMS Local Gateway
FTMS NWB Remote Configuration	Network Banking FTMS Remote Gateway
Magnetic Card Token Manual Input	Counter PC
Magnetic Card Token Validation Function	Counter PC
NBE Server Application	Network Banking Engine
NBS Authorisation Agents	NBS Agent Server
NBS Bulk File Processes	Network Banking FTMS Local Gateway
NBS Confirmation Agents	Agent Server
NBS Counter Application	Counter PC
NBS Counter Application Support	Counter PC
NBS Counter Recovery Application	Counter PC

5.4.5.2 General

NBS enables Counter Clerks in Outlets to carry out On-line banking transactions on behalf of Customers, using the Customer's magnetic swipe bankcard with authorisation for the transaction provided by the FIs responsible for the Customer's bank accounts. In effect, the Counter Clerk can act as a manually operated *Automated Teller Machine* (ATM). The Customer hands his or her bankcard to the Clerk, who swipes it through the standard Counter magnetic swipe card reader. If the card is of a type supported by PO Ltd, the Clerk is provided with a range of available transaction types including cash withdrawal, cash deposit and balance enquiry. Each of these requires On-line authorisation from the Customer's FI, and must be verified by the Customer's *Personal Identification Number* (PIN) or, pending installation of a PIN Pad in an Outlet, by signature.

The End-to-End systems supporting NBS are shown below.

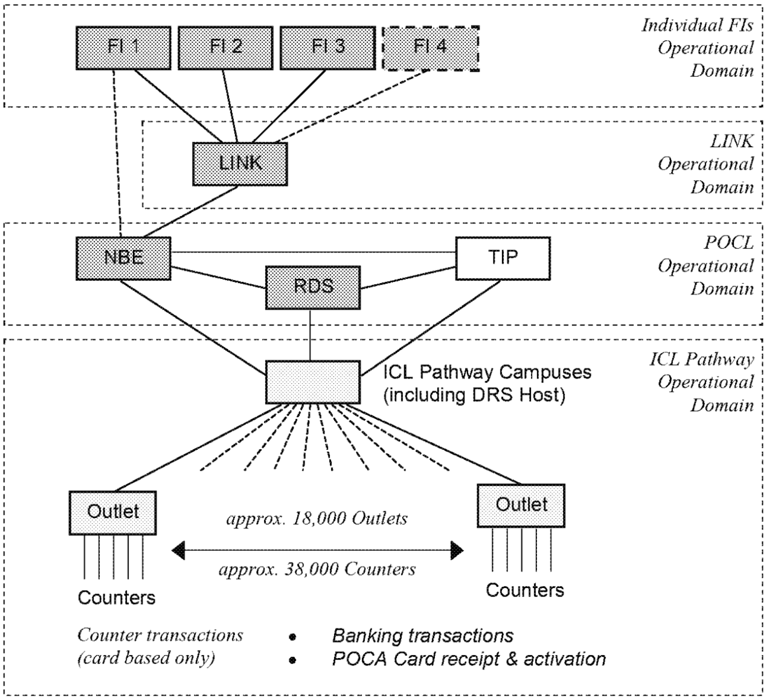
FI 1
FI 2
FI 3
FI 4
Individual FIs Operational Domain
LINK
LINK Operational Domain
NBE
TIP
RDS
POCL Operational Domain
ICL Pathway Campuses (including DRS Host)
ICL Pathway Operational Domain
Outlet
Outlet
approx. 18,000 Outlets
approx. 38,000 Counters
Counters
Counters
Counter transactions (card based only)
Banking transactions
POCA Card receipt & activation

Figure 5.20 – NBS Operational Domains

The NBE converts communications dialogues with individual Client FIs into a single set of transactions for the Horizon domain. The NBE interfaces with FIs directly or via the LINK protocol. It interfaces in a generic manner with the Horizon Campus systems.

NBS supports a set of transaction types for FIs and account types defined by PO Ltd Reference data. This enables FIs and/or transaction types to be added, modified or removed relatively speedily and with minimum disruption.

NBS depends on a number of data flows between various components of the end-to-end system shown above. The following diagram shows the major data flows, and the relationship of NBS to four external entities: the FIs, the NBE, the Post Office and the retail Customer.

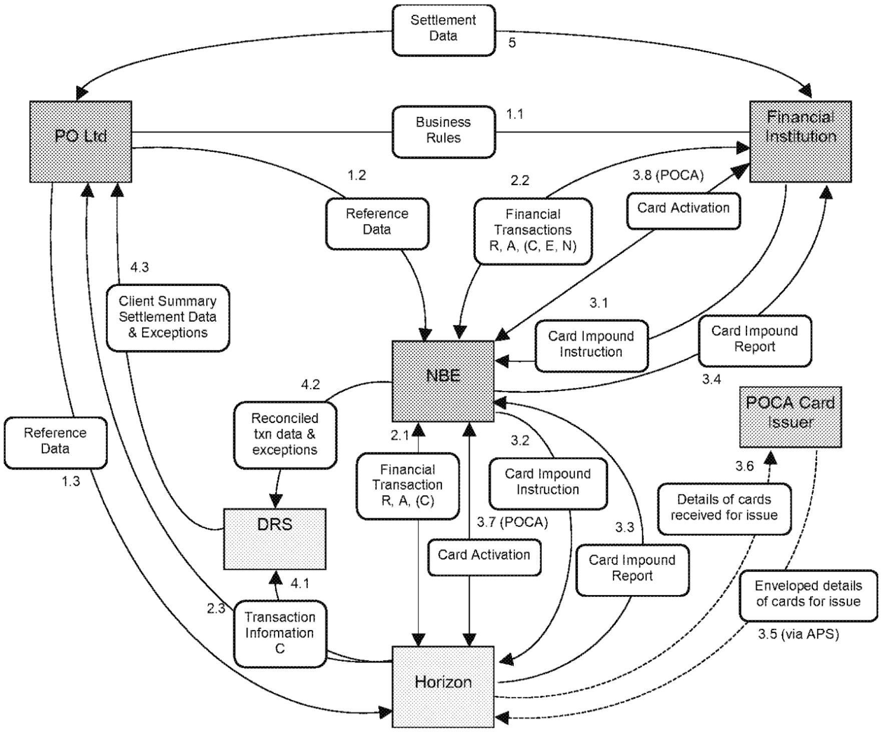

Figure 5.21 – NBS Context Diagram

The key transaction flows within NBS are defined by the "RAC" model shown below. This diagram specifies the platforms on which various processes and data stores are located.

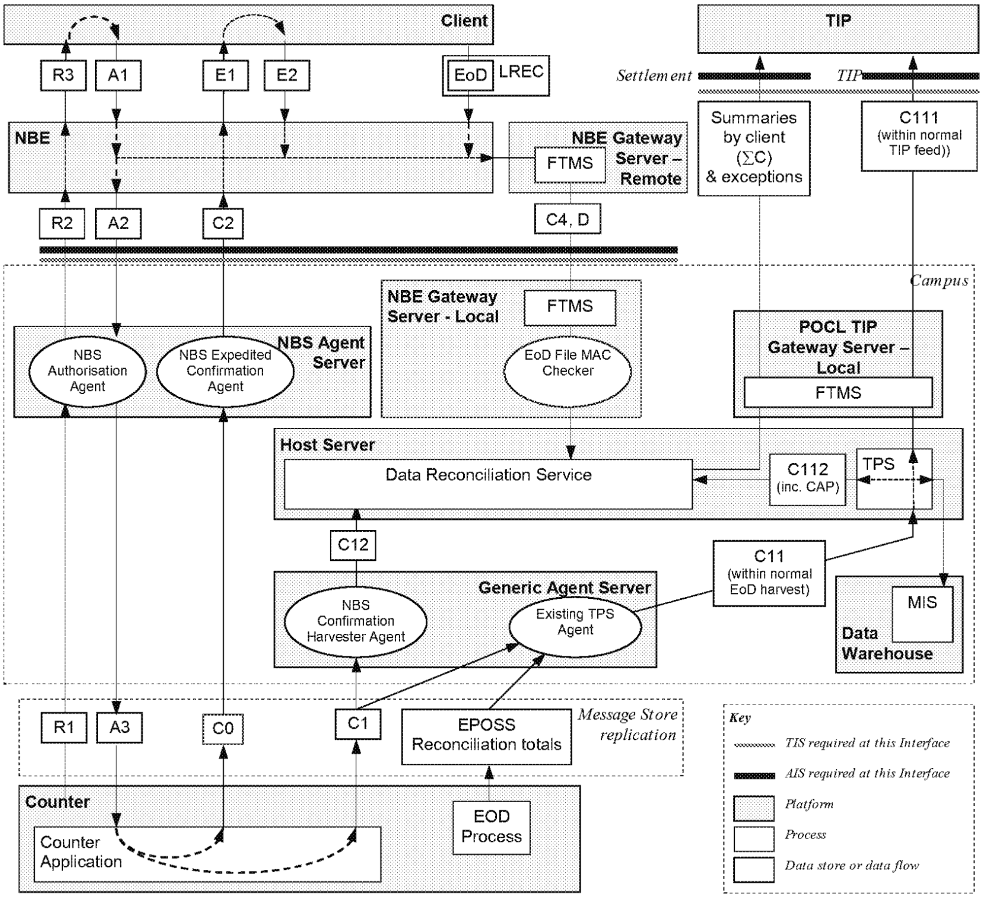
Client
R3
A1
E1
E2
EoD
LREC
TIP
Settlement
TIP
NBE
NBE Gateway Server – Remote
FTMS
Summaries by client (ΣC) & exceptions
C111 (within normal TIP feed))
R2
A2
C2
C4, D
Campus
NBE Gateway Server - Local
FTMS
NBS Authorisation Agent
NBS Expedited Confirmation Agent
NBS Agent Server
EoD File MAC Checker
POCL TIP Gateway Server – Local
FTMS
Host Server
Data Reconciliation Service
C112 (inc. CAP)
TPS
C12
C11 (within normal EoD harvest)
Generic Agent Server
NBS Confirmation Harvester Agent
Existing TPS Agent
MIS
Data Warehouse
R1
A3
C0
C1
EPOSS Reconciliation totals
Message Store replication
Counter
Counter Application
EOD Process
Key
TIS required at this Interface
AIS required at this Interface
Platform
Process
Data store or data flow

Figure 5.22 – RAC Model and Data Flows

Each transaction has three steps, each generating a separate message:

- The transaction originates as a Request [R1] at the Counter. This is written as a priority message to the local message store. The Outlet will seek an immediate connection and replicate the message to the Campus. An *NBS Authorisation Agent* processes the Request, reformatting it into the [R2] message and sends the request to the NBE
- The NBE passes the [R] to the relevant FI, and returns the resulting Authorisation [A] (*Approve* or *Decline*) to the Campus as an [A2] message. The same *NBS Authorisation Agent* will process the [A2], and write it back to the message store on the Correspondence Server as an [A3] message. This will contain timing data to the message to show how long was spent in the *NBS Authorisation Agent* and potentially other timing information, if available from the NBE, such as time spent within the NBE, and in the FI system. If no response is received from the NBE, then *the NBS Authorisation Agent* will write an [A3] message with a result code indicating that the message had timed out. The [A3] will be replicated from the Campus back to the Outlet. The communications line to the Campus remains open at least until the [A3] is received (or is timed out)
- The Counter continues with the transaction and at the end will write a [C1] Confirmation Message to the EPOSS stack showing what actually happened. This is committed to the message store at the end of the Customer session

- Should the transaction be abandoned at the Counter, other than because the Authorisation was Declined by the NBE, an immediate [C0] message is written. This is replicated to the Campus, and passed to the NBE by the *NBS Expedited Confirmation Agent*. This is configured to send the message to the same NBE partition that handled the original [R]. The NBE will transform this into a "Reversal" message and send it to the relevant FI.
- The next time that the Outlet is connected to the Campus, outstanding [C1] messages are sent to the Campus and the *NBS Confirmation Harvester Agent* writes the [C12] messages to the *Data Reconciliation Service* (DRS)

See [NBSE2ESDS].

5.4.5.3 NBS Counter Application

This supports the agreed functionality of the NBS application.

5.4.5.4 NBS Counter Application Support

This comprises a set of utilities that support the NBS application.

5.4.5.5 NBS Counter Recovery Application

This handles recovery of any NBS transaction that may have been in progress when a Counter failed or was switched off.

5.4.5.6 NBS Authorisation Agents

These handle [R] messages from Counters, and sends them to the NBE. It receives the [A] response from the NBE and sends it back to the Counter.

5.4.5.7 NBS Confirmation Agents

These take confirmed NBS transactions and write them to the DRS for subsequent reconciliation.

5.4.5.8 NBS Data Reconciliation Service (DRS)

The DRS is the component that provides reconciliation processing. It interacts with the Outlets, the NBE and Horizon central systems.

Reconciliation takes places at several levels.

- The interface to the FI is managed by the NBE, which is responsible for reconciling differences between the FIs reported positions against [R], [A] and [C2] messages passing across the NBE to Horizon interface. Confirmed (i.e. reconciled) transactions are reported to the DRS as [C4] messages. Transaction exceptions are reported to the DRS as [D] messages:
  - [D] indicates an exception or error condition
- Transaction details are forwarded to TIP based upon the reported end of day from each Outlet. The transaction details are derived from the [C1] messages. If a communications failure occurs, or other failure leading to delayed EoD reporting this flow may be delayed by (up to) several days. Existing EPOSS reconciliation measures are used to detect and report on discrepancies across this interface.

- The DRS provides reconciliation between the FI's view and the TIP view by maintaining tables of each reported transaction outcome across each interface.

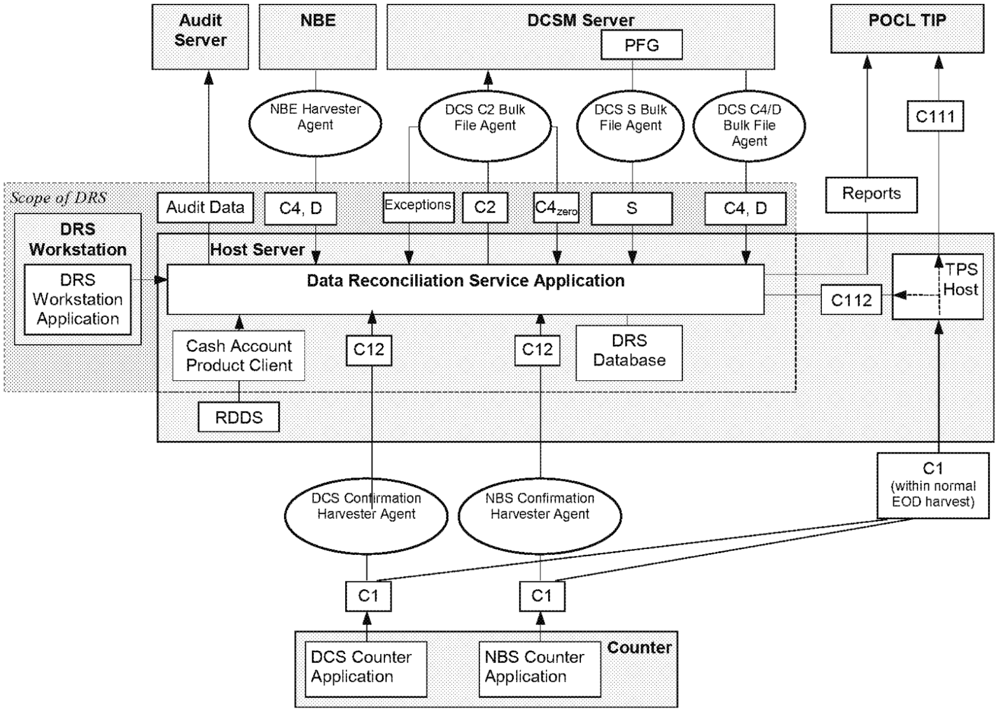

Figure 5.23 – Scope of Data Reconciliation Service

5.4.5.9 DRS Database

This Oracle database holds transactions until they are reconciled by DRS, and for 90 days thereafter.

5.4.5.10 DRS Workstation Application

This provides facilities for MSU staff to manually reconcile or write off transactions held in DRS.

5.4.6 Debit Card Service (DCS)

Component	Platforms
DCS Authorisation Agents	DCS Agent Server
DCS Bulk File Agents	DCS Management Server
DCS Confirmation Agents	Agent Server
DCS Counter Application	Counter PC
DCS Counter Recovery Application	Counter PC
FTMS DCS to TIP MID/TID Local Connection	POCL TIP Gateway Server - Local
FTMS DCS to TIP MID/TID Remote Connection	POCL TIP Gateway Server - Remote
MID/TID Allocation Database	DCS Management Server
MID/TID Allocation Service Application	DCS Management Server

5.4.6.1 General

DCS enables customers to pay for goods and services by means of a *Debit Card.* It is architecturally similar in concept to NBS, but differs from it in some important respects.

The similarities include:

- Use of the RAC model with on-line authorisation of the transaction by a third party
- Use of Reference Data to determine the card ranges supported, and their properties

Differences include:

- Authorisations are supported by signature, rather than PIN
- Authorisations are provided by a *Merchant Acquirer* (MA), using industry-standard APACS protocols. These differ from the bespoke protocols used to the NBE, and lead to a variation in the RAC model, principally to do with processing of S messages
- The interface to the MA is handled, as in industry practice, by a third party application suite. In the case of Horizon, this is the Solve/SE and Solve/PFG utilities from Retail Logic. Solve/SE handles authorisations, and Solve/PFG the subsequent generation of *Payment Files* that confirm the payments actually completed and confirmed at the Outlets.

The DCS Context Diagram is as shown here.

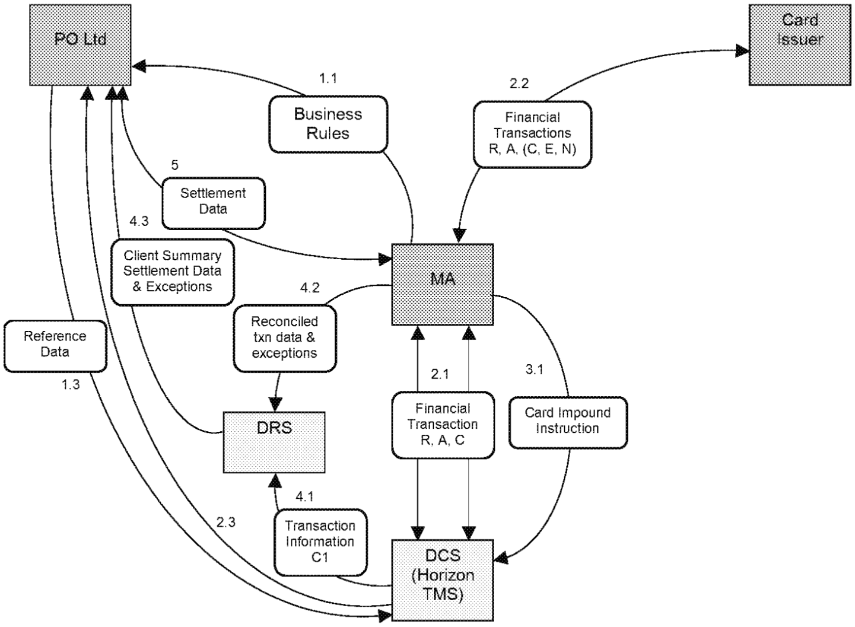
PO Ltd
Card Issuer
1.1
Business Rules
2.2
Financial Transactions R, A, (C, E, N)
5
Settlement Data
4.3
Client Summary Settlement Data & Exceptions
MA
4.2
Reconciled txn data & exceptions
Reference Data
1.3
2.1
Financial Transaction R, A, C
3.1
Card Impound Instruction
DRS
4.1
Transaction Information C1
2.3
DCS (Horizon TMS)

Figure 5.24 – DCS Context Diagram

The corresponding RAC model is shown here.

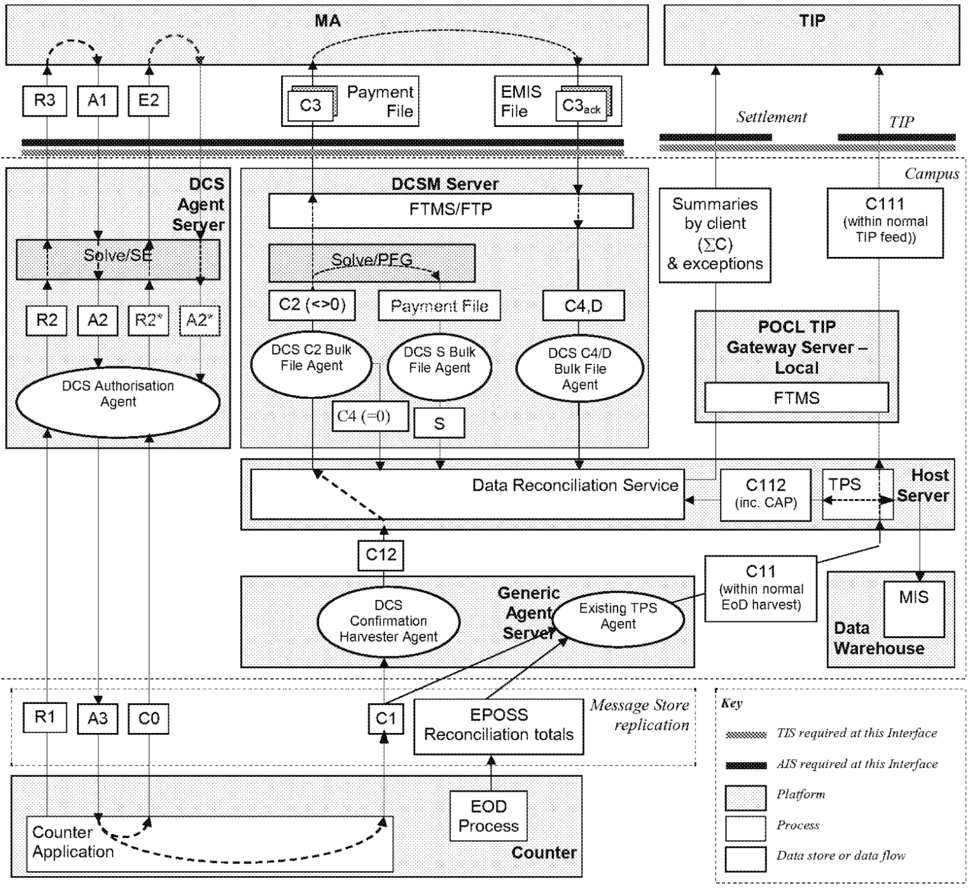

Figure 5.25 – RAC0C1 Model and Data Flows

The DCS functionality is as follows.

- The transaction originates as a Request [R1] at the Counter. This is written as a priority message to the local message store. The Outlet will seek an immediate connection (if one does not exist) and replicate the message to the Campus. A *DCS Authorisation Agent* will process the Request, and generate an [R2] message
- Solve/SE software running on the DCS Agent Server reformats the [R2] message in [APACS 30] format, and passes it to the MA. The MA may Authorise or Decline the message itself, or may pass it back to the CI. In either case, it returns an Authorisation [A] (*Approve* or *Decline*) to the Campus as an appropriate [APACS 30] response. This is processed by Solve/SE, which returns the message to the *DCS Authorisation Agent* as an [A2]. This Agent will process the [A2], and write it back to the message store on the Correspondence Server as an [A3] message. The [A3] will contain timing data to show how long was spent in the MA (and beyond). If no response is received from Solve/SE within a configurable timeout period, then the *DCS Authorisation Agent* will write an [A3] message with a result code indicating that the message had timed out. The [A3] will be replicated from the Campus back to the Outlet. The communications line to the Campus should remain open at least until the [A3] is received (or is timed out)
- The Counter continues with the transaction and at the end will write a [C1] Confirmation Message to the EPOSS stack showing what actually happened. This is

committed to the message store at the end of the Customer session. The [C1] will contain timing data to show how long was spent in the Pathway domain, and how long in all other domains. This data is used subsequently at the Data Warehouse to calculate data relating to SLAs

- A transaction can be abandoned, in accordance with defined business rules, prior to its commitment to the *Electronic Point Of Sale Service* (EPOSS) stack. If the transaction is abandoned at the Counter, other than because the Authorisation was Declined by the MA, an immediate [C0] message is written. This is replicated to the Campus, and harvested by the *DCS Authorisation Agent*. The Agent converts the message to an Explicit Reversal ([E]) and transmits it via Solve/SE to the MA. The Agent will receive a normal Acknowledgement from Solve/SE of the [E], and writes this to the message store (for audit purposes) as an [A4]
- The next time that the Outlet is connected to the Campus, outstanding [C1] messages are sent to the Campus. The *DCS Confirmation Harvester Agent* writes the [C12] messages to the *Data Reconciliation Service* (DRS), so that they can be reformatted for onward transmission to the DCSM

5.4.6.2 DCS Counter Application

This is the Counter application that supports DCS. It is developed using the same framework that supports NBS, and is largely configured by Reference Data.

5.4.6.3 DCS Counter Recovery Application

This handles any DCS transaction that may have been in progress when the Counter failed or was switched of.

5.4.6.4 DCS Authorisation Agents

This Agent is responsible for handling all [R1] messages from the Counter, and the corresponding [A2] messages returned from Solve/SE. Using the same Agent to handle both types of message enables simple monitoring of Solve/SE response times and provides the ability to timeout late responses without the need for clock synchronisation.

The same Agent also handles [C0] messages, reading them from a Riposte *Real Time Message Port*, and generates a corresponding Explicit Reversal ([E]) message to Solve/SE.

5.4.6.5 DCS Confirmation Agents

The *DCS Confirmation Harvester Agent* harvests [C1] messages as they are received from the Outlets and to passes them to the DRS, from whence they are eventually passed to the MA in a *Payment File*. As with NBS, it uses continual interactive harvesting with a checkpointed message port. This technique uses bulk inserts into Oracle, and co-ordinates checkpoints with Oracle commit units.

5.4.6.6 DCS Bulk File Agents

A number of pseudo-Agents run at the Host layer and carry out processes that involve the DRS.

- *DCS A3 Harvester Agent* reads all Approved [A3] messages and writes them to the DRS for later "Orphan A" analysis. Its operation will be similar to that of the *DCS Confirmation Harvester Agent*, the only difference being the class of messages harvested.
- *DCS C2 Bulk File Agent* takes [C2] files generated by the DRS on a periodic basis and produce transaction log files ready for processing by the Solve/SE PFG application.
- *DCS S Bulk File Agent* is responsible for loading the Payment File and generating appropriate [S] messages for each Payment File transaction. These messages are written to a single file and passed to the DRS.
- *DCS C4/D Bulk File Agent* is responsible for handling all Confirmation acknowledgement messages ([C4]) and Discrepancy messages ([D]) from the DCSM and passing them to the DRS. Data is transmitted in a file derived from the EMIS file.

5.4.6.7 MID/TID Allocation Service Application

Merchant Acquirers require that each Outlet of a merchant (in this case, PO Ltd) is allocated at least one unique identifier (Merchant ID) by their MA. Each MA will require a different set of MIDs.

In addition, each Counter offering DCS functionality must be allocated a unique identifier (Terminal **ID**). The TID will be common across all MAs, but can only be associated with one MID per MA. Solve/SE uses Source **ID**s (SIDs) to map a specific TID to the different MAs' individual MIDs. The SID is derived by the DCS Authorisation Agent.

Pathway manages the MID/TID allocation, using MID/TID values provided by Streamline Merchant Services and Outlet information provided by OCMS. The allocation is made by a MID/TID Allocation Database and information is passed to PO Ltd via the standard TIP physical links and a specific FTMS service.

5.4.6.8 MID/TID Allocation Database

This SQL Server database supports the allocation of MIDs and TIDs to Outlets and Counters.

5.4.6.9 DCS Solve Configuration Generation Utility

Configuration data required by Solve/SE is generated by a Pathway-developed utility using a number of standard templates and other files provided by Retail Logic, as well as input from the MID/TID Allocation Database. The structure is as shown here.

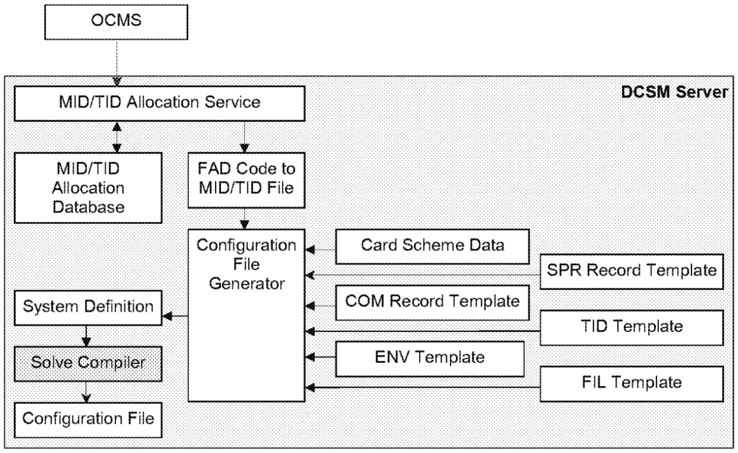

Figure 5.26 – Solve/SE Configuration File Generation

5.4.6.10 DCS Transaction Log Obfuscation Utility

Transaction logs and other files generated by Solve/SE contain sensitive data, i.e. information that could (possibly in conjunction with other relevant data) be used to contravene the Data Protection Act or to execute a fraud. This information is obfuscated when no longer required in files that are used for long-term audit purposes.

5.4.6.11 DCS Operational Utilities

A number of processes are required to enable support staff to manage the operation of DCS. In general, these are outside the scope of an SDS, but in this case some of the necessary processes require software developments to support them. These include the following.

- A process, and underlying utility, to switch the Transaction Log and error log files used by Solve/SE on a periodic or immediate basis
- A process, and underlying utility, to verify that the Payment File is complete and consistent following a Solve/PFG run. This will be invoked by Maestro schedule after the PFG process runs

5.4.7 Mails

5.4.7.1 General

This is an Escher product that is driven by Reference Data and provides all facilities related to the handling of mails products in Post Offices.

5.5 OTHER APPLICATIONS

5.5.1 Auto-Configuration Service

This is an SQL Server application, and is driven by Auto-Configuration Client PCs with an appropriate client application. The Auto-Configuration application runs under the control of the Maestro scheduler and feeds information into the Boot Server when new Outlets are about to be installed.

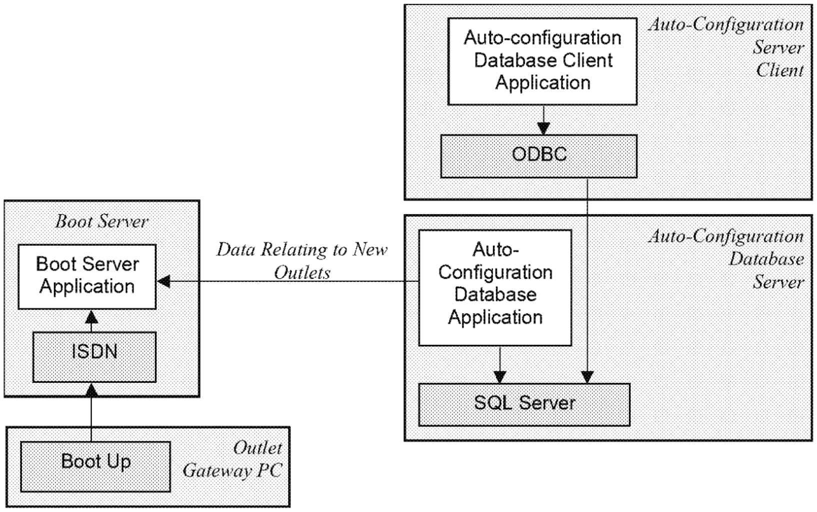
Auto-configuration Database Client Application
Auto-Configuration Server Client
ODBC
Boot Server
Boot Server Application
Data Relating to New Outlets
Auto-Configuration Database Application
Auto-Configuration Database Server
ISDN
SQL Server
Boot Up
Outlet Gateway PC

Figure 5.27 - Auto-Configuration Service

5.5.2 Encryption Facilities

5.5.2.1 Bespoke Crypto Facilities

5.5.2.1.1 Structure

Component	Platforms
Atalla Key Loading Software Tool	Atalla Card Loader Workstation
CAPU Check Handler	Agent Server Counter PC KMA Server KMA Workstation POCL TIP Gateway Server - Local
Core Signing Functions (CSF)	Agent Server AP Client Gateway - Remote Audit Server Auto Configuration Signing Server CM Signing Server Counter PC DCS Agent Server NBS Agent Server Network Banking FTMS Remote Gateway Outsourcing Software Depot Pathway Software Depot PIN Pad Key Generation Workstation POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote
Core Verifying Functions (CVF)	AP Client Gateway - Local Counter PC Counter PC - Mobile Counter PC - Non-Gateway Network Banking FTMS Local Gateway Outsourcing Software Depot Pathway Software Depot
Crypto API for Network Banking	NBS Agent Server Network Banking FTMS Local Gateway
Crypto Keystore Service (CKS)	Agent Server AP Client Gateway - Local AP Client Gateway - Remote Audit Server

	Auto Configuration Signing Server Boot Server CA Workstation CM Signing Server Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation NBS Agent Server Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway PIN Pad Key Generation Workstation POCL Standby Gateway - Remote POCL TIP Gateway Server - Local
Cryptographic Functions API	Agent Server CA Workstation Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation NBS Agent Server Network Banking FTMS Local Gateway Outsourcing Software Depot Pathway Software Depot PIN Pad Key Generation Workstation Staging Server
Entropy Generation Application (EGA)	CA Workstation KMA Server KMA Workstation Offline Key Generation Workstation
File Encrypt/Decrypt Library (glued)	Audit Server SSC Support Server
File Sign/Verify Library (glued)	AP Client Gateway - Local AP Client Gateway - Remote Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway Outsourcing Software Depot POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote
PMMC Agent PMMC Common Library	Counter PC Agent Server CA Workstation Counter PC KMA Server KMA Workstation Offline Key Generation Workstation
Siemens Metering Counter Siemens Metering Offline TeamWARE Crypto (TWC)	Counter PC Offline Key Generation Workstation CA Workstation Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation Support Support Access Server

5.5.2.1.2 Layer7

Component	Platforms
Layer7	Agent Server AP Client Gateway - Local AP Client Gateway - Remote Audit Server Auto Configuration Signing Server Boot Server CA Workstation CM Signing Server Counter PC DCS Agent Server DCS Management Server

KMA Server
KMA Workstation
NBS Agent Server
Network Banking FTMS Local Gateway
Network Banking FTMS Remote Gateway
Offline Key Generation Workstation
Outsourcing Software Depot
Pathway Software Depot
PIN Pad Key Generation Workstation
PIN Pad Proving Workstation
POCL Standby Gateway - Remote
POCL TIP Gateway Server - Local
POCL TIP Gateway Server - Remote

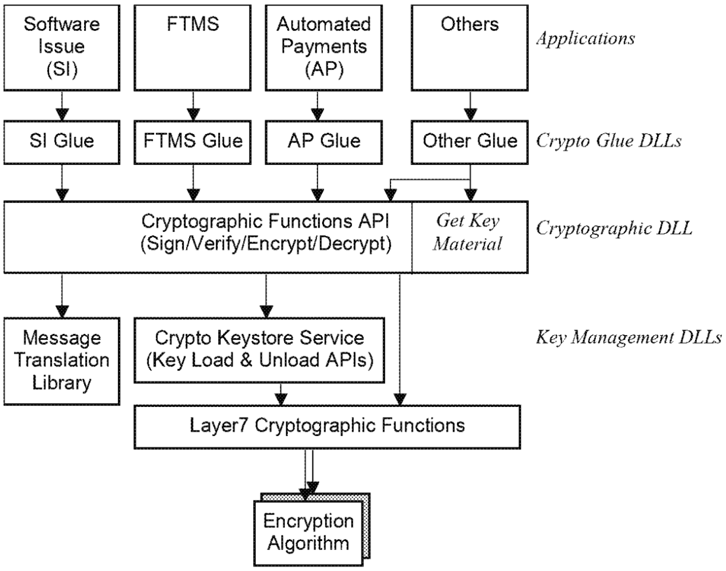

Figure 5.28 - Cryptographic Architecture

5.5.2.1.3 Layer7 Cryptographic Functions

Layer7 from Sapher Servers Ltd can invoke a number of different crypto algorithms, depending on the function called, including a CESG-approved implementation of the Red Pike algorithm, which is used for protection of RESTRICTED material. Layer7 is used on a number of Platforms, and for a number of purposes. These are outlined in Chapter 16 "Security".

5.5.2.1.4 Cryptographic Functions API Library

System components requiring to either encrypt or decrypt some data, or seal a message, or verify a message seal, call on a standard *Cryptographic Functions API Library*. This invokes a function-specific *Key Management APIs* that obtain and maintain the Key sets appropriate to the application.

Actual encryption is carried out by the Layer7 code.

5.5.2.1.4.1 File Encryption Libraries

Older applications access a set of "glued" libraries that provide access to the crypto APIs.

5.5.2.1.4.2 *Generating and Verifying Signatures*

Signing is used as a message protection device for messages passing to and from AP Clients. Verification is used to check the signature on an object. Verification needs to take into account the *Latency* of the signature, or the time between it being signed and the signature being verified.

Signature generation and verification are performed by standard library procedures (the *Core Signing Functions* and *Core Verifying Functions)* that may be called by Agent and Counter applications. The libraries can handle arbitrary messages of any length, and treat them as binary streams.

Signed messages or message portions are inserted into Riposte messages with an appropriate surrounding attribute grammar by the Agent or Counter application.

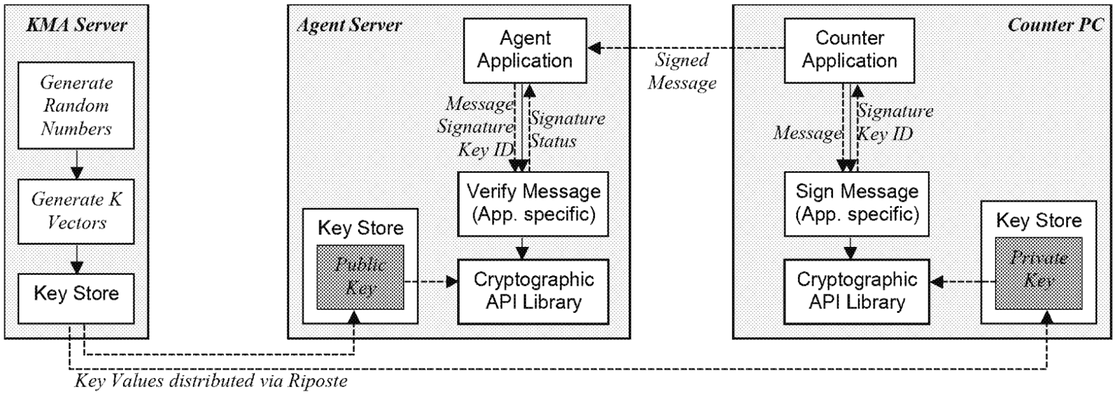

Figure 5.29 - Message Signing

5.5.2.1.5 PMMC Agent

This is an Agent running on the Counter PC, that handles the interface between the POLO start up facilities and the Riposte Message Store. It also provides facilities to enable an “unattended reboot”, where this is required by software distribution facilities.

5.5.3 Key Management

5.5.3.1 KMS Data Feeds

Keys are generated as required, for example for newly installed Outlets, according to a data feed sent to KMS by Tivoli ten days before the Outlet is due for installation. The same data feed can also indicate Outlets that have closed. This data feed is described in [KMADF].

5.5.3.2 Key Generation and Storage

They are generated and held in a Key Management Application database that is architecturally equivalent to a Host. The Key Management Application (KMA) runs on an SQL Server database. It is accessed by a KMA Workstation that, for example, permits the Key Custodian to revoke Keys. The functionality provided by KMS is outlined in Chapter 16 "Security" and described in [KMAHLD].

5.5.3.3 Key Distribution

Keys are distributed when required by a set of *Key Management Agents* that extract new key material from this database and transmit it, via Riposte, to the relevant Platform.

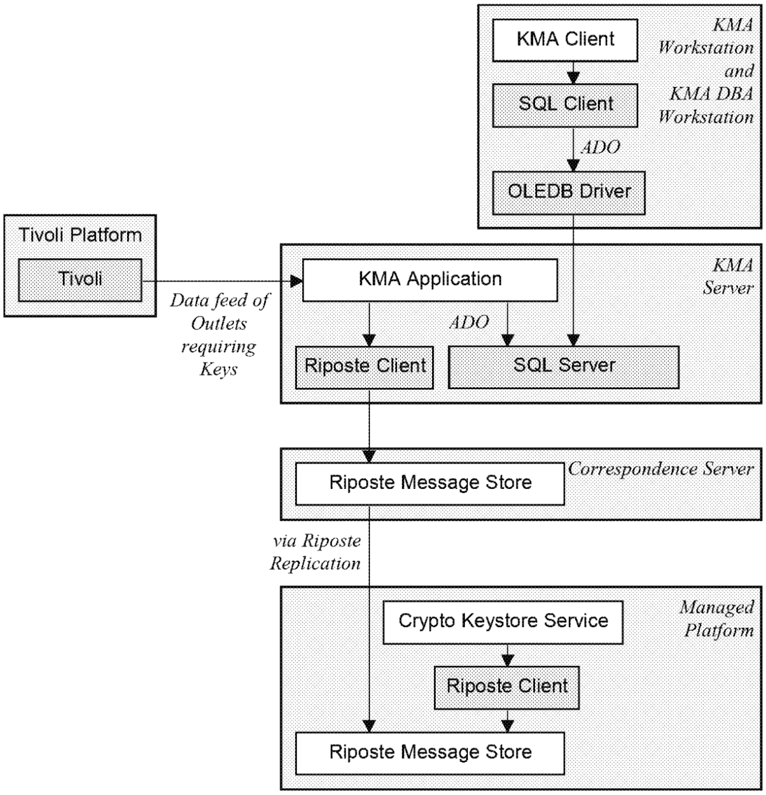

Figure 5.30 - Key Management Application

5.5.3.3.1 Crypto Keystore Service

Each Platform that is involved in encryption or decryption operations has a Riposte Client service running on it. A *Crypto Keystore Service* is provided on each relevant platform to enable the Key Management client applications to obtain new key sets, or revocation instructions, from Riposte as and when the appropriate messages arrive.

5.5.3.4 Generating Entropy

Generating Crypto Keys requires a large random number (typically 160 bits). These numbers are generated by an *Entropy Generation Application* (EGA) that invokes a hardware-based Random Number Generator within the Key management Server.

5.5.3.5 POLO Recovery

The *POLO Process* requires the Post Office Manager to use a token (the *Post Masters Memory Card* (PMMC)) and specify a PIN. If the PIN or token is lost, the Post Office manager calls the HelpLine, as described in Chapter 4 “Overview”. The Help Desk Operator can initiate a process whereby the Key Management application delivers the Recovery Key to the Outlet. A Key Management GUI is available on selected Horizon

Help Desk Terminals. This has access to the KMA Server, and can use the recovery information stored there to recover the Key for the Post Office Manager.

5.5.4 Performance Management System

Chapter 15 “Performance” assesses the capacity requirements for the principal system components and their major resources.

Capacity Management provides the means to detect when particular resources are overloaded or are soon likely to overload. Pre-defined criteria are used to monitor individual resources. An example could be the “per cent allocated of a named drive”. When the criterion is met, it can take a defined local action and/or generate an event.

The *Performance Management System* (PMS) gathers performance information from major components of the Horizon system, and analyses and presents it to CS for review and action.

5.5.4.1 Purpose

Performance management focuses on the production system and includes:

- Monitoring of systems, databases, networks, applications, etc
- Support facilities to pinpoint and diagnose performance problems
- Current performance analysis & reporting
- Historic performance analysis & reporting
- Analysis & reporting of performance trends
- Future performance including the changes to the workload resulting from the implementation of new services

Its aim is to ensure that the production system behaves as expected and continues to provide the required level of service.

See [PMSSOD].

5.5.4.2 Structure

Component	Platforms
FTMS PMS Local Connection Configuration Metron Athene Acquire - Dynix Performance Management	Capacity Management Server Data Warehouse Server Host Central Server
Metron Athene Acquire - NT Performance Management	ACDB Server Agent Server
Metron Athene Acquire - NT Performance Management	AP Client Gateway - Local AP Client Gateway - Remote Audit Server Correspondence Server Counter PC DCS Agent Server DCS Management Server General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote KMA Server NBS Agent Server Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway OCMS Server POCL TIP Gateway Server - Remote SMDB Server SSC Support Server VPN Exception Server

	VPN Policy File Management Server VPN Server
Performance Management Analysis Tools	SSC Support Workstation
Performance Management Database (PMDB)	Capacity Management Server
Performance Management Package "Athene"	Capacity Management Server Short-term Performance Database Server

5.5.4.3 Architecture

The PMS uses the Athene software from Metron systems.

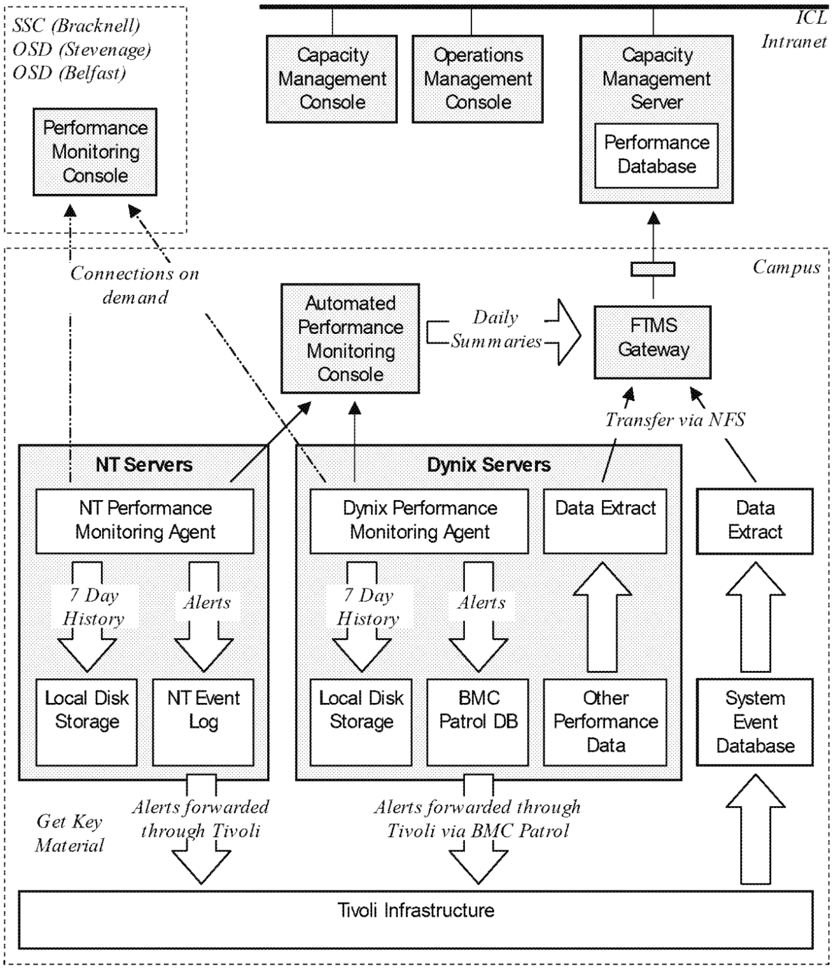

Figure 5.31 – Performance Management Service

5.5.4.3.1 NT Performance Monitoring Agent

An agent runs on each NT server platform and collects any relevant performance statistics. This is kept in a historical log that, by default, includes the last seven days' data. Existing platform performance metrics interfaces are used wherever possible. Any divergence from expected performance is logged as events in the NT Event Log, and is collected from there by the Tivoli event collection mechanisms.

5.5.4.3.2 Dynix Performance Monitoring Agent

A similar agent runs on the Sequent Dynix platforms and collects performance information. Alerts are forwarded to Tivoli via the BMC Patrol subsystem. Historical data is kept in filestore.

5.5.4.3.3 Data Extract

Data extract facilities are provided to take information from the performance databases on each managed platform and forward it to the external Performance Database Server.

5.5.4.3.4 Performance Monitoring Console

Authorised users within the Pathway secure network can view real-time performance information on these consoles. They can also start and stop the agents, and vary their configuration profiles (for example the thresholds for generating alerts). They can also export data on diskette for analysis by third parties.

5.5.4.3.5 Capacity Management Console

Users outside the Pathway secure network can view historical performance information on this console and use the Analysis tools to analyse it.

5.5.4.3.6 Capacity Management Server

This server holds a database of historical performance information. It also supports a range of analysis and reporting tools. Facilities are provided to subset data and to view data from different sources concurrently.

5.5.5 Outlet Monitoring Service (OMS)

5.5.5.1 General

This service is used to monitor the connection times of Outlets, and report on any that are out of contact with the Campus for a reasonable period of time.

5.5.5.2 Structure

Component	Platforms
Counter Network Information Monitor	Counter PC
Service Management Database (SMDB)	SMDB Server
TMS Outlet Monitor Agents	Agent Server Correspondence Server

5.5.6 Office Applications

There are some situations where applications or their users need access to straightforward office applications such as document processors, spreadsheets or simple databases. In line with Fujitsu Services' alliance with Microsoft, these needs are satisfied by members of Microsoft's Office 97 suite.

5.5.6.1 Structure

Component	Platforms
Microsoft Access	Audit Server SecurID Admin Workstation
Microsoft Excel	OCMS Client

Microsoft Office 2000 SR1	CA Workstation KMS Admin Workstation
Microsoft Office 97 Microsoft Office 97 Professional	SSC Support Workstation Audit Workstation MIS Client Workstation MIS Support Workstation RDMC Administrator Workstation
Microsoft Office 97 SR2	Audit Workstation MIS Client Workstation MIS Support Workstation RDMC Administrator Workstation SecurID Admin Workstation
Seagate Crystal Reports (Professional)	KMA Workstation KMS Admin Workstation

5.5.6.2 Microsoft Word 97

This is used for document preparation and amendment.

5.5.6.3 Microsoft Excel 97

This is used for spreadsheet applications.

5.5.6.4 Microsoft Access 97

This is used for simple database applications.

5.6 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 4	Overview of the Horizon Architecture	Provides an overview of the technical infrastructure which supports and constrains the applications that provide services to Pathway's customers
Next	Chapter 6	Distributed Application Services	Discusses the mechanisms that enable application components to be distributed across two or more Platforms
FTMSE	TD/DES/107	File Transfer Managed Service at CSR+	Describes the ways in which FTMS services are constructed and used
GENAPI	TD/STD/004	Generalised API for OPS/TMS	Describes in detail how an application should be prepared for integration into the Horizon system.
HADDIS	TD/STD/001	Host Applications Database Design and Interface Standards	Defines the standards used in the design and development of Oracle based Host applications.
KMAHLD	RS/DES/018	KMA Design	Describes the functionality and construction of the Key Management Application

Further Chapters in this Document elaborate on the infrastructure services made available to applications or on the constraints that are imposed on application designs.

Chapter 6 - Distributed Application Services

6.1 SCOPE

This Chapter thus discusses the mechanisms that enable application components to be distributed across two or more Platforms.

Distributed Application Services cover the construction, integration and operation of large-scale systems, composed of separate application systems (or other autonomous application components) linked together. This integration must be able to adapt to multiple standards, components from different suppliers and differences in location, environment and system qualities.

The mechanisms used include the following.

- Riposte Message Service (RMS). This is used to distribute messages from the Campuses to Outlets, and return the results of transactions to the Campus. Riposte is also used for Crypto Key distribution
- Remote Procedure Call mechanisms. These enable applications to communicate with each other even though they run on different Platforms
- Distributed Database facilities such as SQL*Net from Oracle
- Shared filestore mechanisms
- Transaction control mechanisms for on-line access from external sources.

File Transfer mechanisms are also used, but are not considered in this Chapter.

6.2 DISTRIBUTED APPLICATION SERVICES REFERENCE MODEL

This shows the main components of the Reference Model. In practice, few technologies exist which illustrate all the major features of the ISO model for distributed application support. (CORBA, used to support the Tivoli environment, is one of the few that do.) Most of the technologies used are chosen for their availability and relevance to the technical needs of the solution, rather than for their architectural completeness.

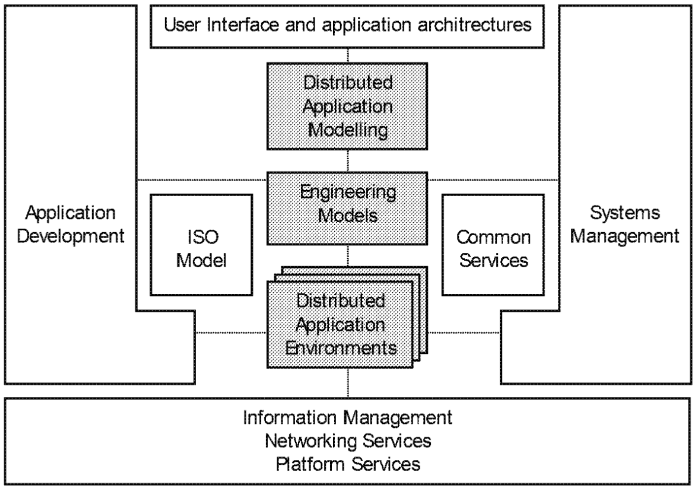

Figure 6.1 - Distributed Application Services

6.3 Remote Procedure Call

This technology enables an application to make a call on another application, without needing to know which Platform the called procedure is running on. It provides for the calling procedure to be compiled with a “stub” that points to the called procedure. When the calling procedure is loaded, the stub is used to complete the link.

6.3.1 Classes of RPC Call

There are two classes of RPC:

- local RPC
- non-local RPC

Local RPC is used where the called procedure presents an RPC interface, but the calling procedure knows that it resides on the same Platform as the called procedure and thus can use a very lightweight protocol. Non-local RPC is the full-strength protocol used where the called procedure may be on the same of a different Platform.

6.3.2 Use of RPC

RPC is used between Windows NT Platforms, for example from Agent Server to Correspondence Server.

6.3.3 RPC Locator

Where a particular function is supported by a system component that may be replicated for resilience or performance reasons, the calling process should not and need not know which particular instance of the called component will handle the call. This is the case, for instance, where an Agent process invokes a Correspondence Server by RPC. A number of Correspondence Servers are used, depending on the message load, and the call from an Agent may be handled by any Correspondence Server within the Outlet’s Cluster.

A mechanism known as an "RPC Locator" is used to ensure that the call is handled by a competent application. The compiled version of the calling procedure includes a "stub" which identifies the called procedure and, when invoked, directs the call to the Redirector service. This passes the call to an appropriate target system, for example on a round robin basis.

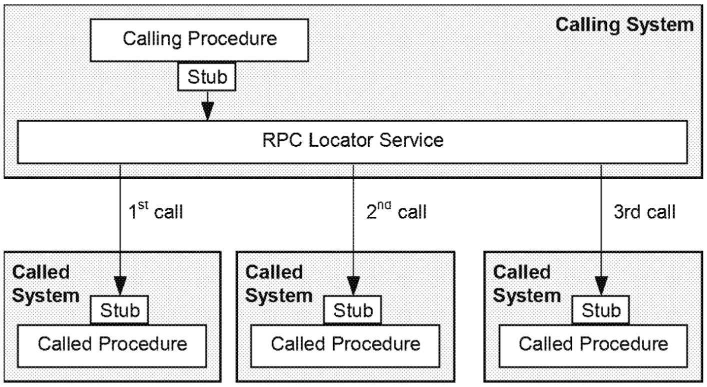

Figure 6.2 - RPC Locator Service

Note that, for reasons to do with resilience and the use of Riposte Clusters, Agents do not use RPC Locators in their normal running. The LUC mechanisms do use RPC Locators in their initial set-up, but subsequent calls are sent directly to the proper Correspondence Server using the information retrieved by LUC.

6.3.4 RPC Fault Management

The major difficulty with systems that use RPC calls for inter-system interworking is that the call may not return. This may happen for a number of reasons: for example, there are no servers with the called service running, or the called service fails, or the network between the calling and called systems is unavailable.

There is no simple answer to this problem. It is mainly an issue for Agents, and hence a work-around is used in the Agents. When these call upon the Correspondence Servers by RPC, the time-out value on the call is set to a low value (say one minute). When the call returns, if the result code indicates a time-out, then the Agent immediately repeats the call.

6.4 SOCKETS

These provide a means for one application to pass data to another, without needing to know in detail where the second application is located. The message is passed to a specified TCP/IP address and port number, and the receiving application listens on this combination for any incoming traffic.

These mechanisms underlie many of the other communication mechanisms described in this Chapter. Both Riposte and Tivoli use named sockets for inter-platform communication.

The port number is a 16-bit value. A number of port number values have specific and conventional meanings agreed by RFC. Applications wishing to use their own port numbers must ensure that they do not encroach on any of these, and (perhaps more importantly) on the application-specific port numbers used by other applications.

Specific port numbers are used by the following UDP and TCP services.

- Riposte (2995)
- Riposte mirror (2996)
- Tivoli

6.5 RIPOSTE

Riposte (*Retail Integrated Point of Sale Transaction Environment*) is both a set of applications and a messaging infrastructure (or "middleware") that supports the distribution requirements of these applications between the Counter PCs and the Correspondence Servers at the centre.

6.5.1 The Riposte Message Server

This provides a highly resilient, fault tolerant, high performance distributed messaging system. It receives messages from the Central systems and distributes them to the appropriate Outlets. Conversely, it receives messages from each Outlet and makes them available to the Central systems. In doing so, it optimises the communications links from the Campuses to the Outlets. All messages are stored within the RMS for a period determined by their individual expiry period.

Expiry periods should be set by the application, depending on the type of message. Default values are as follows:

Default maximum:	100 days
Default minimum:	10 days
Default object:	10 days

In practice, 35 days is usually used as this spans a three-week Cash Account period.

6.5.1.1 Riposte Groups

The Counter PCs within a single Outlet are defined as being part of a *Riposte Group*. The Group is represented within four Correspondence Servers, two at each Campus. Each Correspondence Server will be part of many Groups.

6.5.1.2 Riposte Client

Counter PCs and Agent Servers include the *Riposte Client* software. This offers a set of APIs that enable applications to obtain messages from the RMS, and write messages to it.

6.5.1.3 Message Replication and Synchronisation

When a message is created on one member of a Group, it is stored locally and then automatically distributed to all other members of the same Group. When a new member joins a Group, it automatically brings itself into line with the other members of the Group. (In the case of Counter PCs, a progress indicator is displayed on the desktop while this takes place.)

This co-ordination is achieved by the frequent interchange of Markers between the Group members.

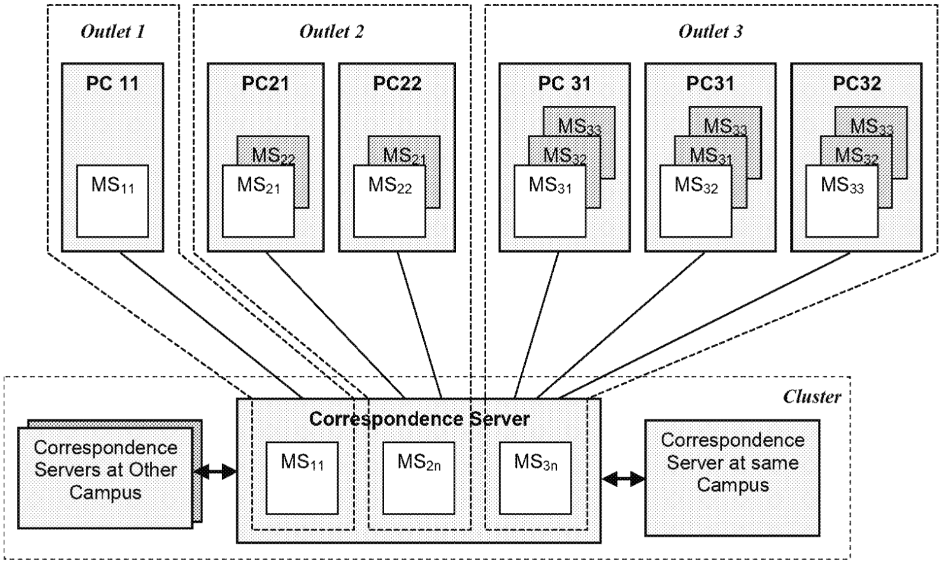

Figure 6.3 - Riposte Message Store Co-ordination

This diagram shows three Outlets: one with one, one with two, and one with three Counters. The messages belonging to the three-counter Outlet (MS_{31}, MS_{32} and MS_{33}) are replicated within each of the other Counter PCs at that Outlet, as well as in the Correspondence Server to which the Outlet connects. Unless the Outlet has a permanent connection, this latter replication is not instantaneous but happens the next time that the ISDN link to or from the Outlet is established. The frequency with which Counters synchronise with the Correspondence Servers is a configurable parameter that is set to balance between call costs, the response times required to real time messages, and the need to minimise the amount of lost data should an Outlet be damaged beyond repair.

Message stores contain the messages generated at the Counters, as well as messages generated at the Correspondence Servers and directed to that Outlet. Any message generated by a member of a Group will eventually appear in every other member of the Group.

Riposte APIs are provided to define which Counters form part of a Group, or to change the membership of a Group.

This method of message replication conceptually has the advantage that there is no need for backup procedures, media or devices to secure the message store. It provides seamless, unattended recovery following the failure of any Correspondence Server or Counter PC once this is repaired or replaced. In practice, such recovery can be exceedingly slow, and Correspondence Servers are backed up in to tape at regular intervals.

6.5.1.4 Riposte Clusters

Each Group is theoretically known to every Correspondence Server. The replication process could copy all messages to all Correspondence Servers, but this would raise two performance-related issues:

- Each Correspondence Server would need enough filestore to hold the entire peak Message Store for all known messages and Collections.
- Correspondence Servers would spend most of their time doing message replication.

To avoid these, the total set of Correspondence Servers is divided into a set of *Clusters*, so that each Group appears in two Correspondence Servers, one at each Campus. Normal message replication is confined to the members of the Cluster. Each Correspondence Server need only hold the message stores corresponding to the Groups that are in its Cluster.

Where an Agent or Counter Application needs to write a Riposte message to another Group, it does not know whether this is in the same Cluster or not. The supporting Multi-Riposte library calls the LUC Server discussed in Chapter 5 “Application Architectures”, which returns the identity of the Cluster to which it relates. Multi-Riposte then sends the message to the appropriate Group.

Riposte now includes facilities that can remove the need for the clustering and hence for LUC. These facilities can be used to nominate which Correspondence Servers a Group is to reside in, and replication will then be limited to this set. Message passing to and from Agents will be routed automatically by Riposte to an appropriate Correspondence Server that contains the target Group. This strategy would require some major reworking to the Agent strategy, as the Correspondence Servers will appear as a single resource. For example, the use of parallel Agent instances within each Cluster, for performance reasons, will need reviewing.

6.5.1.5 Message Transfer

Messaging between Riposte instances uses *User Datagram Protocol* (UDP) over the *Internet Protocol* (IP). This is a very efficient mechanism, but has no acknowledgement feature. Any failures are detected by next Marker exchange. Riposte requests the retransmission of any missing messages.

6.5.1.6 Priority Messages

Priority Messages are used by applications that need to make an immediate communication with a remote neighbour. An example is a Foreign Encashment, where it is necessary to determine at once if there is a "stop" on an Order Book, rather than wait for the regular synchronisation between Outlet and Campus.

A Priority Message causes the communications link to be opened, and is then sent immediately. It is sent again at its normal position in the message run.

An implication of the use of UDP is that Priority Messages may sometimes be lost. However, the message synchronisation processes will ensure that they are transferred eventually, though possibly not with the desired urgency.

(Messages that are out of sequence the “wrong way” indicate a major failure such as a platform masquerading as a different Riposte node. Riposte closes down the offending message service and this must be manually recovered.)

6.5.1.7 Real Time Message Ports

Real Time Message Ports (RTMPs) are similar to Priority Messages, in that the ISDN line is opened immediately if it is not already open. They differ in that the message sent over the RTMP is sent first, and *followed* by any other outstanding messages.

6.6 DISTRIBUTED DATABASES

6.6.1 Oracle

Oracle is described in Chapter 7 "Information Management". It is used primarily in a client-server paradigm, where the database itself is located on one Platform but client software on other Platforms provides access to that database in a controlled way.

6.6.1.1 SQL*Net

This is a mechanism used by Oracle client-server applications and for server-to-server communication. It hides the details of the underlying communications protocols.

SQL*Net is mostly used to support Agent processes that need to communicate with Host databases, as described in Chapter 5 “Application Architectures”. The overall structure is shown here. It also supports the *database links* between databases which are discussed in Chapter 7 “Information Management”.

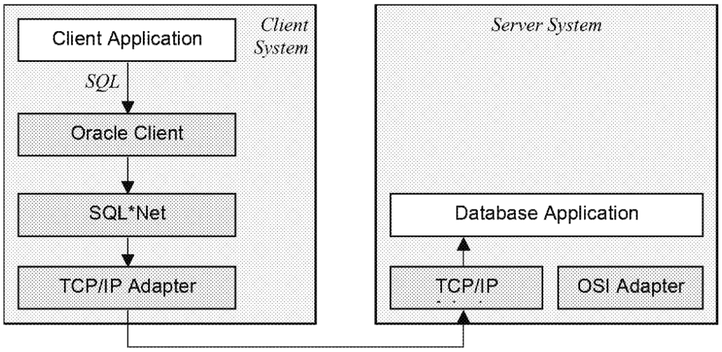

Figure 6.4 - SQL*Net Structures

6.6.1.2 PL/SQL

This is a Procedural Language for Oracle databases.

6.6.1.3 Oracle Forms

This provides a form-based mechanism to interrogate or modify data in an Oracle database. It is described in more detail in Chapter 8 "User Interface"

6.7 TRANSACTION MANAGEMENT

6.7.1 General

Transaction Management is the process of allowing a set of related actions to be carried out in such a way that either they all complete, or they are all considered not to have started. This can be achieved by a number of different protocols. The essential feature is that the application needs to be able to declare the *start* of a transaction sequence, and then subsequently it *commits* all the actions carried out within it. If it fails to commit the transaction, then all the actions carried out are *rolled back* and deemed not to have happened.

A transaction can fail for a number of reasons. For example, the Platform may fail before it completes, or it may fail to obtain one of the resources it requires - for example because it is locked by another process.

Transactional integrity is usually guaranteed by a *two-phase commit. W*hen all the services involved reach a point at which they are ready to commit, they then agree to commit, and subsequently confirm to each other that they have committed. Should any of the Platforms fail to commit the transactions, then all the Platforms involved roll it back.

6.7.2 Riposte Transactional Integrity

Riposte provides the means for an application to generate a sequence of messages that are deemed to be part of a single transaction. The implication is that another process must be able to read all of them, or none of them.

The replication process understands the *start transaction … end transaction* Markers in the message store. It does not begin replication of the messages until the *end transaction* Marker arrives. An application cannot read the first message in a transaction until all the component messages are securely replicated.

6.7.3 Agent Co-ordination of Oracle and Riposte

Transactional integrity is not assured anywhere else.

Agent Servers need to co-ordinate the updates that they make to a Host System (via Oracle client calls) with those they make to the RMS (via RPC calls). Agents must be designed so that they duplicate data, rather than ignoring it, following a failure. Both Hosts and Counters are designed to accept that some data may be duplicated but none will be lost.

6.8 CORBA

This sub-section is included for completeness.

The *Common Object Request Broker Architecture* (CORBA) is a set of object oriented support mechanisms which are used primarily to support the Tivoli Management Environment (see Chapter 12 "Systems Management").

There are no plans to use CORBA facilities directly.

6.9 SHARED FILESTORE

A common method of data sharing is *shared filestore*, where a file or directory on one Platform is explicitly made available to designated users on another. It is most useful where the receiving Platform does not store the file in its original form, but transforms it or forwards it to a third Platform.

6.9.1 Windows File Sharing

Windows NT Servers and workstations may make any part of their filestore accessible to users on other Platforms within their own Domain or Workgroup. The other Platform accesses the shared resource as if it were another drive (D:, E: and so on) within its own system. Sharing is subject to a number of constraints, including access controls set by the Platform that offers the resource for sharing.

Windows File Sharing is used by the FTMS. This runs within a pair of External Interface Gateway servers, as described in Chapter 5 “Application Architectures”. The initiating FTMS service can be directed to transfer files originating on a third Platform, in a directory which is shared with it. Similarly, the receiving Platform can copy the decompressed, decrypted file to a directory that in reality is situated on a fourth Platform.

6.9.2 NFS

NFS is a standard UNIX facility for sharing files between servers. It is available on Windows NT as well as on the Host Central Servers. It is used to pass files from the Host to the Windows NT based External Interface Gateway Platforms for transmission to the External Client Systems. Using NFS means that the transfer of data between the Host and the External Interface Gateway Platforms can be overlapped with that between the central and remote gateway Platforms.

6.10 Further Reading

Ref	Document	Title	Comments
Previous	Chapter 5	Application Architectures	Describes the Application Architecture to be adopted for applications running within Horizon
Next	Chapter 7	Information Management	Describes the Information Management facilities used in Horizon
HADDIS	TD/STD/001	Host Application Database Design and Interface Standards	Sets out the standards to be used by Host applications with Oracle databases.

Chapter 7 - Information Management

7.1 SCOPE

This Chapter discusses the storage and interchange of data within Horizon.

The term *Information Management* embraces database technology in its widest sense, together with the technology for information interchange. It includes the techniques used to model information structures and encode them, so that components of the architecture can communicate with each other.

Information within Horizon can represent business data of either Pathway or PO Ltd and its Clients. Business data originating from PO Ltd itself or Clients that are part of HMG (such as the DWP Benefit Agency) is classified as RESTRICTED and must be protected according to guidelines laid down and enforced by CESG. These are discussed in more detail in Chapter 16 “Security”.

The information management systems covered include:

- Riposte
- Oracle Databases
- Microsoft SQL Server
- Flat Files

Information repositories described include:

- The Data Warehouse
- The Archive Service

7.2 RIPOSTE MESSAGE SERVER

RMS is a messaging system that supports a dedicated Retail application within the Counter PCs.

It provides the functions that the Pathway Contract with PO Ltd describes as those of the TMS. In practice, it provides considerably more functionality than is implied there, and the term TMS cannot usefully be applied to any discrete part of the architecture described in this Document.

The RMS is used to pass data between Counters and Agents in a resilient manner. The processes that provide these functions are described in Chapter 6 “Distributed Application Services”.

This Chapter focuses on the ways in which Riposte stores its internal data, the purposes that this data supports, and the ways in which applications can manipulate it.

Riposte is a fundamental part of the Horizon system. It provides data-driven messaging facilities, and it many cases the bulk of the application logic in a new application can be generated by the appropriate use of Riposte Persistent Objects and Reference Data. This makes the cost of generating such applications quite low.

7.2.1 Structure

7.2.1.1 WebRiposte

Component	Platforms
Asset Manager Web Services	Counter PC
Memo View	Counter PC
Rconsole	SSC Support Workstation
WebRiposte Client	Agent Server Counter PC DCS Agent Server DCS Management Server
WebRiposte Client	NBS Agent Server Network Banking FTMS Local Gateway Outsourcing Software Depot Pathway Software Depot SSC Support Workstation
WebRiposte Data Centre - Software Unsigned by Escher	Agent Server Audit Server Audit Workstation Correspondence Server DCS Agent Server DCS Management Server NBS Agent Server Network Banking FTMS Local Gateway Outsourcing Software Depot SSC Support Server
WebRiposte Desktop	Counter PC
WebRiposte Message Server	Agent Server Audit Server Audit Workstation Correspondence Server Counter PC DCS Agent Server DCS Management Server NBS Agent Server Network Banking FTMS Local Gateway Outsourcing Software Depot Pathway Software Depot SSC Support Server

7.2.1.2 Riposte Utilities

Component	Platforms
Riposte Integrity Checker	Audit Server
Riposte Tools	SSC Support Workstation
Riposte Utilities from Escher	Agent Server Audit Workstation Correspondence Server
Riposte Utilities from Escher	SSC Support Server

7.2.2 WebRiposte Message Structures

Everything that WebRiposte handles is stored as a *message*. Messages are constructed using a format known as A*ttribute Grammar*. This is a self-defining and nested record format that is technology-independent. Data fields (or *attributes*) are not positional, but are identified by a preceding attribute name. Attributes can be optional and new attributes can be added over time without existing applications being affected. Applications use just those attributes they are interested in and are not aware of the rest.

The following fields are added automatically by Riposte when the message is created.

- A *Key*, consisting in general of:
  - *GroupId* - identifies the Group within which the message is created
  - *NodeId* - identifies the hardware platform within the Group
  - *Num* - a sequence number identifying the sequence of the message within the "message run" generated by a particular message server
- *Date* - on which the message was generated
- *Time* - of message generation (in GMT)
- *User* - ID of the Counter user on whose behalf he message was generated. (If the message is generated by an Agent, this field is omitted.)
- *Expiry* - number of days for which the message is to be retained
- *CRC* - *Cyclic Redundancy Check* used to protect the integrity of the message.

In addition, a 64-bit bitmap is added to the message and is used to indicate which members of a Group the message has been replicated to.

Applications are responsible for adding some other fields, and for specifying these as part of the search criteria when reading messages. This includes an identification of the application responsible for the message, Where appropriate, it also indicates its version.

7.2.3 WebRiposte Application Separation

Chapter 5 "Application Architectures" stresses the point that each Application must be independent of all others. In Riposte, this is achieved by ensuring that any Riposte message is uniquely identified with one and only one application. Messages must include a field <Application>, which applications then specify as one of the search criteria when reading messages.

(Note that the Riposte syntax conventions make it somewhat difficult to include strings containing "<" and ">" in attribute grammar messages. Riposte provides APIs to avoid this difficulty, and these APIs should be used by any application that needs to be able to handle strings containing these reserved characters.)

There are no effective controls at present on the ways in which applications identify themselves, or ensure that these identifications are unique. Some applications are complex.

In addition, messages should include the Version number of the application that created the message. This is to cater for a situation where different versions are in use in different parts of the architecture. Riposte will not return a message to an application if it was generated by a later version of the application.

7.2.4 The RMS on Windows NT

The RMS is implemented as a Windows NT service, with configuration information stored in the Registry. Error reporting is via the Windows NT application event log, which can be retrieved by Tivoli (see Chapter 12 "Systems Management"). Configuration and systems administration facilities are provided by Riposte for use by Post Office Managers or visiting engineers.

The Message Store itself is implemented as one or more standard Windows *NT File System* (NTFS) files. On a Counter PC, it is normally one file. On a Correspondence Server, it is normal practice to map the Message Store onto one file for each physical volume, thus enabling Riposte to optimise disk performance. If a new disk is added, Riposte will begin to use it automatically for new messages.

7.2.5 Use of Riposte Messages

7.2.5.1 Types of Messages

The major use of Riposte messages is to pass information between Counters and Agents. However, there are two classes of message that provide some additional facilities. These are *Persistent Objects* and *Reference Data*. These are described below.

Riposte supports a number of message-handling APIs that are implemented via RPC mechanisms. These can be invoked by Agent code. They support natural C or C++ interfaces to a local or remote client. Functions are implemented as OCXs that can be multi-threaded within the Windows NT environment and which support Visual Basic error handing mechanisms. They can thus be used by Desktop Applications that are coded in Visual Basic.

There are in fact three layers of APIs.

- The Message Layer, which includes standard facilities for creating and manipulating messages
- The *Persistent Object Layer*, which includes additional facilities for creating, updating, searching for and selecting Persistent Objects.
- The Reference Data Layer, which provides additional facilities to select records that are effective and applicable to the caller. Reference Data is a particular example of Persistent Objects, and is used to pass parameters to applications and make applications aware of changing data. Reference data messages can be created with an "effective date" in the future, and the Reference Data interface, if called in an Outlet, will not return the record until that date. Similarly, some Reference Data is only applicable to some Outlets (for example, not all Outlets sell Vehicle Excise Licences). Data is only returned if it is relevant.

These are shown here. An implication of this diagram is that Reference Data is accessible through the Persistent Object APIs as well as its own APIs, and everything is accessible via the Messaging APIs.

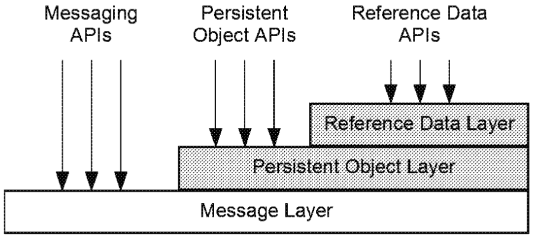

Figure 7.1 - Messages, Persistent Objects and Reference Data

APIs is a somewhat loose term here. Reference Data is intended for use by Counter Applications, and a set of Riposte OCXs is provided to access it. Agents also need to access Reference Data. They need access to a set of APIs other than these OCXs, and these APIs have been provided by Pathway.

7.2.5.2 Message Handling

All information used by Riposte is held as messages. Most messages are created as a consequence of information being passed down to Counter applications or as a result of customer transactions at the Counter.

Messages are used for the following purposes.

- Transactions (where a group of messages are handled as an atomic set, and should a system failure occur before the transaction is committed, any messages created within the transaction are rolled back)
- Enquiries and responses (e.g. requests for any messages satisfying a set of criteria)
- Audit and monitoring information
- Authorisations and instructions (for example DCS card authentication or OBCS Foreign Encashment authorisation)
- To define the text of instructions to Counter Clerks
- To maintain a session context
- To record system events such as user Login, use of a card, etc.

Riposte will not store a message it receives from another node unless it has the preceding message from that node. If it has not, it will request the missing messages from the other node.

APIs are provided within Riposte to retrieve messages, to parse messages, and retrieve attribute names and values. Similarly, there are APIs to enable an application to construct a Riposte message and define its attributes.

7.2.5.3 Persistent Objects

These are designed to be created at the Campus and passed down to the Outlets. They provide a means of permanent storage of standard values and other data. They have additional properties over and above normal messages. The main two properties are:

- The content of a persistent object can be changed by the creation of a new version and Riposte will always return the latest version
- The latest version of a persistent object is never purged. Earlier versions are purged on the same basis as normal messages

Counter PCs must not generate Persistent Objects.

7.2.5.3.1 Persistent Object Attributes

As well as the standard message attributes, Persistent Objects have four additional fields:

- Collection name
- Object name
- Version (set by Riposte, not the application)
- Deleted flag

APIs are provided to enable applications to retrieve persistent data.

7.2.5.3.2 Persistent Object Collections

The Persistent Object store corresponds in many ways to a database table. The *Collection Name* corresponds to a Table Name, and the Object name to a Prime Key. It is possible to define a “query”, with syntax similar to a SQL *Select …* statement. Where more than one message has the same collection name and object name, that with the highest version number is returned, unless the "deleted" flag is set in the highest-numbered version in which case no record is returned.

In some circumstances, for example following a network failure, it is possible for two messages to arrive in the message store with the same Collection name, Object name and Version. By definition, this can only occur between different members of the same Group, and implies that the link between these Group members is unavailable. When it is returned, the RMS detects the discrepancy, and ignores one of the offending messages.

7.2.5.4 Reference Data

The Counter applications are heavily dependent on standing or "reference" data. This is needed to instantiate the Counter Applications and to feed other system components with information generated by PO Ltd or its Clients.

Other Reference Data is generated by Pathway, for example to define many of the characteristics of applications and their processing.

The mechanisms by which Reference Data is defined, received by Pathway, validated, transformed into Attribute Grammar and distributed to the affected Outlets are defined in Chapter 5 "Application Architectures". Each new application will need to generate some components of this process, and assess its impact on others.

Reference data is stored within Riposte as Persistent Objects. Each item of Reference data has an effective date associated with it. This allows the data to be downloaded to the Counters before it is needed and then it becomes automatically available on the effective date. This avoids dependencies on the whole network being available at the point a reference data upgrade is required.

To support this, Reference data is not read directly from the Persistent Objects by the Counter applications. Instead, there is a "Reference Data Server" subsystem that is aware of the effective date algorithm and provides the calling Counter application with the appropriate value for the reference data it requires, based on today's date.

7.2.6 Markers

The <Num> field within a message identifies its position in the message run of messages generated by that system. Although there is no relationship between the <Num> fields of messages from different systems, Riposte supports the concept of a *Marker*. This is a collection of the latest sequence numbers for each system in the Group. Thus, it is possible to state that a particular message precedes or follows a given Marker.

Markers can thus be used to reliably delineate a cut-off point for a set of messages. For example, when it is necessary to balance the Outlet at the end of the day, a Marker can be used to decide which messages are balanced, and which are held over to the next day.

Markers are also used by Riposte to co-ordinate message stores in the event of failures.

7.2.7 Checkpoints

A *Checkpoint* is a collection of Markers for all Outlets in the system, and thus provides a delineation point for the entire system.

7.2.8 Auditing

Riposte forms a contractual boundary within Horizon, in the sense that ownership of data passed from the application's owner to Pathway when the Agents writes messages to Riposte. Thus, all messages stored in the RMS are copied daily to Flat Files, which are then written to bulk storage media. The Riposte Archiving Agent carries out this task. It writes a Checkpoint each time the Flat File is closed.

7.2.9 The WebRiposte Counter Architecture

The previous section describes the Riposte Message Store. Riposte provides some additional facilities at the Desktop. These exploit the message store. They include a set of "middleware" which controls the total operation of the PC, and a set of Retail applications that support the principal business applications of PO Ltd and its Clients.

7.2.9.1 The Riposte Desktop

WebRiposte is integrated with Windows NT in such a way that it gains control of the user's desktop during system boot up, and retains this for the duration of the session. The ways in which this is implemented are described in Chapter 16 "Security".

The desktop is responsible for the total management of the visual image presented to the user. This interface is described in Chapter 8 "User Interface". The original Riposte desktop HCI is carried forwards into WebRiposte.

7.2.9.2 Riposte Retail Broker

Retail Broker provides a set of facilities to support various classes of goods for sale, and processes to keep track of stock within the Outlet. These are extensively used by the EPOSS application.

7.2.9.2.1 Session Manager

This handles the Transaction stack. Applications may add transactions to this stack, and they appear on the right hand side of the Riposte screen. Transactions are not settled until the Counter Clerk presses a "settle" Button or carries out some other action that is equivalent to this, such as swiping a debit card that is accepted by DCS. As long as the settlement is acceptable, Session Manager writes the total set of transactions and the settlement data to the Message Store as a single atomic unit.

It is possible to hook a "user" application into the settlement process. This is used by EPOSS to invoke the Method of Payment menu and ensure that the net value of the session is zero.

7.2.9.2.2 Modes

Retail Broker supports the concept of a Mode, as described in Chapter 5 "Application Architectures". A Counter PC is in one of a small set of predefined modes at any one time. A Mode may have the effect of making certain Desktop functions unavailable; for example, the Logout function is not available while the Counter PC is in "Serve Customer" Mode.

7.2.9.2.3 Stock Units

Riposte messages are used to keep track of the stock levels within the Outlet. The stock unit at the start of a Cash Account Period is represented by a message. By taking this value and applying all the transactions executed during the account period, the closing stock unit balance can be calculated.

7.2.9.2.4 Timestamps

All messages generated by Riposte are time-stamped. As well as helping with message synchronisation, these timestamps are gathered by the Data Warehouse and are used to check Pathway's conformance to the agreed SLAs.

Timestamps should be in GMT, supported by the Local Time at the Outlet (the time displayed on the Desktop) for completeness.

7.2.9.3 Riposte Peripheral Broker

Peripheral Broker is a part of Riposte that hides the details of the interfaces to all peripherals connected to the Counter PCs, and yet makes the facilities of these available to all terminals. The peripherals covered include:

- Bar Code Readers
- Magnetic stripe reader
- Smart Card reader/encoder
- Weigh scales
- Printers

The overall architecture is shown here.

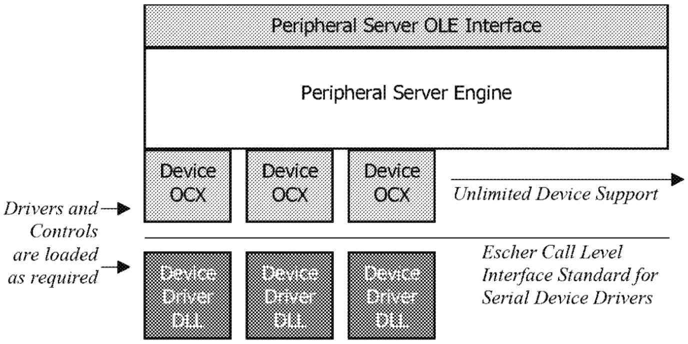
Peripheral Server OLE Interface
Peripheral Server Engine
Device OCX
Device OCX
Device OCX
Unlimited Device Support
Drivers and Controls are loaded as required
Device Driver DLL
Device Driver DLL
Device Driver DLL
Escher Call Level Interface Standard for Serial Device Drivers

Figure 7.2 - Peripheral Broker Architecture

The Microsoft *Object Linking and Embedding* (OLE) interface is exposed by the Peripheral Server.

7.3 ORACLE

Oracle V7 is used to support most databases used by the Host applications running on the Sequent servers in the Campuses. Separate Databases are used for the following services.

- OBCS
- TPS
- APS
- LFS

Oracle V8i is used for the following databases.

- DRS (new at BI3)
- RDMC (upgraded at BI3)
- RDDS (upgraded at BI3)

7.3.1 The Oracle Database Products

Component	Platforms
Oracle - PL/SQL	Data Warehouse Server Host Central Server
Oracle - Pro*C	Data Warehouse Server Host Central Server
Oracle Advanced Replication Option Oracle Developer 2000	Data Warehouse Server Host Central Server MIS Client Workstation MIS Support Workstation Systems Management Access Workstation
Oracle Discoverer 2000 Client	Audit Workstation MIS Client Workstation MIS Support Workstation RDMC Administrator Workstation
Oracle Discoverer Meta Layer	MIS Client Workstation MIS Support Workstation
Oracle Express Objects Workstation	MIS Client Workstation MIS Support Workstation
Oracle for Windows NT4 Networking Products	Agent Server DCS Agent Server DCS Management Server MIS Client Workstation MIS Client Workstation MIS Support Workstation MIS Support Workstation NBS Agent Server RDMC Administrator Workstation
Oracle Forms (Runtime) for NT	MIS Client Workstation MIS Support Workstation
Oracle Forms (Runtime) for NT Oracle Installer Patch Oracle Net for Windows NT (previously SQL*Net)	SSC Support Workstation SMDB Server Agent Server DCS Agent Server DCS Management Server MIS Client Workstation MIS Support Workstation NBS Agent Server RDMC Administrator Workstation SSC Support Workstation
Oracle ODBC Driver Oracle Parallel Query Option	RDMC Administrator Workstation Data Warehouse Server Host Central Server Host Central Server
Oracle RDBMS for Sequent	Data Warehouse Server Host Central Server
Oracle Server	Data Warehouse Server Host Central Server
Oracle Server for Windows NT	Audit Server SMDB Server TME Inventory Server
Oracle Server Manager	Data Warehouse Server Host Central Server
Oracle SQL Worksheet Oracle SQL*Net for Sequent	RDMC Administrator Workstation Data Warehouse Server Host Central Server
Oracle SQL*Plus	Data Warehouse Server Host Central Server RDMC Administrator Workstation SSC Support Workstation
Oracle Table Re-Load Utility Oracle TCP/IP Adapter for Sequent	Audit Server Data Warehouse Server

	Host Central Server
Oracle Tools	Host Central Server
Oracle Web Server	TME Inventory Server
Oracle Xa Libraries	Data Warehouse Server
	Host Central Server
	Host Central Server

7.3.1.1 Oracle RDBMS

Oracle V7 on UNIX supports databases of up to Terabyte sizes on very large multi-processor systems such as the Sequent NUMA-Q servers. Oracle is able to support large numbers of concurrent database users, has high transaction processing performance and is capable of running for 24 hours per day, every day, with minimal down time.

Oracle adheres to industry-accepted standards for the data access language, operating systems, user interfaces and network communication protocols it uses. It has fail-safe security features to limit and monitor data access, and it can enforce data integrity, or business rules, by allowing constraints to be specified so that invalid data can not be input.

Oracle allows processing to be split between the database server and client application programs. The responsibilities for managing the data within the database are handled by the Oracle Server, whilst the workstations manage the interpretation and presentation of that data.

Oracle database systems can also be transparently distributed across networks, allowing data that is physically located on different databases on different computers to appear as if it is all within a single logical database.

7.3.1.1.1 Information Modelling

Oracle uses conventional RDBMS techniques. The logical structure of an Oracle database is determined by the database's schema objects and the mapping of those objects to the physical database via Tablespaces. A schema is a logical collection of database objects associated with a database user. The user name of the database user is the same as the schema name and has a password associated with it to prevent unauthorised use.

The basic units of logical data storage in an Oracle database are *tables*. Table data is stored in rows and columns. Each column is given a column name, a datatype (such as *Number*, or *Date*) and a width. Once a table has been created, valid rows of data can be inserted into it. The table's rows can then be queried, deleted or updated. Other objects which can be created within a schema are views, which are customised presentations of the data in one or more tables, indexes, sequences, synonyms, and database links, which describe paths from one database to another.

The schema objects for all database applications are defined in a Designer/2000 repository. This repository is not only used for the modelling and specification of an application's objects, it is also used to generate automatically all the *Data Definition Language* (DDL) necessary for those objects' definition within a database.

Rows may contain pointers to rows in other Tables. The database is ideally structured so that these links are *normalised*; the definition of this is complex but essentially each data item should appear only once in the database. In practice, most Oracle databases contain a good deal of unnormalised data (which appears as duplicated data items within different but related tables) for performance reasons.

7.3.1.1.2 Information Storage and Retrieval

A database is divided into one or more logical storage units called Tablespaces. A tablespace is used to group together related logical structures, such as tables and indexes. The data of all the logical structures within a Tablespace are physically stored in one or more data files. Within databases running on UNIX systems, these data files are usually created within raw partitions.

At the finest level of granularity, a database's data is stored in data blocks. One data block corresponds to a specific number of bytes of physical database space on disc. A single block size is specified for all the data files within an Oracle database when the database is first created.

Every Oracle database has a set of two or more *redo log files*. The set of redo log files for a database is collectively known as the database's *redo log*. The primary function of the redo log is to record all changes made to data. Should a failure prevent modified data from being permanently written to the data files, the changes can be obtained from the redo log and work is never lost

7.3.1.1.3 Information Interchange and Database Links

A Host application can use data held in another's database. This can only be effective if both applications are designed using principles taken from the Object Oriented approach to software development. Each application must provide interfaces that other applications can call to obtain or write data.

In Oracle, this is provided by *Database Links*, which are conceptual tables within one database but which in fact map onto calls on the second application. The interface mechanism is essentially SQL*Net between the two servers.

Where this mechanism is used, the "called" object need not be an Oracle database. *Transparent Gateways* are software products that fit between the calling application's database and a non-Oracle database. Thus, an Oracle database application could use data, which in fact resided in a Microsoft SQL Server database, using a Microsoft-supplied Transparent Gateway to map the link from one to the other.

Data can be extracted from an Oracle database in a *Comma Separated Value* (CSV) form for long-term storage or for use by another application or database. Similarly, data in CSV format can be input into an Oracle database.

Further details on the mechanisms possible are given in [HADDIS].

7.3.1.2 Oracle Parallel Server (OPS)

OPS is used in situations where the database is spread across more than one "system", and there is effectively no memory-sharing between them. It is used to co-ordinate database locks between these systems using message-passing techniques. A discussion of the nature of single systems, symmetric multiprocessing systems and clustered systems is given in Chapter 10 "Platforms", together with some of the implications for Oracle.

OPS is used with clustered systems. It enables any node to take over the functions provided by another node, should this second node fail, though it will be necessary to fail and then restart the database application. It can do this because the lock tables and other key data is already loaded into the surviving node and hence is not lost when the other node fails.

However, successful use of OPS requires that the database is effectively partitioned between the nodes, and that there is a sensible and well-known strategy for directing transactions at the appropriate node. At Oracle Release 7, this is effectively a manual process. Horizon could, for example, use partitioning based on Post Office identity. If this partitioning is not properly implemented, the nodes can continually fight over the same database pages, with a consequential devastating impact on performance. Thus, Horizon does not use OPS for multi-node working, though it may have benefits in the future for reducing failover times.

At Oracle Release 8i, more "intelligent" partitioning is provided.

7.3.1.3 Oracle Developer 2000

This provides a data modelling repository which is used, as discussed in Chapter 11 "Application Development", to record the structure and usage of all Oracle based applications.

7.3.1.4 Oracle Discoverer

This runs on Client PCs and provides controlled access to an Oracle database. It is used for support purposes.

7.3.1.5 Interactive SQL*Plus

This is not to be used under any circumstances.

7.3.1.6 Oracle Product Structures

This shows the relationship of all the products discussed above.

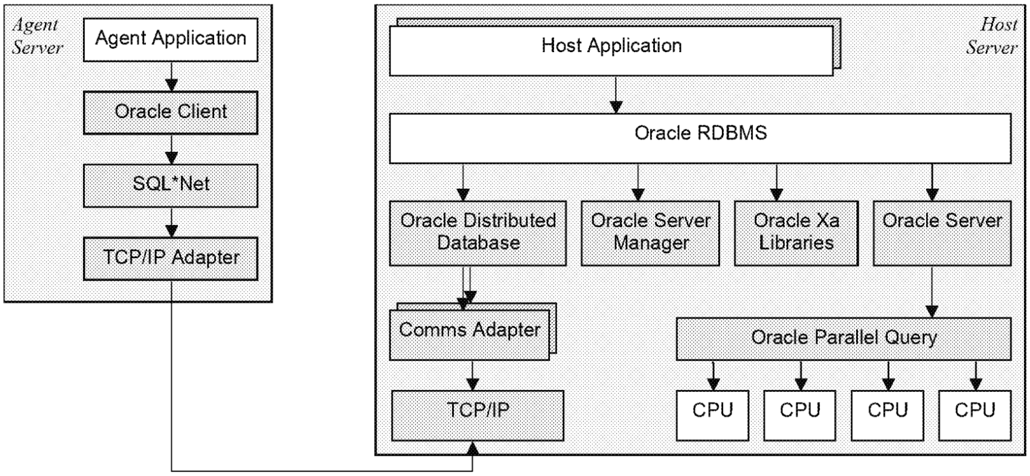

Figure 7.3 - Oracle based Host Application Structures

7.3.1.6.1 Oracle Client

This component (Oracle for Windows NT4 Networking Products) runs on Client platforms, in a client-server paradigm. It and passes Oracle database access requests to the Host platform, and returns the response to the calling application.

7.3.1.6.2 Oracle Distributed Database

7.3.1.6.3 Oracle Server Manager

7.3.1.6.4 Oracle Xa Libraries

These support distributed transaction processing using the OSI Xa protocol.

7.3.1.6.5 Oracle Server

7.3.1.6.6 Advanced Replication Option

7.3.1.6.7 Oracle Parallel Query

7.3.1.6.8 Pro*C

7.3.1.6.9 Oracle TCP/IP Adapter

This maps the generic Oracle products onto a TCP/IP network. It is installed on both Client and Host systems.

7.3.1.6.10 Oracle OSI Adapter

This maps the generic Oracle products onto an OSI network. It is only used for communication with the ESNCS VME systems at the DSS ACC.

7.3.1.6.11 Oracle Forms Run-time

This is used on Client platforms that access Oracle databases.

7.3.1.6.12 Oracle Web Server

This is used on platforms where Web access is provided to an Oracle database. It maps incoming web requests (HTTP) into appropriate database actions.

7.3.2 Use of Oracle Products

7.3.2.1 Host Databases

A number of databases run on each Host Central Server.

- TPS Database
- OBCS Database
- RDMC Database
- APS Database
- LFS Database
- DRS Database

Each database is used by one application. Each Host Central Server is capable of running the entire Sequent-based Oracle workload. In normal working, only one Host Central Server is active. The other acts as a warm standby in case of failure of the active Host or loss of its Campus. The resilience implications of this are covered in Chapter 13 “Availability” and the capacity and performance implications in Chapter 15 “Performance".

A number of design constraints affect the way that new Host applications are constructed. They are documented in [HADDIS]. Those that are specific to the use of Oracle products are as follows.

7.3.2.2 Data Warehouse

The Data Warehouse database is used to store Pathway corporate data. Applications provided within the Data Warehouse are used to report on operational and management issues, and (most importantly) on the adherence to SLAs.

The Data Warehouse is built using Oracle 7 (with the *Parallel Query Option*). It makes considerable use of Oracle's "partition elimination" feature to allow the database to be broken up into manageable chunks. The arrows in this diagram indicate data flows.

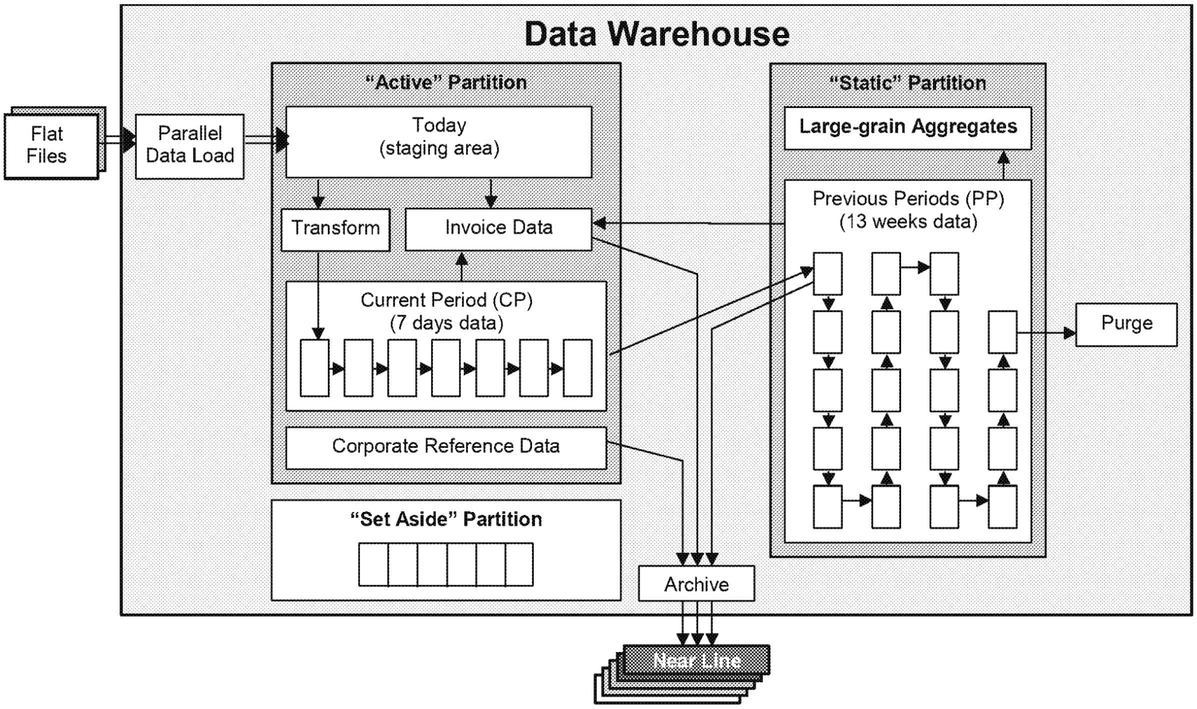

Figure 7.4 - Data Warehouse Internal Architecture

Most data feeds into the Data Warehouse are via Flat Files. (The exception is the names of which flat files are available. This data is inserted directly into the Data Warehouse by the Harvesting Agents.) This isolates it from any need to understand the source applications data structures. Each source interface is defined in a separate AIS. Uploads of files into the Data Warehouse are template driven, and take place in parallel. Any transformations required (such as derivation of values) is carried out on the loaded data, and not as part of the loading process.

The Staged data is used to calculate totals for daily reports, and is then aggregated and transformed into a dimensional structure that is loaded into the *Current Period*. This is built up over the course of a week; it is then moved (untransformed) into the *Previous Periods* area.

The Data Warehouse is designed to be able to hold four full calendar months of transactional data. Data is held in both detailed and aggregate levels. Aggregates are computed across both service and time hierarchies, and are kept for up to five years.

Transactional data older than four months is archived to tape, and may be restored for analysis into a special "set aside" area reserved for this purpose. Archives are written in ISO 8859-1, for Platform independence.

Scheduling and co-ordination of batch-processing tasks is implemented using Maestro.

7.3.2.3 Operational Management Database (OMDB)

There is an Oracle database, the Operational ManagementDatabase, used to hold Outlet statuses, and to record significant events generated by systems management processes. This is used to feed a Web server that permits support staff to view the current state of the event list.

7.3.2.4 Service Management Database (SMDB)

This "clones" certain tables from the OMDB, but is located outside the core Campus firewall so that it can be accessed by a rather wider set of support staff.

7.3.3 Application Development Using Oracle

7.3.3.1 Application Data Modelling

The data model for all application data is stored within a Designer/2000 Repository, and the SQL *Data Definition Language* (DDL) for the application will be generated directly from this repository. Each application should have a single schema that contains all the objects used by that application.

Designer/2000 contains a Repository Object Navigator that enables the application or database designer to view and modify the properties of all the objects used by an application. The set of objects that can be used, and their allowable property classes, is defined in [HADDIS].

7.3.3.2 Application Design

Some aspects of Chapter 5 "Application Architectures" apply to the way in which Oracle applications are constructed. All applications must use a common set of framework tables, designed to handle:

- application control
- exception reporting
- auditing of batch processes and file loading and unloading
- archiving

The set of framework tables is shown below. Their detailed use is defined in [HADDIS].

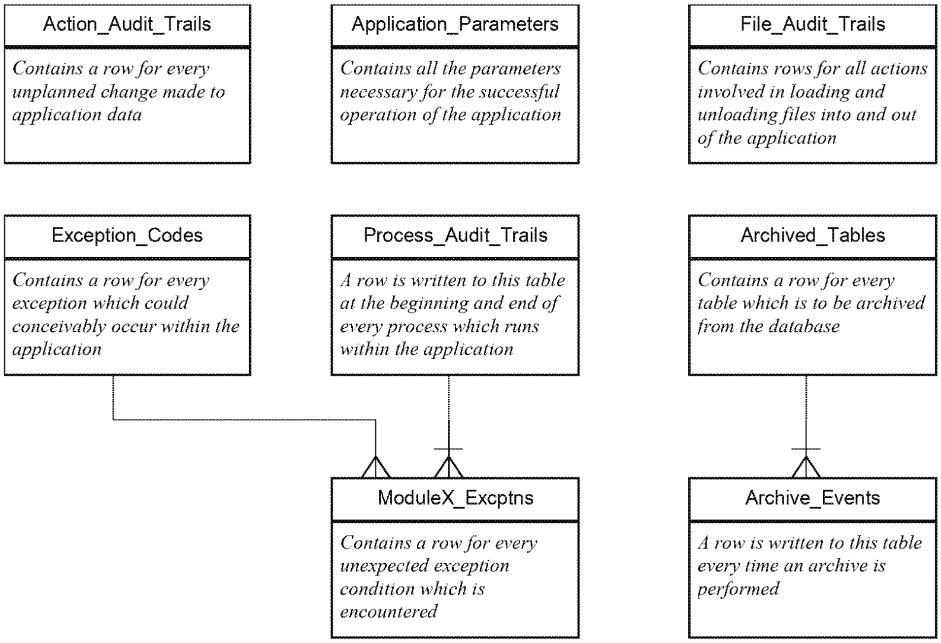
Action_Audit_Trails
Contains a row for every unplanned change made to application data
Application_Parameters
Contains all the parameters necessary for the successful operation of the application
File_Audit_Trails
Contains rows for all actions involved in loading and unloading files into and out of the application
Exception_Codes
Contains a row for every exception which could conceivably occur within the application
Process_Audit_Trails
A row is written to this table at the beginning and end of every process which runs within the application
Archived_Tables
Contains a row for every table which is to be archived from the database
ModuleX_Excptns
Contains a row for every unexpected exception condition which is encountered
Archive_Events
A row is written to this table every time an archive is performed

Figure 7.5 - Application Framework Tables

7.3.3.3 Naming Standards

Pathway-wide naming standards are essential for effective control of the development of database applications. Names should be:

- as meaningful as possible
- as short as practicable

Detailed standards are given in [HADDIS].

7.3.3.4 Auditing

Audit is a term used to cover the collection of information about processes carried out within the system, so that actions (enquiries, updates to live data) can be traced to the human responsible to them.

Audit is covered in detail in Chapter 16 “Security”.

Many of the audit needs, as defined in [ATFS], are implemented via generic mechanisms which require no active involvement of the application. However, applications that carry out modifications to persistent data must make their own arrangements to audit these modifications, using the standard *Action_Audit_Trails*, *Process_Audit_Trails* and *File_Audit_Trails* tables. Data written to these tables is archived daily in a self-defining manner. This enables it to be restored to an empty database at a later date, without this needing to conform to the Schema in use when the data was written.

In addition, each application uses a set of database tables which are called the *Client Interface Table* in Chapter 5 "Application Architectures", and which constitute the interface between the Host Layer and the Agent Layer. Agents should only read from or write to this logical table. It, too, is archived daily in a self-defining format.

Details are provided in [HADDIS].

7.3.3.5 Supportability

Oracle provides facilities for administrators to make on-line changes to application data, via SQL*Plus or equivalent low-level products. However, this is an error prone process, can impact the performance of production applications, and is unauditable. It thus infringes the Pathway security objectives. Some applications require direct user update access to data in an Oracle database, or to the application parameters. These must provide appropriate forms to automate and control this process and ensure that it conforms to the security policy. The form must write an audit record, detailing the amendment, as well as carrying out the amendment.

Where unforeseen enquiry access is required, for example by auditors, it must only be permitted via a tool which is designed for the purpose and which provides suitable auditing. Oracle Discoverer is the tool chosen to meet this requirement for Host applications.

7.3.3.6 Number of Oracle Databases

It is preferable to minimise the number of databases for performance reasons. Thus, where sensible, applications can share databases. However, they should communicate in exactly the same way as applications that have their own database.

7.3.3.7 Performance

Host applications run on Sequent NUMA-Q processors (see Chapter 10 “Platforms”). To obtain the best performance from these machines, applications should be coded to exploit multi-processor architectures. They should use parallel SQL constructs where appropriate. Techniques available include the following. In each case [HADDIS] provides more detail.

- Use the Oracle *Cost Based Optimiser* (CBO; though this can behave differently for test and full-size databases, and hence should used only in conjunction with Oracle “Hints”)
- Use the *Parallel Query Option* (PQO) for nearly all queries on tables with a significant population. Use of the PQO must be subject to detailed large-scale testing, but experience to date shows that any query accessing more than around 1% of a table will run better with PQO than using table indexes.
- Use a number of separate parallel load processes, rather than the Oracle parallel Direct Load function.
- Don’t use Foreign Keys unless there is no practical alternative.

7.3.4 Oracle Express

This is a graphical analysis package that is located on the Data Warehouse. It is used to analyse Service Level and other data held within the Data Warehouse.

7.4 MICROSOFT SQL SERVER

Microsoft SQL Server is used to support the Auto-Configuration Database, OCMS Database and Key Management applications.

7.4.1 Business Issues

SQL Server runs solely on Windows NT Server. It is an RDBMS product with some of the power and flexibility of Oracle but without (at present) the ability to scale to the same degree of Oracle, or to support the same volumes of data or transaction volumes. (Microsoft may disagree, and could demonstrate some specific but not very usable instances in which it is not true.)

It is licensed by Platform (i.e. server or seat) without regard to data volumes or transaction rates. However, licence costs are significantly less than for Oracle. Thus, SQL Server is used for medium-scale Host applications which require some permanent storage or business rule processing, and where the facilities needed fall outside the blanket Oracle licence, and Riposte does not provide sufficient facilities.

7.4.2 Functionality

SQL Server is strictly a client-server-based product. It uses client-based applications such as Microsoft Access to provide the client functionality. Client applications access it via ODBC and Microsoft's implementation of SQL.

7.4.3 Structure

Component	Platforms
ActiveX Data Objects (ADO)	Audit Server DCS Management Server
ActiveX Data Objects (ADO)	KMA Server KMA Workstation OCMS Client OCMS Server Tivoli Support Workstation
Microsoft Data Access Components (MDAC)	KMA Workstation OCMS Client RDMC Administrator Workstation
Microsoft NT Runtime for DAO	ACDB Client Workstation Audit Server Audit Workstation DCS Management Server OCMS Client OCMS Server SMDB Server Tivoli Support Workstation
Microsoft Open Database Connectivity (ODBC) Driver	ACDB Client Workstation Audit Server CA Workstation DCS Management Server KMS Admin Workstation OCMS Client OCMS Server RDMC Administrator Workstation
Microsoft SQL Server	ACDB Server Audit Server DCS Management Server KMA Server OCMS Server
Microsoft SQL Server Client	ACDB Client Workstation Agent Server DCS Agent Server KMA Workstation KMS Admin Workstation NBS Agent Server OCMS Client SSC Support Workstation Tivoli Support Workstation VPN Exception Server

SQL NetLib SQL+	KMA Workstation Short-term Performance Database Server

7.4.3.1 SQL Server Client

This runs on a Client platform and communicates with the SQL Server via ODBC.

7.4.3.2 SQL Server

The Server holds the actual database.

7.4.3.3 ODBC Driver

This runs on all the Client platforms that require access to the SQL Server database. It drives the ODBC protocol that handles the remote access to data in the database.

7.4.3.4 SQL NetLib

7.4.3.5 Microsoft NT Runtime Library for DAO

This provides support for applications that need to manipulate the Data Access Objects (DAO) in an Access or SQL Server database.

7.4.3.6 Microsoft Active Data Objects

7.4.4 Use of SQL Server

SQL Server is used for the following databases in Horizon

- Auto Configuration Database
- Key Management Database
- OCMS Database
- DCS MID/TID Allocation Database
- Audit Checksum Database

7.5 AUDIT SERVICE

This is a service running on the Audit Server. It retains a record of all files archived to the Centera audit data repository. The following classes of audit data are passed to the Archive Service for storage on bulk media:

- records of all messages written to the Riposte Message Store
- records of all bulk file transfers to and from PO Ltd and its Clients
- where necessary, the actual content of the files transferred to and from PO Ltd and its Clients
- records of changes to persistent data made by Host applications
- Host Application's Client Interface Tables
- Help Desk log files
- records of events received by the Tivoli Event Console

7.6 FLAT FILES

There is no accepted definition of what constitutes a "Flat File". For the purposes of this document it is a file that is manipulated by a File Management services, such as Windows NT's NTFS, as opposed to a database which is manipulated by a database management system such as Oracle. Flat Files should be encoded using ISO 8859-1.

> *This is equivalent to ASCII with one or two minor exceptions. The DSS VME systems store data in EBCDIC, and it is translated to and from ASCII as part of the file transfer between the ACC and Horizon.*

Flat files are used in a number of positions, particularly for passing data from one system component to another or from Horizon to an External Client System or vice versa.

In addition, all audit data is written to bulk storage media as Flat Files, and is restored as such. If it is retrieved for audit purposes, it needs to be interpreted properly. Each database type (Oracle, Riposte, Tivoli) provides a mechanism to repopulate an otherwise empty database with data retrieved from the Archive Service.

7.6.1 Structure

The format of some flat files is dictated by suppliers such as Microsoft. Those whose content is under Pathway control must conform to a set of standards that include the following.

- Files must include both a header and trailer
- They must include a record count, and sub-record counts where appropriate

> *These standards are not defined explicitly anywhere so far as I'm aware.*

7.7 INFORMATION INTERCHANGE

> *In subsequent versions of the TED this sub-section will focus on end-to-end data handling with especial emphasis on ensuring the end-to-end integrity of key business data.*

7.8 GENERIC INFORMATION MANAGEMENT ISSUES

7.8.1 Data Recording

All systems used in Horizon store character information in ISO 8859-1.

7.8.2 Character Sets

All Applications should assume that data is presented to them in ISO 8859-1 (Latin Alphabet Number 1).

See **IRRELEVANT** for the Character Code Handbook that discusses this subject in some depth.

Note that Riposte Attribute Grammar includes some reserved characters, in particular "<" and ">". There are Riposte APIs to enable these to be "escaped". Text messages that include non-printable characters need to be sent as Riposte attachments rather than included in a message.

7.8.3 Regional Identification

The Welsh Language Act requires that any official publication must be printed in Welsh as well as English within Wales. All Counter PCs will be provided with an indication of their Region (as well as National Identify, 44) that can be used to determine whether the provisions of this Act apply.

The Regional Identity will be set from information provided by PO Ltd.

7.8.4 Data Representation

7.8.4.1 FAD Codes

The GroupId used within a Riposte message effectively identifies the Outlet. The value used is the six-digit *Financial Accounts Division* (FAD) code, used internally by PO Ltd to identify their Outlets. The value used for any particular Post Office may change over time (for example if it is re-franchised).

7.8.4.2 Time Stamps

Time stamps are used for a number of purposes, including audit.

7.8.4.2.1 Time Representation

All *time stamps* recording the date and time that something took place will be recorded within Horizon in GMT. Where it is necessary to display, record or use local time (for example on Counter PC Desktops) this should be held separately or calculated at the time it is displayed.

Time stamps passed to or from PO Ltd or a Client will be in either GMT or local time as agreed in the relevant AIS. Where the format is *not* GMT, it should either be held in both formats or converted close to the data boundary.

Where it is or may be important at a later date to know both the local time and the actual time that any operation was carried out, both should be recorded. This avoids the need to re-calculate the "missing" time later, when the data necessary to make this calculation may be missing or suspect.

Note that all Horizon systems operate within a single time zone.

7.8.4.2.2 Date Representation

All dates held within the system will use four-digit year fields.

7.8.4.3 File Naming Conventions

File names should follow the Windows NT "long filename standard" whereby a name of up to 256 characters can be followed by ".ttt", ttt being the file type.

Applications may use file names containing date- and time-stamps to differentiate, for example, one day's data from the next. File names used in this way are purely descriptive and hence do not need to contain four-character year identifications.

Changes to the type of a file may be used within an application to represent changes in its state.

7.8.4.4 Digital Signatures

These are used in a number of cases where there is a need to protect the end-to-end integrity of data passed to or from a PO Ltd Client. Their structure is defined by the X.509 standard.

7.9 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 6	Distributed Application Services	Describes the mechanisms that enable application components to be distributed across two or more Platforms.
Next	Chapter 8	User Interface	Discusses the principles underlying the ways in which Horizon is presented to is end-users. This includes the "look and feel" of the interface style; the enablers used to deliver an application user interface; and the tools used by the application developers to develop that interface. It also includes the facilities used to give users easy access to their applications and to automate parts of their work.
Riposte	Release Notice		Information on Riposte and its facilities is best found in the Release Notice for the current Build. These can be found on the Pathway Architecture Team Web Site.
HADDIS	TD/STD/001	Host Application Database Design and Interface Standards	Defines standards for the design and construction of Oracle based Host applications.
MISARCH	DW/DES/003	MIS Release 2: Data Warehouse Architecture Specification	Describes the internal software architecture of the Data Warehouse and the applications that access it.
DWHLD	DW/HLD/002	BI3 Data Warehouse High Level Design Specification	

Chapter 8 - User Interface

8.1 SCOPE

This Chapter discusses the principles underlying the ways in which the Horizon systems are presented to their end-users. This includes the "look and feel" of the interface style; the enablers used to deliver an application user interface; and the tools used by the application developers to develop that interface. It also includes the facilities used to give users easy access to their applications and to automate parts of their work.

Different criteria apply to different components of the architecture. The major differentiators are:

- systems used by what are in effect members of the public
- systems used by members of Pathway
- systems used by staff of Pathway's suppliers or Clients (e.g. PO Ltd)

Systems used by nobody at all, i.e. in "hands off" mode, are not considered here.

8.2 USER INTERFACE REFERENCE ARCHITECTURE

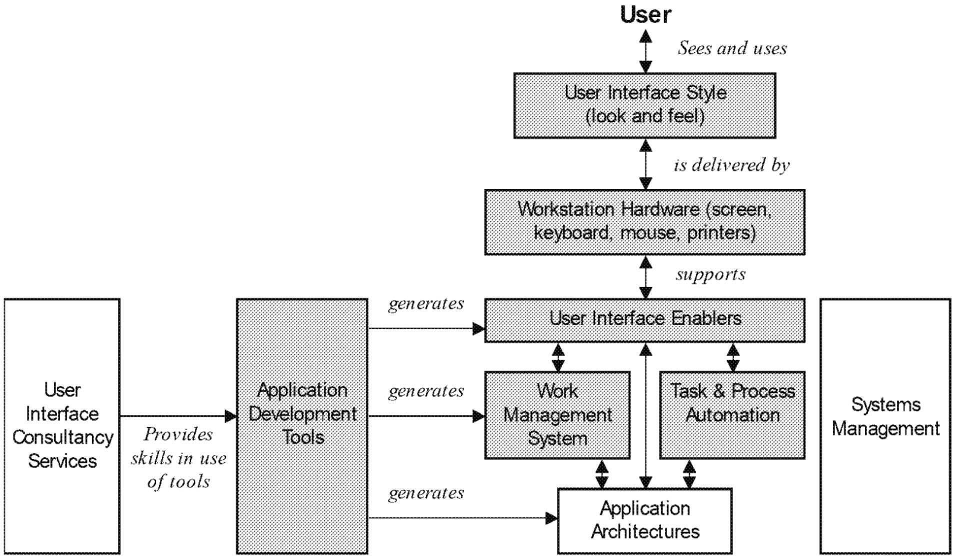
User
Sees and uses
User Interface Style (look and feel)
is delivered by
Workstation Hardware (screen, keyboard, mouse, printers)
supports
User Interface Enablers
User Interface Consultancy Services
Provides skills in use of tools
Application Development Tools
generates
generates
generates
Work Management System
Task & Process Automation
Application Architectures
Systems Management

Figure 8.1 - User Interface Reference Model

8.3 COUNTER SYSTEMS

8.3.1 Users

Counter Systems are used by Post Office Managers and their staff. They need a simple, robust and secure user interface that requires the minimum in the way of computer literacy.

This normal User Interface is implemented by the Riposte Desktop. Post Office Managers have an additional interface, the Post Office Log On (POLO) which they must follow when switching on a Counter PC.

8.3.2 Riposte Desktop

8.3.2.1 The Riposte User Interface Style

There are a number of different facets to the user interface style, implemented by the different devices available on the Counter. The Counter User Interface is designed to be as simple and intuitive as possible and is specifically tailored for use in a Retail environment. The intention is that unless absolutely necessary, the Counter Clerk should not have to type in any data on the terminal. Many transactions are initiated automatically by the Counter Clerk swiping a magnetic card or reading a bar code using the Counter's Bar Code Reader. (There is always a "fallback" facility for the Counter Clerk to enter these details manually if, for example, the bar card reader is out of action.)

8.3.2.1.1 Screen Size

The screen used is relatively small (10" or 12" diagonal) to minimise the space taken at each Outlet Counter position. Interaction with the system is achieved by the keyboard or by touching the screen. This is equivalent to a mouse "click".

Both types of screen support a SVGA (800 x 600 pixel) display with 256 colours.

8.3.2.1.2 Desktop Custom Controls

The user interface makes use of "custom controls" provided as part of the Riposte Desktop system. These constrain the designer to work within a particular style, an example of which is shown here.

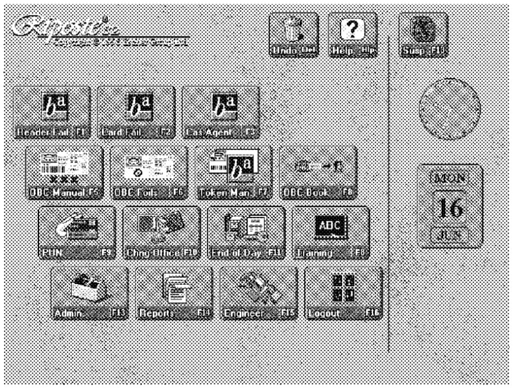

Figure 8.2 - Example of the Riposte Desktop

This style splits the screen into two parts. The left hand portion contains a number of menu Buttons which are valid in the context of the transaction (though some may be marked with a "stop sign" which indicates that they cannot be used in this particular transaction.) The right hand side of the screen is a "stack" showing, for example, the purchases made by the customer so far. Its default content is the time and date.

8.3.2.1.3 Menu Buttons

The desktop contains a menu of *Buttons*, each of which leads to a sub-menu or some application. Each Button is actually an instantiation of an OCX.

A number of standard OCXs are provided, including the following.

OCX	Purpose
Calendar	Displays the current date and is completely under the control of the desktop. It is displayed on the right hand side of the screen when this is otherwise empty.
Clock	Displays the current time and again is under the control of the desktop. It is displayed on the right hand side of the screen, above the calendar.
Card	Displays a "Button" like image with a single Icon and a single matching Function key. When pressed, it displays some other sub-menu or application interface.
Button	More complex than a Card, and permits multiple images (Icons) and multiple lines of text.
Trans	Like a Windows NT "tab", and whose content is completely under the control of the application. It is used for the display of information, and does not respond if pressed.
Pages	Like multiple "tabs", and is used for the display of more data than will fit on a single Trans.
List	Like a Page display but with the page content arranged in a list with multiple columns. The user can select rows, and search for particular entries.
Ledger	Displays multiple columns and multiple pages, and is used for navigation between items. It is usually displayed on the right-hand screen portion.
Script	A tab-like control which runs under an Pathway-defined script. This script offers great flexibility in the design of simple applications. It can display queries to users, react to value entered by the user, and build up a "list" recording the progress of the script (i.e. the choices already made by the user).
Calculator	Used for example to allow the Counter Clerk to enter alphanumerics, numbers, and currency values. It is usually used with the Script OCX.
Message/Error	Merely displays a message or error indication. The Counter Clerk can acknowledge this, or may be given a Yes/No option. It is usually used in conjunction with the Script OCX.
Options	Presents a list of options to the Counter Clerk and enables him to choose one of them by pressing the appropriate part of the screen or an associated function key. It is used with the Script OCX, for example to enable the Counter Clerk to enter a reason why a transaction was aborted (printer error, customer changes mind, etc.)
Help	Provides help information to the user

Table 8.1 - Standard Riposte Desktop Controls

Each OCX supports a complex set of properties which enable them to provide a simple and consistent language for use by applications.

In addition to these programmable OCXs, there is a set of standard OCXs that appear on virtually all desktops. These include:

OCX	Purpose
Desktop	Returns to the top-level desktop, and acts as an "escape" Button.
Previous	Returns to the previous screen, and again is an "escape" Button.
Undo	Used in conjunction with another OCX which is pressed subsequently; it "removes" the corresponding item if one is on the stack. The details of the action are under application control.
Help	When pressed and followed by the Counter Clerk touching another OCX displays a short help message indicating the use of this second OCX.
Suspend	Permits the use of sub sessions. The Counter Clerk can swap between the current

session	session and a suspended session.
Training mode	Enables the user of a training Message Store

Table 8.2 - Additional Riposte Desktop Controls

8.3.2.1.4 Help Facilities

Help facilities are implemented using Internet technology. Entry to the help mechanisms is context-dependent, and the initial help screen depends on the screen context at the time help is invoked. This is displayed using the Microsoft Internet Explorer. Subsequently, Counter Clerks navigate around the help information using the facilities of this Browser. Access to HTML files is controlled by Riposte, which only permits access to those specified by Persistent Objects and held within the Counter PC.

8.3.2.2 Riposte Style Guide

This Document describes only the barest outline of the way in which the Riposte applications are constructed and the interface that they present to the Counter PC user. The definitive Reference Manual for application developers is the *Riposte Style Guide* [STYLE]. This defines the types of Button, Impulse, menu and other interface features that may be used, and the ways in which other screen components are driven. More importantly, it lays down the principles which minimise the amount of time that any particular transaction type takes at the Counter, which is an important consideration at peak times when the Outlet may contain large queues at each Counter.

Amongst the issues addressed by the Style Guide are:

- The system should appear to the user as intuitive, and any actions than can be taken during a dialogue can be discovered without leading the user into an irrecoverable position
- It should give a clear indication of the current Mode of operation
- Colours should be chosen to reduce glare and enhance contract and visibility of information
- Text should be in mixed cases
- Menu Buttons should be identified by appropriate Icons
- Screen titles should appear in consistent locations and should be consistent with the Menu Buttons from which they were activated
- Buttons should display a "No Entry" logo when the product or function that they represent are not available in that Outlet or to that user
- Menu hierarchies should be restricted to a maximum of four levels

There are many others.

8.3.2.3 User Interface Enablers

The basic enablers for the Riposte User Interface style are provided, as indicated above, by Windows NT OCXs.

8.3.2.4 Application Development Tools

Most of the features of the Riposte User Interface are available via standard Windows development tools such as Visual Basic. The Escher Group standard for developing Riposte applications is Visual Studio.

8.3.2.5 Work Management

Riposte maintains the users Desktop and the links between the transactions recorded, the controls applicable to the current transaction, and the mechanisms needed to "close" a stack of transactions when the user wishes to settle these.

8.3.2.6 Task and Process Automation

The *MemoView* facility in Riposte is used by Customer Service staff to send simple messages to all Outlets, or a selected Group of Outlets.

8.3.3 Menu Hierarchy

Riposte uses a hierarchy of menus. As shown in Figure 8.2, each screen has room for 16 Buttons. Within the menu hierarchy, each Button usually leads to another sub-menu.

Some of the items represented by branches in the menu hierarchy are limited to particular Outlets or classes of Outlets, or indicate items of a similar nature but whose exact identity varies from area to area. In these cases, the menu hierarchy is the same across all Outlets, but selecting a particular menu item leads to a "pick list" which lists the items appropriate to that Outlet.

The resulting generic Menu hierarchy is described in [OPSMENU].

8.3.4 Workstation Hardware

8.3.4.1 Screen

The Counter PC screen is specifically designed to help the user interface style paradigm presented by Riposte. It is small (10" diagonal) to minimise the space taken on the Counter. It provides a colour display to exploit the detail that only colour can bring, and which Riposte exploits extensively. It provides a *Touch Screen* interface, so that the user can simulate a mouse "click" by touching a Button on the screen.

For Outlets with insufficient space for a CRT, there is the option of a 12" diagonal flat screen. This supports SVGA, whereas the CRT supports VGA. Riposte supports both, and will adapt to the screen properties. It uses a Persistent Object to determine which screen resolution to use.

8.3.4.2 Keyboard

The keyboard is custom designed for PO Ltd. It includes a magnetic stripe reader and a Smart Card interface. There are dedicated blocks of keys within the keyboard that support specific application actions.

Applications register their interest in a particular card IIN. The magnetic stripe reader interface in Riposte will then automatically activate the appropriate application to deal with the type of card swiped.

The first six digits in the card number identify the card issuer. Different Riposte procedures are set up to deal with different cards or groups of cards.

8.3.4.3 Printer

These are discussed elsewhere. There is a combined tally roll and slip printer, used mainly for printing receipt slips for customers. There are a number of variations.

There is a "back office" printer, used for printing reports.

8.3.4.4 Bar code reader

Each Counter has a hand held *Bar Code Reader*. Similarly to the magnetic stripe interface, the bar code interface will activate the appropriate application to deal with a particular bar code.

It may in the future be used for reading bar codes on standard retail products.

8.3.4.5 Weigh scales

There are fewer weigh scales than Counter positions. Typically, one is shared between two Counters. It is plugged into a serial port on one of the Counter PCs and shared across a preconfigured set of Counters on the local network.

When a parcel (or whatever) is placed on the weigh scale, the Counter Clerk must press a Menu button on the Counter PCs to "acquire" the scales and read the weight of the item.

8.3.4.6 Smart Card Reader

The keyboard includes a smart card reader that is used in the first instance to authenticate the Post Office Manager during Counter switch on.

This reader is also used to read and update information stored on "credit card" style Smart Cards issued by Utilities and other agencies.

8.3.4.7 PIN Pad

Most Counter peripherals are designed for use by Counter staff. The exception is the PIN Pad, introduced at BI3 to support NBS. It is located on the customer side of the Outlet screen, and is used by the customer to enter a PIN value to verify an NBS transaction.

Note that clearing banks have committed that, by 2005, all EFTPoS-enbled cards will contain a chip supporting the EMV protocols, and that Debit Card transactions will be verified by a PIN that is checked against the application held on the PIN. The Horizon PIN Pad has a chip card capability, but does not at present support EMV. However, it is expected that EMV support can be added by a firmware upgrade that can be distributed using the standard software distribution mechanisms.

8.3.5 Post Office Log On (POLO)

POLO is invoked in the following circumstances:

- the first time an Outlet is used after installation
- if a Counter PC is switched off (for example following a power fail)
- if the system suspects that the Post Office Manager's PIN has been compromised.

It is menu driven and requests the Post Office Manager to insert the PMMC into the keyboard's Smart Card reader. If this is valid, a recovery code is printed and the Post

Office Manager is requested to input the PIN. If this, too, is valid, the Counter PC completes its start-up sequence.

8.3.6 Auditors

Auditors are given access to special Riposte facilities to display and print reports of activity at a designated Outlet over a given time period. The interface to this is the same as to other Riposte functions; the necessary controls and Menu Buttons are only available in an appropriate Role.

8.4 CLIENT SYSTEMS

A number of systems in Horizon provide Client access to database or other applications. These include the following. In each case, the Client is a Windows NT Workstation that supports the standard Windows GUI.

Client	Host	Database or Application
Horizon Help Desk Terminal	n/a	
MIS Client PC	Data Warehouse Server	MIS
MIS Support WS	Data Warehouse Server	MIS
Audit Workstation	Audit Server	
RDMC Administration Workstation	Host Central Server	RDMC
SSC Support Workstation	n/a	
One Time Password Workstation	n/a	
Auto Configuration Database Client	Auto Configuration Database Server	ACDB
SecurID Admin Workstation	SecurID Server	ACE/Server
CA Workstation	n/a	
KMS Admin Workstation	KMA Server	KMA
KMA Workstation	KMA Server	KMA
Tivoli Support Workstation	n/a	
Generic Support Workstation	n/a	
OCMS Client Workstation	OCMS Server	OCMS

Table 8.3 - Windows-based Client Workstations

8.5 WEB BASED SYSTEMS

A number of systems used for internal monitoring or reporting are implemented as *Web Browsers* providing access to material held on a Web Server. Examples include the following.

Client	Host	Database or Application
Security Event Browser	Tivoli Event Console	
Client PC	Various	n/a

Table 8.4 - Web-based Client Workstations

8.6 CENTRAL HOST SYSTEMS

These are Sequent NUMA-Q Servers running under the Dynix operating system, which is a variant of UNIX. It supports the conventional character-based User Interface. Because of well-known security weaknesses with these processes, users (including operators and support staff) who wish to access these servers do so via a product called COS/manager. This replaces the Dynix Login facilities with a GUI based front end that uses menu-based Roles to restrict the functions available to users according to their defined privileges. It enables operators to manage the system without the need for root access to the operating system. All system administration and operations activity is initiated through the COS/manager interface.

8.7 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 7	Information Management	Describes the facilities used to hold and manipulate data
Next	Chapter 9	Networking Services	Describes the networking facilities used to support the delivery of the Horizon services
OPSMENU	SD/DES/016	Horizon OPS Menu Hierarchy	Describes the desktop menu hierarchy and the icons used.
STYLE	SD/STD/001	Pathway Horizon Office Platform Service Style Guide	Describes the Riposte style guide.

Chapter 9 - Networking Services

9.1 SCOPE

This Chapter describes the various networking facilities used within Horizon.

Networking Services support the distribution of users, data and applications by providing interconnection and interworking services over local and wide area networks.

The key services that must be supported by the networking services are:

- Access to business applications running on remote servers
- Transfer of files to and from remote systems
- Access to applications and information on remote servers
- Remote support and management of both internal systems and Pathway supplied systems installed on external sites

These facilities are required to link together a number of different types of location.

- Around 18,500 Post Office Outlets
- Two Pathway Campuses at Bootle and Wigan
- Benefits Agency site used for OBCS support
- PO Ltd site at Huthwaite
- IBM NBE sites at Greenford and Warwick
- Streamline Merchant Service sites in Scotland
- Suppliers who provide software and data to Pathway
- Suppliers who require on-line access to components of the system for support purposes
- Pathway locations used for development and support

In addition, there is a need for internal communications within some of these locations.

Horizon uses a communications infrastructure supporting a variety of types of connection and bandwidth, depending on the needs of the services using that link. Resilience is included by the provision of alternative routes where appropriate. A number of networking services are provided over this communications infrastructure.

9.2 NETWORKING REFERENCE MODEL

The OSI seven-layer reference model identifies the various layers of the networking architecture, and the classes of Interworking Services that may be required.

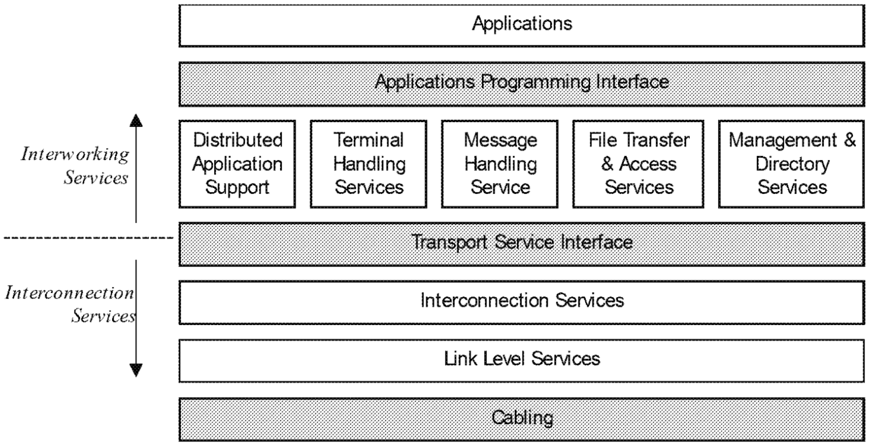
Applications
Applications Programming Interface
Interworking Services
Distributed Application Support
Terminal Handling Services
Message Handling Service
File Transfer & Access Services
Management & Directory Services
Transport Service Interface
Interconnection Services
Interconnection Services
Link Level Services
Cabling

Figure 9.1 - Networking Reference Model

The Chapter follows this model, and discusses the following subjects.

- Cabling services
- Link Level services
- Interconnection services
- Interworking Services

9.3 CABLING SERVICES

- Static cabling is used between the Campuses, and between the Campuses and principal suppliers and Clients
- Dial-up cabling is used to the majority of the Outlets and to some support sites and AP client sites

9.3.1 Static Cabling

Static cabling services *between* Pathway locations, to PO Ltd sites, and to some of its suppliers, are provided by *Energis Ltd*. The core backbone services are provided by Fibre cables strung along the pylon system of the National Grid. These are connected by strategically placed switches.

Energis is Pathway's preferred partner for large-scale networks and supports high bandwidth networking links across the whole of the UK. It buys local services from BT.

9.3.1.1 The Energis Backbone Network

The Energis backbone network supports S*ynchronous Data Hierarchy* (SDH) communications into the Campuses. This provides 622 Mbps of bandwidth per cable, which is usually used to provide four 155 Mbps *Asynchronous Transfer Mode* (ATM) circuits. Energis provide an ATM switched network over these circuits.

9.3.2 Dial-up Cabling

Other communications between locations use mainly ISDN services provided by BT. Locations where ISDN is not available are connected via Satellite.

- ISDN provides a dial-up 64 Kbps connection, with a call set-up time of less than two seconds. More than 85% of all Outlets can be connected via ISDN
- Outlets with a high business load may use a permanent ISDN connection for all or part of the day
- Outlets that cannot be connected via ISDN are supplied with a satellite phone system that presents a Frame Relay interface to the Counter PC. These are all single-Counter Outlets

9.3.3 Business Issues

Static cabling services are charged by the bandwidth delivered, whether this is used or not. The key business objective is to ensure that only the necessary bandwidth is procured.

Charging for ISDN services is by a combination of call set-up and call duration. The major business objective is to limit the number of times any one ISDN link is opened, and to minimise the call duration once it is opened.

9.4 Link Level Services

9.4.1 Classes of WAN Connection

Two classes of link level communications are carried over this network.

- Asynchronous Transfer Mode (ATM) circuits are used between the two Campuses.
- Frame Relay (FR) circuits are used elsewhere except where dial up connections are used

9.4.2 LAN Bridges and Virtual LANs

There are a number of cases where it is necessary to carry a LAN subnet between the two Campuses. The principal need for this is where a single IP address is used by Client applications to access a service that runs on a server at one Campus, but may fail over to the other Campus. For the single IP address to be able to follow the service, the two servers must be on the same subnet.

This is implemented by bridging the two Campuses, at OSI Link Level, to create "Virtual LANs" (VLANs) spanning the two Campuses.

9.5 Interconnection Services

9.5.1 Classes of LAN Connection

Pathway uses the following network classes.

- High speed LAN connections based on Fast Ethernet (100baseT)
- Conventional Ethernet LAN connection (10baseT)

9.5.2 Permanent Virtual Circuits

A number of *Permanent Virtual Circuits* (PVCs) are used between the Campuses and other locations. In general, at least two PVCs are defined to each location, routed to different Routers or switches within the Campuses for resilience. Each is given a *Committed Information Rate* (CIR), which is effectively the reserved bandwidth for that PVC. The bandwidth needed for the links is the sum of the CIRs for the PVCs.

9.5.3 High Speed Links

The two Campuses are inter-linked through the Energis network, as shown below. The physical circuits are shown as fixed lines, with the PVCs within the Energis network shown as dotted lines.

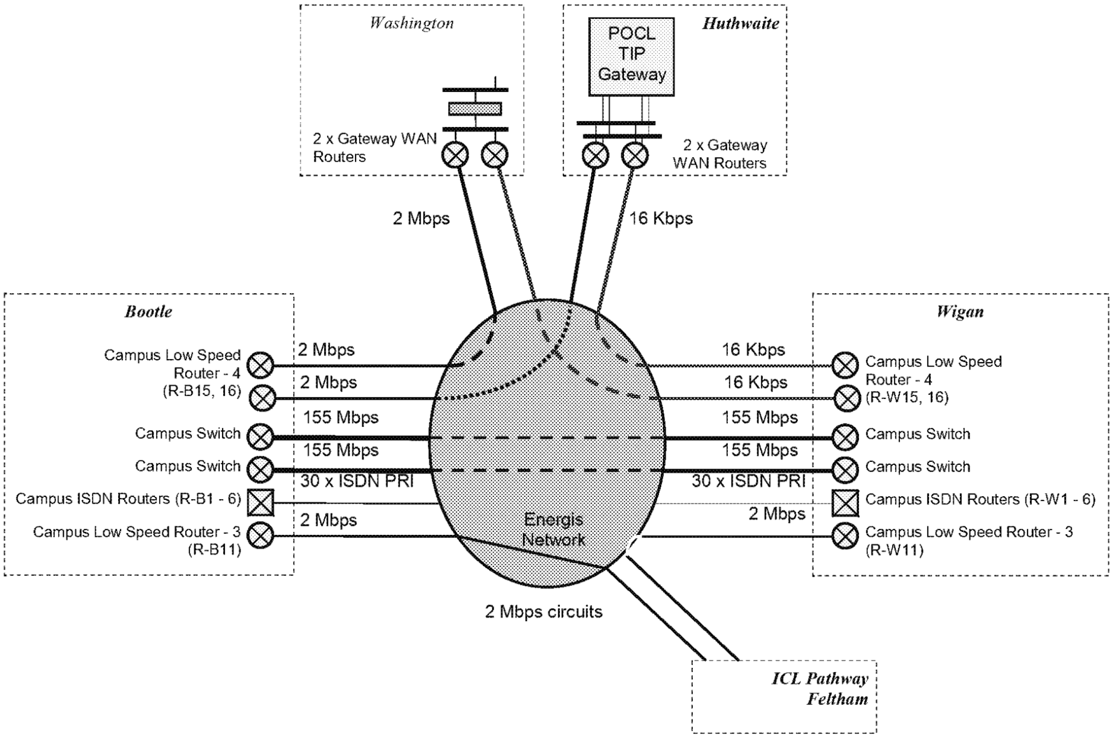

Figure 9.2 - Inter-campus links

Revise this diagram to include FRIACO Routers

9.5.3.1 Energis Diverse Routing

To increase resilience, the Energis network uses diverse routing through a number of switches, as shown here. Each Outlet has a set of 01620 numbers, which are routed via the BT/Energis network to one or other of the Campuses. In addition, there is an 0800 (freephone) number in case either of these primary numbers is unreachable.

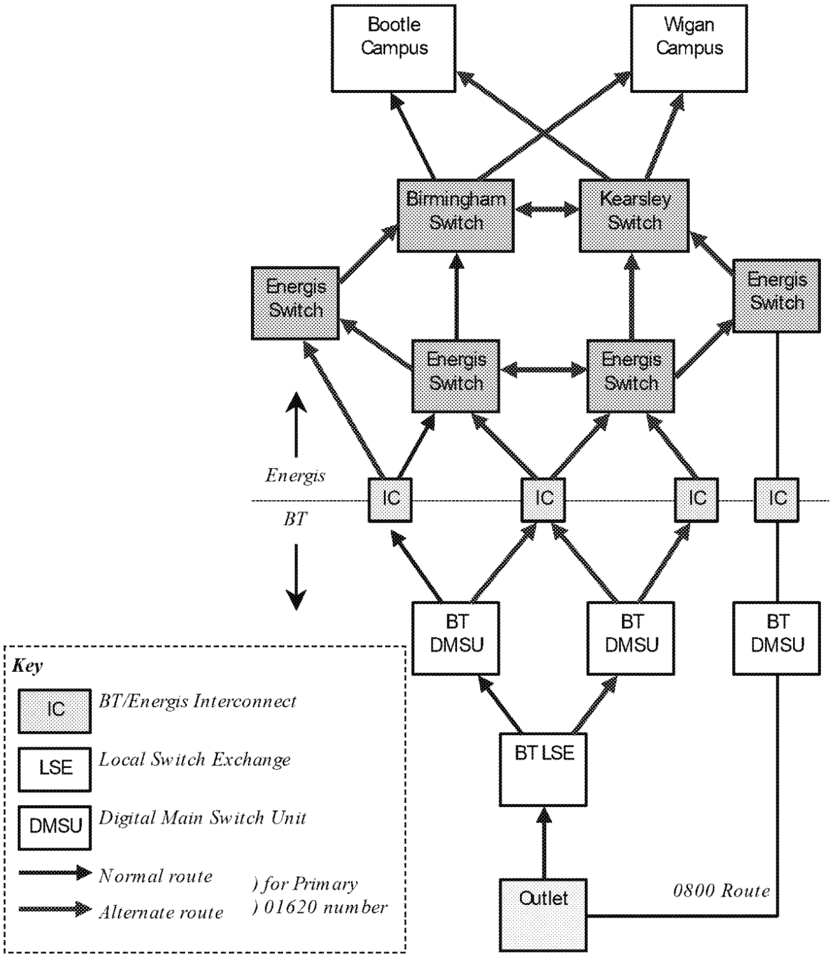

Figure 9.3 – Energis Diverse Routing

9.5.3.2 Energis Links into the Campuses

Energis provide two separate Fibre Optic cables into each Campus, each linked to a nearby *Equipment Access Module* (EAM), which forms a tap on the backbone network. The links are 12-core cables. Each is terminated at a *Synchronous Multiplexor Add-Drop* (SMA) installed in the Campus. This then connects to the Campus Routers and other equipment as shown here. The cables into the Campuses are separated by at least 20 metres.

There are two OC-3 ATM links into each Campus. The ATM links support inter-Campus traffic and go directly into a pair of ATM Switches that support:

- 34 Mbps circuits to support EMC Symmetrix disc mirroring between sites. This connects to a GSN 9800 device that converts the EMC's ESCON channel presentation to a standard E3 interface
- Catalyst 6500 LAN switches that support the Campus LANs and other inter-Campus traffic. These switches also provide a Virtual LAN (VLAN) capability between the two Campuses so that in the event of Campus failover, client applications that connect to a roving IP address do not need to be reconfigured

In addition to these, there are a number of other links as follows:

- 24 x ISDN *Primary Rate Interface* (PRI) circuits for ISDN-connected Outlets
- 1 x ISDN PRI circuit for Boot Server use during Auto-configuration
- 1 x ISDN PRI circuit for Diagnostic purposes
- 2 x 2 Mbps Frame Relay circuits for Outlets connected by this means

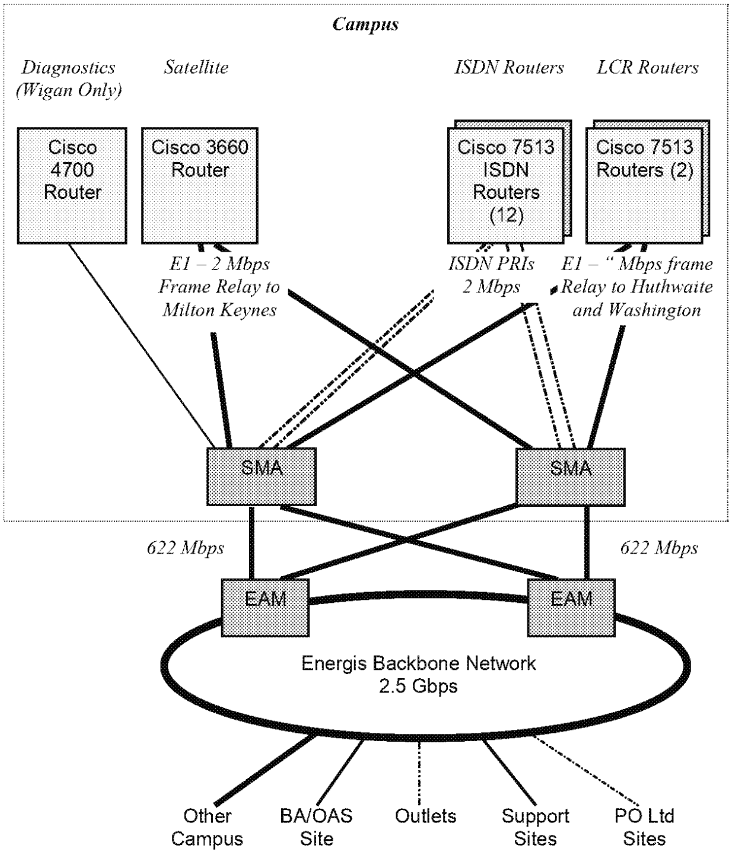

Figure 9.4 - Campus Connections

9.5.3.3 OBCS Links

Within the ENCS ACC, Pathway provides two Routers connected via a DSS-supplied Firewall to the site LAN. Firewalls play an important part in the Network Infrastructure. Their purpose, capabilities and the types are discussed in Chapter 16 "Security".

During normal operation, both links from each site are routed to the Campus where the Host applications run. Under site failover situations both links are re-routed to the other Campus.

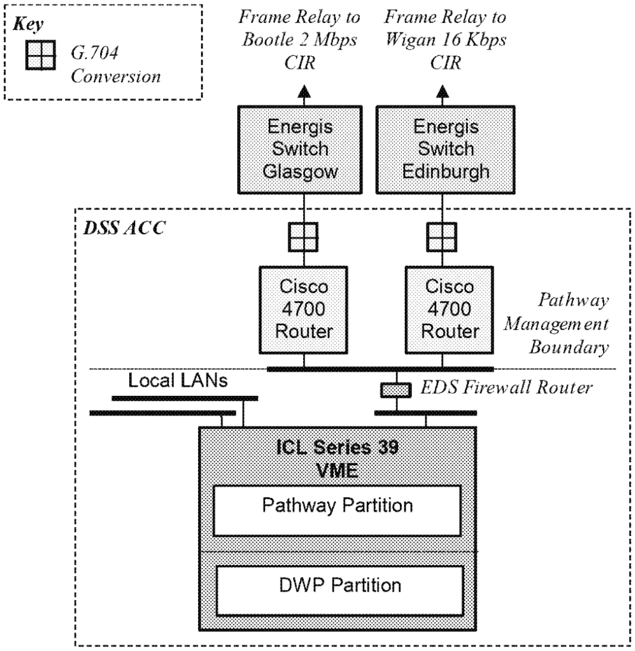

Figure 9.5 - OBCS System Links

9.5.3.4 TIP Links

The PO Ltd TIP and Reference Data systems are co-located on the same PO Ltd site at Huthwaite near Chesterfield. The same links are used for both systems. During normal operation, these are both routed to the Campus that runs the TIP Host and Reference Data Host systems. Under fail-over conditions, the links are re-routed to the other Campus.

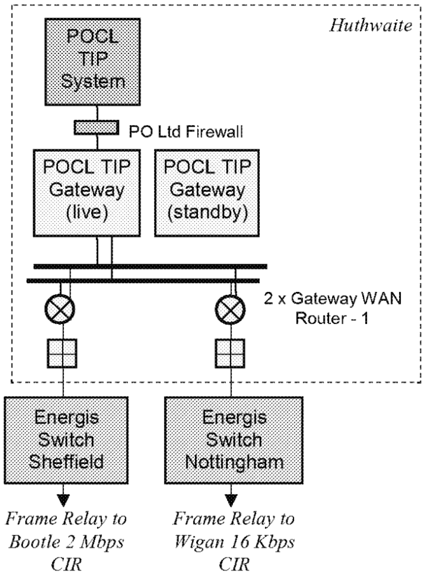
Huthwaite
POCL TIP System
PO Ltd Firewall
POCL TIP Gateway (live)
POCL TIP Gateway (standby)
2 x Gateway WAN Router - 1
Energis Switch Sheffield
Energis Switch Nottingham
Frame Relay to Bootle 2 Mbps CIR
Frame Relay to Wigan 16 Kbps CIR

Figure 9.6 - Pathway Connection to PO Ltd Huthwaite

A similar configuration is installed in the PO Ltd disaster recovery site at Isleworth.

9.5.3.5 Horizon Campus to NBE and/or MA

9.5.3.5.1 DCS De-Militarised Zone

X.25 and ISDN links are required linking the Horizon Campuses to the MA. Two 64 Kbps Kilostream links are installed at each Campus. This provides up to 1024 virtual channels (256 per Kilostream link) into the MA for Authorisation requests. Payment File delivery will be performed using ISDN dial-up. Four ISDN lines (eight 64 Kbps channels) can be bonded to provide greater bandwidth.

For security reasons, these links will terminate, at the Campus end, within a *De-Militarised Zone* (DMZ) that protects the Horizon network from intrusion attempts originating in the PO Ltd network.

A *Primary Domain Controller* (PDC) and *Backup Domain Controller* (BDC) are required within the DMZ in line with standard Pathway security practice.

The overall topology required for DCS is shown in the following Diagram. No Pathway-provided equipment is installed at the MA. Thus, the X.25 and ISDN Routers installed at the MA will be those owned and operated by SMS.

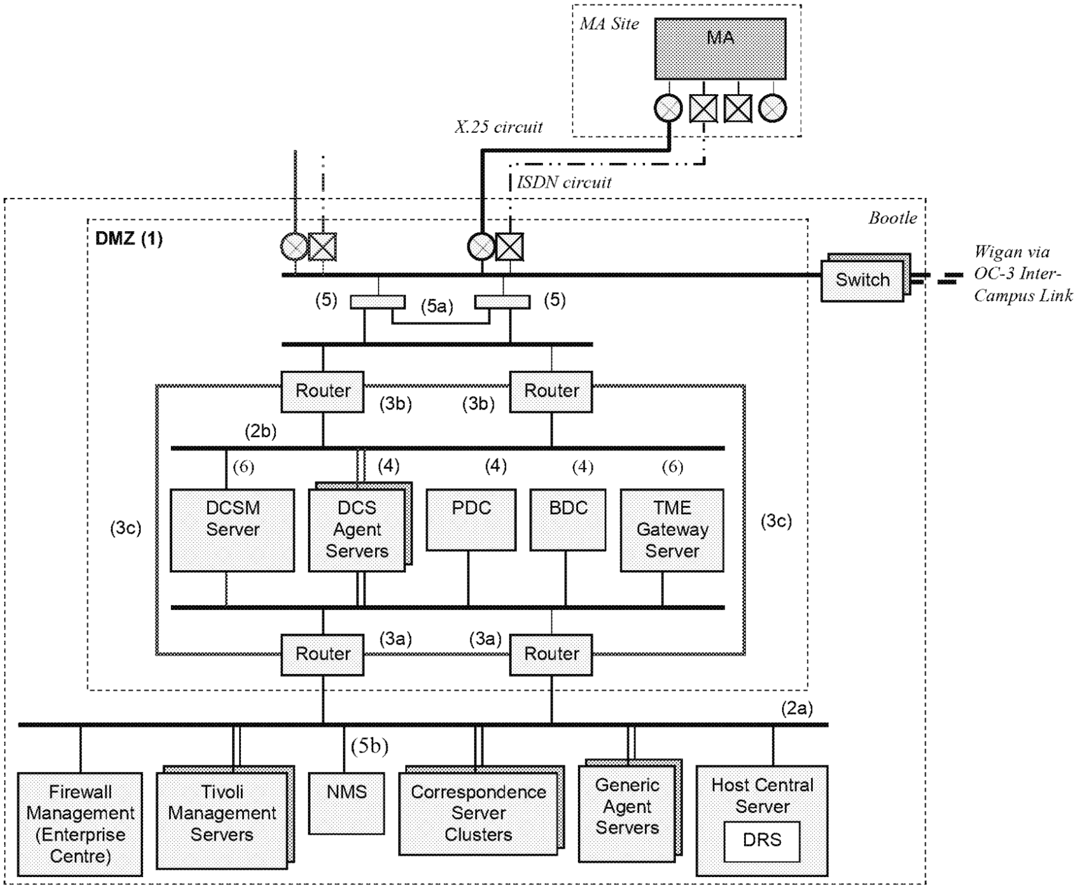

Figure 9.7 – Secure Network Architecture – DMZ

9.5.3.5.2 Joint Firewall Farm

Firewalls are used to mediate the interactions between Horizon and external sources. The principle characteristics of the Firewall are as follows.

- Applies filters to only allow authorised protocols and services for identified addresses between Horizon and the external sources
- Applies *Network Address Translation* (NAT) to conceal Horizon addresses from the external sources
- Uses Firewall clustering to provide a resilient and scalable solution (5a)
- Intrusion audit files will be transferred to a Vulnerability Monitoring Workstation (introduced at BI2) where they can be examined for Networking and Security purposes (WebTrends – Firewall Audit Analysis software). Security reports from the analysis (Alerts, alarms and responses) will be sent to Operational Security Management for review and investigation

The following diagram shows the detailed implementation of the fault tolerant firewall farm in the Campuses.

- Level 2 processing is provided by the Catalyst 6500 switches
- Levels 4-7 are provided by the *Content Services Switch* (CSS) 11050
- The NBS Internal LAN and DCS Internal LAN each comprise a cross-Campus VLAN
- As well as the Servers shown on the NBS and DCS Internal LANs, Domain Controllers and other servers will be installed as shown in Figure 9.7
- Separate Firewalls are used for NBS and for DCS. The NBS Firewalls are Cisco PIX 515Urs. Those for DCS are supplied by Nokia
- The DCS WAN Routers are Cisco 7204V XRs

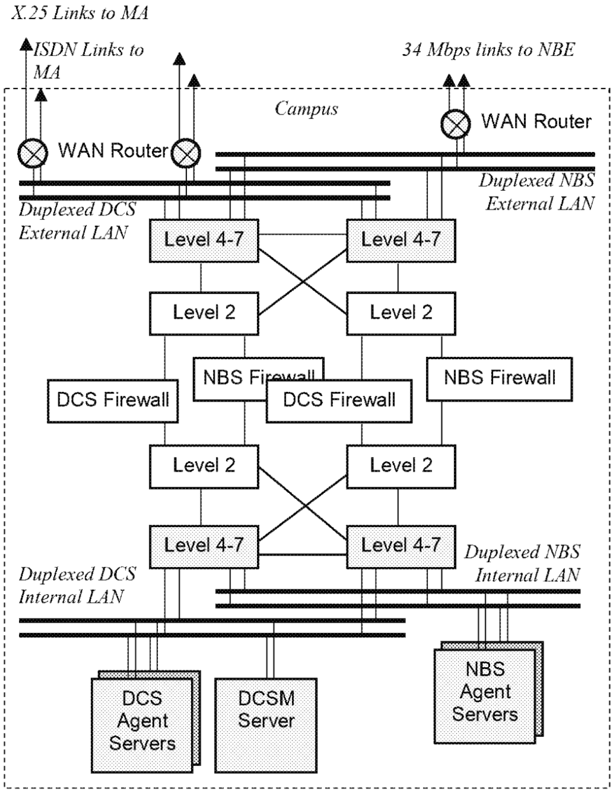

Figure 9.8 – Fault Tolerant Joint Firewall Farm

9.5.3.5.3 X.25 Connections to MA

Each DCS Agent Server will be configured to use a set of IP addresses and ports on a round-robin basis. These addresses will be handled by the two DCS WAN Routers at each Campus, which will map them to X.25 circuits on a round-robin basis.

SMS provides two Data Centres, one active and the other as standby. These share a common set of *Network User Addresses* (NUAs) that make these Data Centres, to Horizon, appear as a single Virtual Location. The DCS WAN Router will be configured to use a range of X.25 addresses, which map onto both Data Centres in a way that is not meaningful to Pathway. If it cannot make a connection to the first NUA, it will try the second. SMS provides automatic data replication between the two Data Centres, so Pathway does not need to know which Data Centre handles a particular request.

9.5.3.5.4 ISDN Connections to MA

Pathway has agreed with PO Ltd and SMS that this link will be protected by use of Microsoft Point-to-Point Encryption (MPPE). MPPE supports 128-bit encryption keys. Keys are changed by SMS on a monthly basis, and the new key is communicated by a telephone call.

These mechanisms fall well below Pathway's normal security measures, but follow normal industry practice.

9.5.4 Within each Campus

Figure 4.10 illustrates the principal LANs and platforms in the Campuses.

9.5.4.1 Campus LAN

The *Campus LAN* network is designed to support VPN.

9.5.4.1.1 Three-Layer Campus LAN

VPN is implemented in such a way that there is a three-layer Routing capability within each Campus for links to the Outlets. This is shown here in logical form.

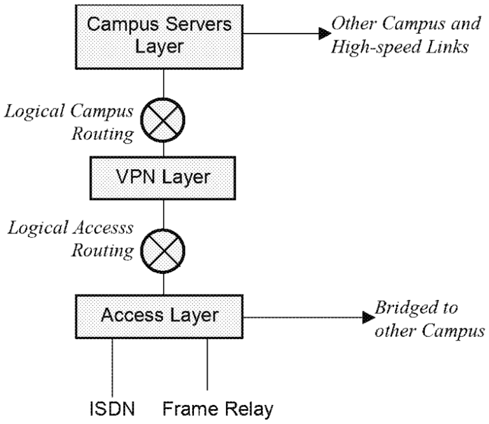

Figure 9.9 - Routing Layers with VPN

9.5.4.1.2 The Logical Campus Layer

The *Logical Campus Routing* (LCR) function fans the server traffic to a number of VPN servers. Traffic from these is handled by the *Logical Access Routing* function, which directs it via the *Access Layer* to an appropriate end-point using the ISDN or Frame Relay connection method.

The *Server LAN* connects to the Campus servers. The other layer consists of a number of LAN that are connected to the Routers providing access to external sources including the Outlets.

9.5.4.1.3 The VPN Layer

This Layer contains the VPN Servers and VPN Exception Servers.

9.5.4.1.4 The Logical Access Layer

The two layers are connected by the *Logical Access Routers* (LARs), as shown below. This provides an "indirection routing" facility, which avoids the need for the Campus servers to know the exact network route to remote locations.

9.5.4.1.5 Access LAN

There is an *Access LAN* in each Campus. The Outlets connect to this via an appropriate Router. The LAN may be bridged to the corresponding LAN in the other Campus, to simplify the dialin procedures from Outlets.

Not all of the Campus servers are located on the main Server LAN. Certain servers are located on other discrete LAN segments, separated from the Campus LAN by Routers. Separate segments are used for the following.

- The Boot Server, which is accessed directly from new Outlets
- External Interface Gateway servers
- The TME Management Servers are connected to two separate Virtual LANs that are bridged through the Campus LAN Hubs and Inter-Campus link to adjoin the similar LANs in the other Campus.
- The VPN Servers are similarly bridged via a VLAN to the servers in the other Campus.
- The KMA Servers are also bridged via a VLAN to provide a single IP address for clients to use. This address is switched to the failover server should this be necessary.

Inter-connection within the Campuses uses Fast Ethernet (100baseT). This has low latency and is therefore good at handling short discrete messages. It also has a high bandwidth.

9.5.5 Low Speed Links

Low-speed links are defined as dial-up connections, or permanent circuits at less than 2 Mbps. These links are used for the following low-volume applications.

- POCL AP Clients
- Pathway's Suppliers
- Pathway development and support sites
- Pathway's Support Organisations
- Help Desk

Where link encryption is required, a permanent circuit is used. Otherwise, ISDN dial-up connections are used.

9.5.5.1 Horizon to PO Ltd AP Clients

Horizon communicates directly with the PO Ltd AP Clients. Pathway provides a managed service on the Client premises. This consists of an AP Client Gateway with an ISDN card. It connects via ISDN to a Campus Low Speed Router. Data is digitally signed.

In some cases, a second set of platforms is installed at the Client's Disaster Recovery site.

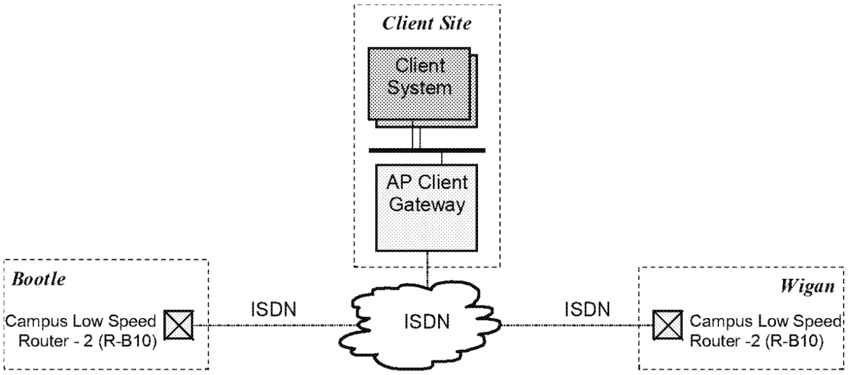
Client Site
Client System
AP Client Gateway
Bootle
Campus Low Speed Router - 2 (R-B10)
ISDN
ISDN
ISDN
Wigan
Campus Low Speed Router -2 (R-B10)

Figure 9.10 - Horizon Connection to AP Clients

9.5.5.2 The Campuses to Pathway

9.5.5.2.1 Feltham

Encrypted Megastream lines are used between Pathway's Feltham HQ and the Campuses. Further encrypted WAN links are used to connect Feltham to the Pathway SSC at Bracknell.

A secure LAN in Feltham contains the systems used by the Key Management teams.

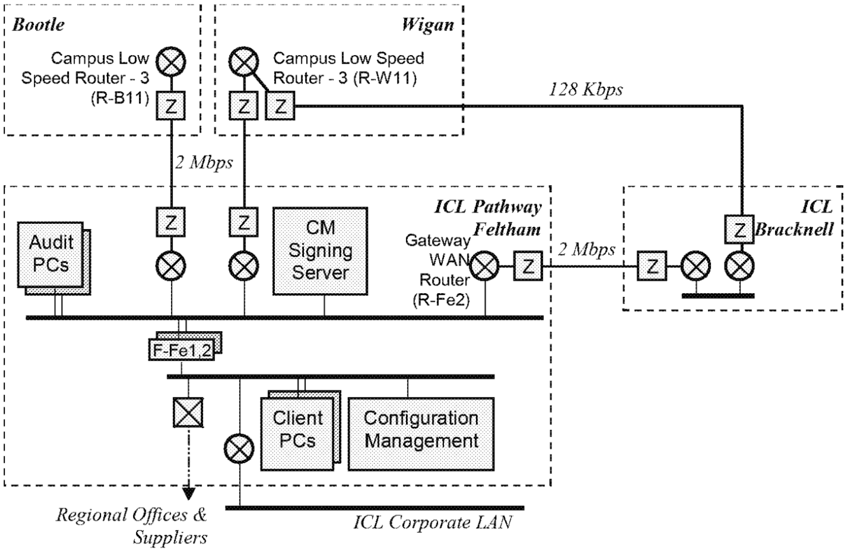

Figure 9.11 - Pathway HQ connections

Client PCs are used by Pathway management to access the applications that run on the Data Warehouse system. Audit Workstations in a secure area can retrieve and analyse audit information from the Audit Server.

9.5.5.2.2 Bracknell

Bracknell contains two Pathway units:

- The SSC, responsible for support of the live systems
- CS, responsible for Customer Support

The connections are as follows.

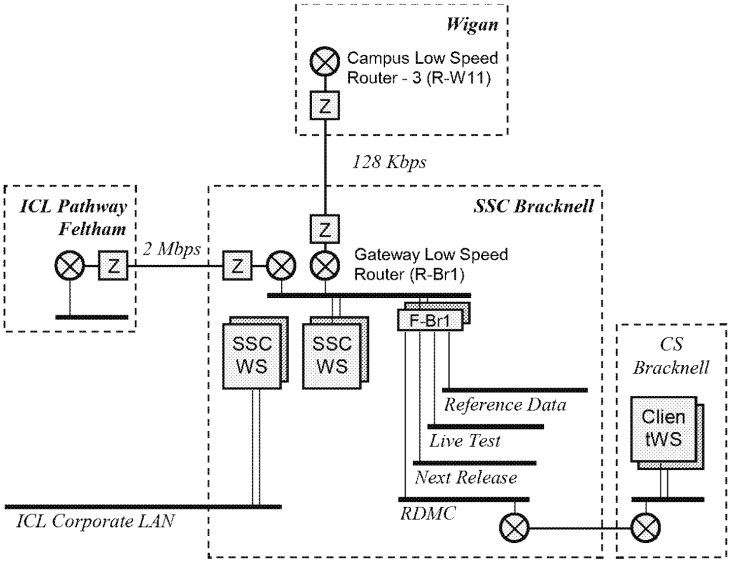

Figure 9.12 - Pathway Bracknell connections

Some SSC Workstations have controlled access for maintenance purposes via the Live Test Environment and a dedicated, encrypted link to Wigan. Others can access the Fujitsu Services Corporate LAN. None can access both.

9.5.5.3 Pathway to its Support Organisations

9.5.5.3.1 Fujitsu Core Services (FSCS)

FSCS sites at Stevenage, Bracknell and Lytham St. Annes carry out systems management of the Horizon infrastructure. FSCS is also responsible for the day to day operation of the Campus servers. All these links are encrypted.

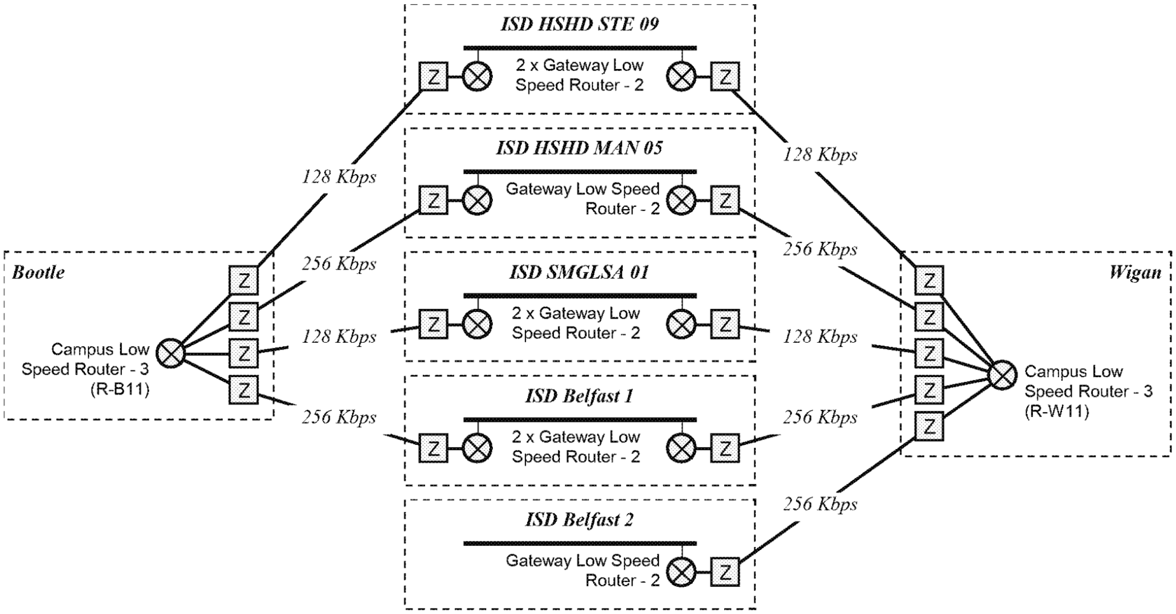
ISD HSHD STE 09
2 x Gateway Low Speed Router - 2
ISD HSHD MAN 05
Gateway Low Speed Router - 2
ISD SMGLSA 01
2 x Gateway Low Speed Router - 2
ISD Belfast 1
2 x Gateway Low Speed Router - 2
ISD Belfast 2
Gateway Low Speed Router - 2
Bootle
Campus Low Speed Router - 3 (R-B11)
Wigan
Campus Low Speed Router - 3 (R-W11)
128 Kbps
256 Kbps
128 Kbps
256 Kbps
128 Kbps
256 Kbps
128 Kbps
256 Kbps
256 Kbps
Z

Figure 9.13 - FSCS links to Pathway

9.5.5.3.2 EMC

EMC support the Symmetrix disks used on the Host Central Servers. These disks are monitored by an internal system. On a disk or controller failing or exceeding a predefined threshold, the system automatically dials the EMC support unit in Cork, Eire. Support staff can then:

- Investigate the fault through the automatic connection, with read access
- Request an on-line connection from FSCS
- Visit the Campus

9.5.6 Between the Campuses and the Outlets

Communications with the Outlet should support a high bandwidth (Kilostream speeds) with low cost and low set-up time.

ISDN is the preferred medium as it supports 64 Kbps communication. It provides speedy connection for “burst” type communication. “Nailed up” (permanent) connections are used for a portion of the Outlets, using FRIACO services provided by Energis.

Satellite links are used for Outlets with no ISDN availability. The link presents a Frame Relay interface to the Counter.

9.5.6.1 History

The original Horizon system was designed around a scenario in which the bulk of transactions in the Outlets did not need an on-line interaction with the Campus. Only around 2% of transactions (OBCS Foreign Encashments) did require an on-line response, and there were fallback procedures should this not be available.

With the advent of the NBS and DCS services in BI3, the proportion of off-line to on-line transactions has changed radically, and this has had a significant impact on the nature of the ISDN network. Both NBS and DCS make an immediate call to the Campus to obtain an authorisation, and if the network connection is not available then the transaction is terminated. To cope with these changes in the requirements on the Outlet network, a number of architectural changes have been made.

- The network, which previously used the BT/Energis ISDN voice network, has been redesigned to use a data network. The data network is designed primarily for access to Internet Service Providers, and is *asymmetric*, in that it provides "dialin only" access. Thus, the situations in which the Campus may make a call to the Outlet have been reworked to ensure that an inward call (Outlet to Campus) is made instead
- To reduce the call latency and chances of being unable to make a call when required, a number of Outlets are configured to be permanently connected forall or part of the day. The proportion of Outlets that behave in this way, their identities, and the exact behaviour, are configurable. Essentially, the Outlet makes a call and never terminates it until the permanent connection window is past. If the call fails for any reason, it is immediately remade by the Outlet
- Where business levels justify it, the Outlet will use a FRIACO "unmetered" connection, where calls are terminated at a fixed port within the Campus and the cost is for the rental of the port rather than of the connection itself

The detailed arguments in favour of this approach are discussed in [SDSINF].

9.5.6.2 ISDN at the Outlet

One Counter PC in each Outlet (the Gateway PC) is fitted with an ISDN adapter card. This PC is configured as an IP Router, and is declared as the default Router for each other Counter PC in the Outlet. The *Counter Network Information Monitor* (CNIM) within the Gateway PC will automatically set up an ISDN call when a datagram needs to be sent to a Campus and a connection does not already exist, and keep it open during a configurable time window.

If the line is not permanently connected, a connection will be made when a real-time message is generated, or at a scheduled interval. Once the line is open, any Riposte messages that have been waiting are also transmitted. When the transmission is complete, the line closes after waiting for a short inactivity time-out to occur (subject to attaining the minimum call duration needed to permit ISDN router optimisation to work). This inactivity timer is set to a longer value than any real-time message's timeout value at the Campus.

This control mechanism is not used for Systems Management applications. To them, the ISDN connection is just an IP Router and the line is opened whenever access is required.

Each Outlet is configured with a set of four telephone numbers to call, in a predefined order. Where the Outlet is configured to support a permanent connection, two of these numbers may map on to the FRIACO ports at the Outlet's primary Campus. If this fails, the Outlet tries first a different Router and then the other Campus.

9.5.6.3 Use of FRIACO Service

At BI3, the ISDN network is modified to use the Energis provided FRIACO service.

9.5.6.3.1 Point to Point Tunnelling Service

The ISDN solution is based upon *Point-to-Point Tunnelling Protocol* (PPTP). A Counter PC wishing to connect to a Campus from a remote location would normally require a long distance telephone call, as shown here.

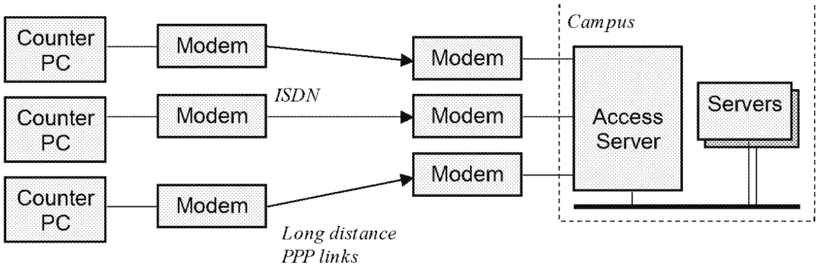

Figure 9.14 – Remote Access Without Point-to Point Tunnelling Protocol (PPTP)

With PPTP, it connects instead with a local *Internet Service Provider* (ISP). The Counter then obtains a virtual connection to the Campus. Thus, only a local call is made, via ISDN or the *Public Switched Telephone Network* (PSTN) to the local DLE, and the call is forwarded to the data network of the supplier. This is determined by the "destination" number being called.

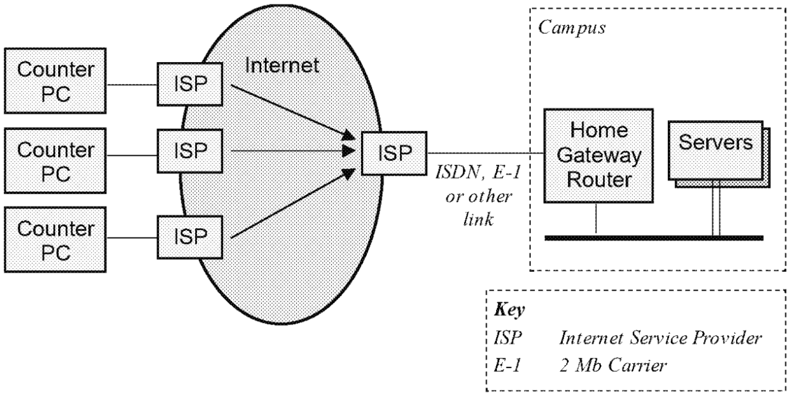

Figure 9.15 – Remote Access With Point-to Point Tunnelling Protocol (PPTP)

With a FRIACO service, the primary protocol used is the IETF *Layer 2 Tunnelling Protocol* (L2TP). A typical Internet connection for a dial up user involves the *Point-to-Point Protocol* (PPP). This allows users to run TCP/IP. The TCP/IP packets are put into PPP frames for transport across the dial-up link to an ISP. The ISP then extracts the TCP/IP packets and forwards them onto the Internet.

L2TP enhances PPP by providing a way for a remote user to extend a PPP link across the Internet all the way to a target site. A tunnel is established from the ISP to the Campus, and frames are transmitted through the tunnel. Once the tunnel is established, the ISP is out of the picture and the user communicates with the target site over what appears to be a direct dial-up connection.

The network provider's *Remote Authentication Dial-In User Service* (RADIUS) authenticates the call and ascertains where the target *Home Gateway Router* (also known as the *L2TP Network Server Router* (LNS)) resides and how to get there. The LNS Router connects onto the target site's LAN onto which the Routers present the data IP packets as initiated by the Counter PC.

The standard FRIACO service provides the following:

- Two connections to the host site, terminating with two LNS Routers, thus providing resilience
- Appropriate bandwidth as determined by the number of FRIACO ports purchased
- Management of the LNS Routers
- Management of the Network RADIUS server
- Management of the IP Data network

9.5.6.3.2 FRIACO L2TP service

The solution adopted by Pathway enhances the strategy described above, by moving the tunnel termination into the Campus. This allows Pathway to implement and manage the LNS Routers (which terminate the tunnels) so that they co-exist with the Campus network and whatever local routing protocols are required. Pathway uses the *Open Shortest Path First* (OSPF) protocol within the Campuses.

The termination point for the L2TP tunnel is a *L2TP Network Server* (LNS). The LNS operates on any platform capable of PPP termination. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS may have a single LAN or WAN interface, yet still be able to terminate calls arriving at any of the LAC Router's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). A high-speed connection between the supplier's data network and the target site (typically 34 Mbps or 155 Mbps) terminates on the target site at a Feed Router. Calls are authenticated by a RADIUS server, and then fed to the LNS routers via a Fast Ethernet connection.

9.5.6.3.3 Call Routing

The call from an Outlet on the FRIACO service goes to a BT DLE at which there are at least two Energis owned, E1 circuits (2 Mbps) which connect to one of two main Energis switching centres, namely Birmingham and Watford. Each BT DLE connects to one or the other of the Energis switch centres, but not both. However, the E1 circuits terminate on separate Switches within an Energis switch centre. There are two *Configuration Policy Manager* (CPM) systems located within Energis. These control and analyse customer network usage. The main function of the CPM is for the control and management of VPN tunnels created from the Outlet through to the LNS routers for VPN tunnel termination. The CPM servers communicate with each other to maintain continuity in case one of the CPMs fails.

The Campus uses *Calling Line Identity* (CLIP) to determine the Outlet that originated the call.

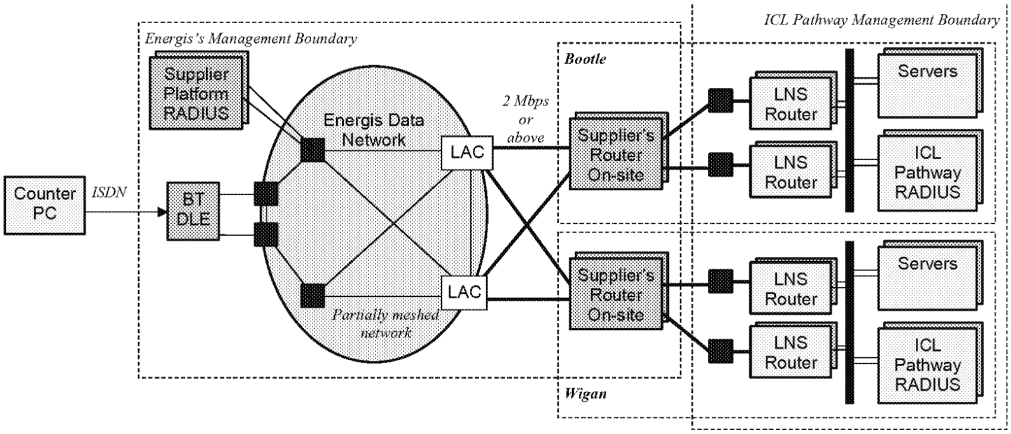

Figure 9.16 – Resilient Feeds and Dual LANS

At the Campus, FRIACO services are presented in the same way as ISDN connections.

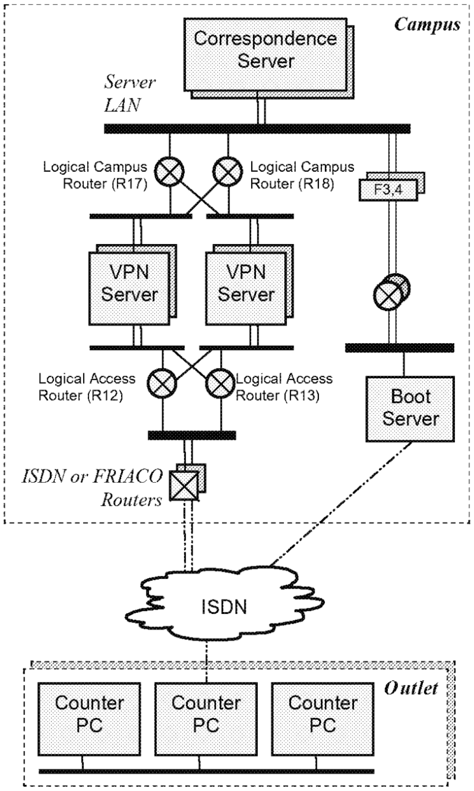

Figure 9.17 - ISDN Connections to the Campuses

Because ISDN is a dial-up network, special VPN security measures are needed to ensure that a call to the Campus comes from an authentic Outlet. These measures are described in Chapter 16 “Security”.

When the Counter is first installed, it connects to the Boot Server in one of the Campuses. This carries out the steps necessary to implement these security measures, and thus allow the Outlet to connect to the Correspondence Servers on subsequent connections. Connections to the Boot Server are protected by Firewalls from accessing the main Server LAN.

Subsequent access from Counter PCs to Correspondence Servers is routed via the Logical Access Routers to the main Server LAN.

9.5.6.4 Satellite Communication

Outlets that cannot be reached by ISDN are connected by Satellite. Each such Outlet is supplied with a Portable Earth Station (PES) that connects into a Frame Relay router within the Outlet. Communications links are supplied via a satellite owned by Hughes Olivetti Telecomms. The other end of the link is at Hughes' site in Milton Keynes. There, a pair of 2 Mbps links funded by Pathway are used to connect to a a pair of Frame Relay Routers in the Campuses.

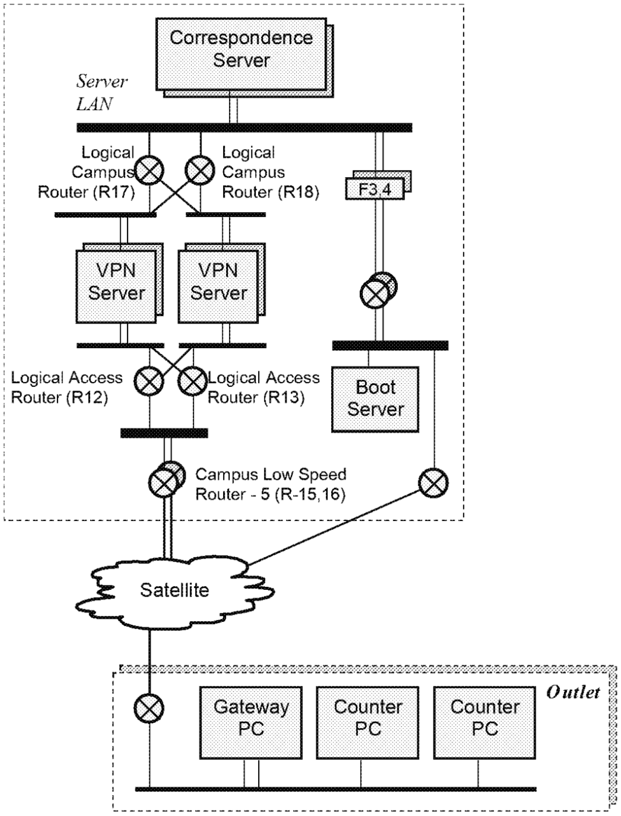
Correspondence Server
Server LAN
Logical Campus Router (R17)
Logical Campus Router (R18)
F3.4
VPN Server
VPN Server
Logical Access Router (R12)
Logical Access Router (R13)
Boot Server
Campus Low Speed Router - 5 (R-15,16)
Satellite
Outlet
Gateway PC
Counter PC
Counter PC

Figure 9.18 - Satellite Connections to the Campuses

Each Outlet contains a single Frame Relay Router, connected to the Outlet LAN.

Two *Campus Low Speed Routers* are provided at each Campus and dedicated to Frame Relay traffic to and from the Outlets. Each has three 2 Mbps connections to the Hughes Olivetti ground station. Each Gateway PC is configured with three dedicated PVCs: two to its preferred Campus, and one, as fallback, to the other Campus. The Gateway PC has two LAN cards. The VPN software is bound to one and the other is used for intra-Outlet communication.

Other Counter PCs have the Gateway PC declared as their default Gateway Router.

9.5.7 Within each Outlet

Where there is more than one Counter PC in an Outlet they are inter-connected with a LAN using 10baseT. Where there are only two Counters, their LAN cards are connected directly via a crossover lead. For other offices, one or more small (eight-port) Ethernet hubs are used.

Note that Satellite connected Outlets are all single-Counter.

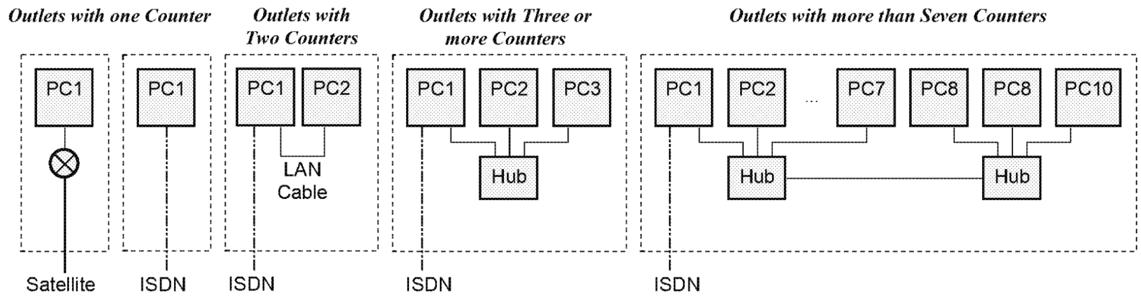

Figure 9.19 - Intra-Outlet Communications

The Counter peripherals use serial connections.

9.6 INTERCONNECTION SERVICES

9.6.1 Links Within the Horizon Network

The major protocol used within the Horizon network is TCP/IP, with Riposte mainly using UDP over IP. Each Platform has one or more IP addresses. All Counter PCs (even those in single-Counter Outlets) are fitted with an Ethernet card to provide an identifying IP address. The subnet mask used is 256.256.256.0, thus allowing a maximum of 254 Counters per Outlet.

Other protocols are used for specialised purposes, including *Simple Network Management Protocol* (SNMP).

9.6.2 Links to External Locations

The usual communication method to external bodies is via the Windows NT file copy process, running over TCP/IP.

9.6.3 Links Between Campuses and Outlets

Riposte communications use a connectionless, best-effort messaging model, based upon UDP/IP. This uses the Windows Sockets 2.0 implementation. Each Counter PC has its own IP address.

Communication between Counters also uses UDP/IP.

9.6.3.1 UDP over ISDN

The ISDN card in the Gateway PC at the Outlet is configured as an IP Router with its own IP address. In a multi-Counter Outlet, this connection is configured as the default

Router for each other Counter PC. Messages from Outlets are transmitted to both Campuses, and to all interested Correspondence Servers. Messages from Correspondence Servers to Outlets are directed to the IP address of the Gateway PC in the Outlet, which is known to each Correspondence Server.

The ISDN Card in the Gateway PC uses a *Network Device Interface Standard* (NDIS) driver that enables the card to behave as a normal LAN connection. The driver manages the dialup, connection establishment and connection termination activities. Thus, ISDN call set-up is done automatically when the Gateway PC sends a message over the link. Similarly, a call is set up (if none exists) when a Correspondence Server sends a message to an Outlet.

To avoid too frequent calls, Riposte only sets up a call when an urgent message has to be passed in either direction, or when a normal message has to be passed and a "handshake" timer expires. The timer starts at the completion of the transfer of the previous set of messages. If there are no messages to pass, no call is made, so a small rural Outlet may not catch up until the end of day.

Once a call has been established then all waiting messages are transferred in both directions. The call is cleared down on expiry of an idle timer with a default setting of twenty seconds. An implication of this process is that *all* communications traffic between the Outlets and the Campus must go via Riposte.

There is thus usually some delay between a message being created at a Counter position and that message reaching the Campus. The resilience and recovery implications of this are discussed in Chapter 13 "Availability".

This process is designed to ensure that the fifteen-minute calls from Outlets are spread out in a random pattern. Applications must avoid any measure (such as a timer-based Priority Message) that could have the effect of "bunching" calls to the Campuses. In particular, End of Day messages must not be Priority messages.

9.6.3.2 UDP over Frame Relay

UDP/IP is also used to Outlets connected by Frame Relay. Correspondence Servers do not need to know the link level connection method to an Outlet.

Messages from the Outlets use Multicast facilities (implemented below the Riposte level), thus ensuring that they go to each Campus and to each interested Correspondence Server. This differs from the ISDN case, where the Outlet connects to only one Campus.

9.6.4 Virtual Private Network (VPN)

A *Virtual Private Network* (VPN) service is used between the Outlets and Campuses. This provides a means of making a "tunnelled" connection through the IP connection from Outlet to Campus.

9.6.4.1 Operation of a VPN Connection

The usual passage of a datagram from one system (System A) to another (System B) is shown here. The datagram contains a *destination address* (here 1.2.3.4) and a *payload*.

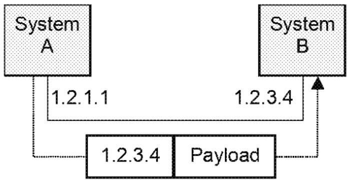

Figure 9.20 - Simple IP Datagram

Where the transfer is via a VPN circuit, the datagram is transmitted via a standard IP Gateway server at each end of the connection. The Gateway has two network connections, each with a different IP address. IP forwarding is enabled. The situation is as follows.

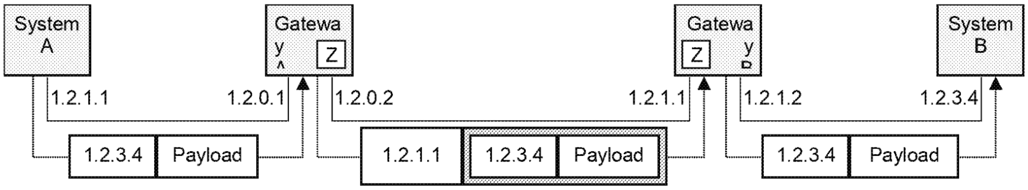

Figure 9.21 - IP Datagram Forwarding

In normal TCP/IP usage, the Gateway node knows that the destination of the datagram is not on its own subnet. It passes it to another gateway node which, it hopes, will either have a direct connection to the destination, or can pass it to another gateway. The datagram passes unchanged through each gateway.

VPN takes advantage of this. Each Gateway node is supplied with two network connections. A component inserted on the outward-facing network connection "encapsulates" the original datagram within the payload of the message sent from Gateway A to Gateway B. The destination address within the transmitted datagram is that of Gateway B.

This component is indicated by the box marked "Z" on the diagram. It enables the forwarded packet to be encrypted using a Symmetric Key known only to the two Gateways. This is indicated by the green (darker) envelope round the original datagram.

Gateway B also contains an Encryptor component. If this can decrypt the datagram, using their shared Key, it knows *ipso facto* that the datagram originated at the Gateway A, and can forward it to its destination. This is true regardless of the communications medium between the two Gateways. Further, the fact that the whole of the target IP address will be within the encrypted payload means that it will not be visible to anyone eavesdropping on the communications link.

9.6.4.2 Benefits of VPN

This mechanism operates regardless of the communication medium used, and thus can be used with ISDN and Frame Relay.

It provides *de facto* authentication of both ends of the link. ISDN communication normally uses CHAP authentication, though this is flawed. Using VPN removes the need for CHAP. There is no equivalent to CHAP for Frame Relay, and thus the use of VPN gives the ability to provide adequate line authentication on these links.

9.6.4.3 VPN Structure

Component	Platforms
VPN Config Application	Counter PC
	VPN Policy File Management Server
VPN Counter Configuration	Counter PC
VPN EWYC Watcher Application	VPN Server
VPN Loopback Workstation Configuration	VPN Loopback Workstation
VPN PMC Pin Reader Application	VPN Exception Server
	VPN Loopback Workstation
	VPN Policy File Management Server
	VPN Server
VPN Policy Management Client Application	VPN Exception Server
	VPN Loopback Workstation
	VPN Server
VPN Policy Management Server Application	VPN Policy File Management Server
VPN Policy Management Server Configuration	VPN Policy File Management Server
VPN Remote Management Client Application	SSC Support Workstation
	VPN Exception Server
	VPN Server
VPN Remote Management Service Application	VPN Exception Server
VPN Server Configuration	VPN Server
VPNConfig	Counter PC
	Short-term Performance Database Server

9.6.4.4 VPN in the Campuses

Each Campus contains a number of *VPN Servers*. This reflects the logical three- layer model shown in Figure 9.9. These Platforms run under Windows NT Server. Two banks of these are provided, for resilience, with each bank linked to two LANs.

9.6.4.4.1 Clear LANs

The *Clear LANs* are linked via a pair of Logical Campus Routers to the duplexed Campus LAN. The purpose of the Logical Campus Routers is to load-share the network traffic across the bank of Gateway servers, and provide resilience to the failure of any of these.

9.6.4.4.2 Encrypted LANs

The other LAN on each gateway bank is the *Encrypted LAN*. All traffic across this is encrypted by the VPN Servers, using a session key derived from the Outlet's unique Key. The VPN Servers do not do any routing, They encapsulate outgoing traffic with a destination gateway address. Thus, the Encrypted LANs are linked to two *Logical Access Routers,* which handle the routing of traffic to Outlets via an appropriate communications medium. The Logical Access Routers check that all incoming traffic from remote locations is targeted at the Encrypted LAN. They discard other incoming traffic.

9.6.4.4.3 VPN Policy File Management Service

A VPN Policy Management Server acts as a central policy manager and controls the set of Outlets that are accessed via VPN. It accepts data feeds from Tivoli and OCMS of steady state changes.

9.6.4.4.4 VPN Policy File Management Client

Other VPN platforms contain a *VPN Policy File Management Client* that communicates with the server and ensures that the platform has an up-to-date copy of the VPN Policy File.

9.6.4.4.5 Loopback Workstation

A VPN Loop Back Workstation is used to enable Network Management Stations to verify that they can communicate with encrypted services.

9.6.4.4.6 Load Balancing

The Outlets are assigned to VPN Servers in a way that ensures that the Outlet load is balanced across the available servers.

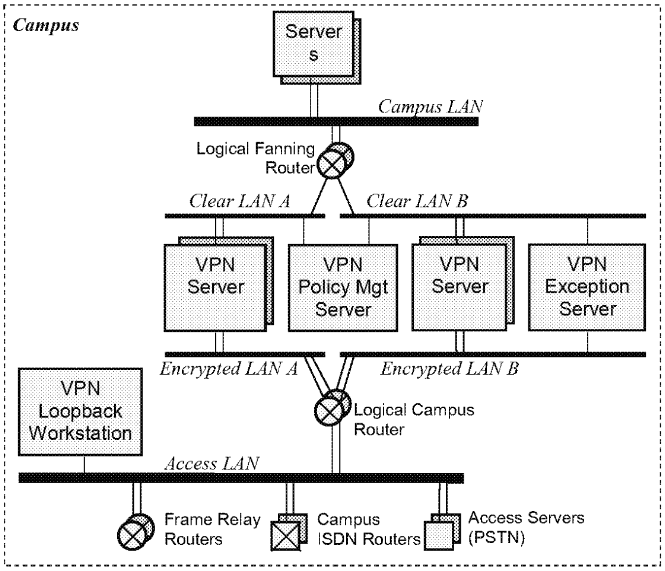

Figure 9.22 - Campus Use of VPN

9.6.4.4.7 VPN Driver

Within the VPN Server and VPN Exception Server, the VPN Driver is bound to the encrypted LAN card. It uses the destination IP address to determine the "tunnel" IP address to be used for the destination.

9.6.4.4.8 VPN Red Pike

The VPN product has been enhanced for Pathway to support replaceable Crypto algorithms. This module implements the CESG-mandated Red Pike algorithm.

9.6.4.4.9 Key Management

VPN Keys are generated by a Utimaco Key Generator, which is co-located with the CA Workstation. Keys are distributed by the KMA Server and carried via Riposte.

The Outlet's unique Key is delivered to it during the installation or upgrade process, and is stored on the Post Office Manager's PMMC.

9.6.4.4.10 Key Recovery

An Outlet that is *being* installed, or upgraded, or in which the Post Office Manager has mislaid the PMMC, will not be able to carry out a normal encrypted communication with the Campus. To cater for this, each Campus contains a *VPN Exception Server*. This is used by Outlets that do not have a private Key. It contains a *KMS Proxy Server Function* that relays the data traffic direct to the KMS Server. This server then delivers a new Key to the Outlet. This process is described in [KMPROXY].

9.6.4.5 VPN in the Outlets

9.6.4.5.1 VPN Filter Driver

The VPN Filter Driver also runs within the Gateway PC and is bound to the Campus-facing *Network Interface Card* (NIC). This ensures that traffic from *any* Counter PC is encrypted across the communications link to the Campus. The Gateway PC in multi-Counter Outlets has two NICs so that communication *between* Counters is not encrypted.

The Gateway PC contains a VPN Private Key that is supported by an X.509 Certificate. The Private Key is used to construct a *Session Key* that is used to encrypt all communications over the VPN channel.

9.6.4.6 Establishing VPN Communication

The use of VPN requires the two ends of each link to agree a session key that is used to encrypt all subsequent communications. The process of establishing the key must itself be encrypted. This process is discussed in Chapter 16 “Security” and described in detail in [VPN].

When first installed or if the Private Key is lost, a pre-installed Exception Key is used. Traffic using this Key is directed by a VPN Exception Server to the KMA Server, which delivers a new Private Key to the Outlet.

Whether or not the Gateway Server encrypts an outgoing message, or attempts to decrypt an incoming one, is determined by a *Policy File* and can vary depending on the remote IP address. Thus, during the initial implementation of VPN, it was used for some remote addresses (for example those of the Outlets with VPN installed) but not for others.

9.6.4.7 Utimaco VPN Software Structure

The following software is provided by Utimaco, and installed on the platforms specified to support the use of VPN.

Component	Platforms
Utimaco Cryptware PKI (CA/RA)	CA Workstation
Utimaco Cryptware Toolkit Runtime	CA Workstation
Utimaco Key Generator	CA Workstation
Utimaco Registration Authority Batch (RAB)	CA Workstation
Utimaco SG VPN	VPN Exception Server VPN Loopback Workstation VPN Policy File Management Server VPN Server
VPN Red Pike Driver	Counter PC VPN Exception Server VPN Loopback Workstation VPN Server

9.7 INTERWORKING SERVICES

The following classes of Interworking Services are used.

- Distributed Application Support
- Terminal Handling Services
- Message Handling Services
- File Transfer Services
- Management and Directory Services

9.7.1 Terminal Handling Services

Terminal Handling Services are used only for direct (X-terminal) access to the Host Central Servers, Data Warehouse Server and Routers. This is needed so that FSCS in Belfast can operate these servers.

Network Routers and Firewalls support Telnet connections from the Network Management System. This is located within the Campus.

9.7.2 Message Handling Services

The RMS provides a sophisticated messaging service between Counters and Correspondence Servers. This is described in Chapter 6 "Distributed Application Services".

9.7.3 File Transfer and Access Services

Horizon makes major use of File Transfer services, in particular between Pathway and its suppliers and Clients.

9.7.3.1 File Transfer Managed Service

These services are organised by the FTMS, which is described in Chapter 5 "Application Architectures". The file transfer protocol is the Windows NT file copy.

9.7.3.2 File Transfers Within Client Sites

Where the file transfer is via an External Interface Gateway, the Client Systems access the remote Gateway using an appropriate file transfer mechanism. Those supported on the Pathway supplied Gateways are as follows.

9.7.3.2.1 FTP

This uses the standard Windows NT FTP over TCP/IP.

9.7.3.2.2 NFS

NFS over TCP/IP is provided by the PC-NFS for Windows NT product from Hummingbird

9.7.3.2.3 ZIP Drive

Though not strictly a file transfer product, in certain cases files are transferred across an "air gap" by a removable Zip or Jaz drive

9.7.3.3 File Transfers to and from Sequent Servers

9.7.3.3.1 Hytec FTF

The *Hytec Sonnet* FTF product is used, running over ptx/OSI, is used on the Host Central Servers to transfer data directly to and from the DSS VME systems. This uses OSI/Null Internet as that is supported by VME, and Tivoli is not involved in these links.

9.7.3.3.2 Sequent NFS

File transfers within the Campuses (for example to External Interface Gateways) are handled by Sequent's ptx/NFS.

9.7.4 Management and Directory Services

9.7.4.1 Management Services

9.7.4.1.1 Tivoli

Management facilities are provided by the Tivoli Management Environment; see Chapter 12 “Systems Management”. The Tivoli Management Infrastructure provides common facilities for management information to pass between managed and managing nodes.

9.7.4.1.2 Time Services

As discussed in Chapter 12 “Systems Management”, servers in the Campuses co-ordinate their clock times with a local Time Server which in turn sets its clock by reference to GPS satellite signals.

9.7.4.1.2.1 Network Time Protocol (NTP)

This is the protocol used by other servers to co-ordinate with the Time Server. It runs over TCP/IP. NTP includes sophisticated facilities enabling a server to estimate its time from a number of sources that may be some distance away with unknown network delays. These facilities are not required because the Time Server is attached to the same Campus LAN as the servers that require its services.

NTP was developed by the University of Delaware, and implementations of it are effectively “freeware” for which no royalties are payable nor any support available.

9.7.4.2 Firewalls

9.7.4.2.1 General

Firewalls protect portions of the Campus network from invalid access by users outside those network portions. In particular they protect the Horizon network from users outside that network. Though not strictly an Interconnection Service, Firewall technology is used because of limitations with the TCP/IP based Interconnection Services. It is thus appropriate to describe it here. The need for, and exploitation of, Firewall services is covered in Chapter 16 “Security”.

9.7.4.2.2 Types of Firewall Facilities

A number of types of facility are provided by Firewalls.

9.7.4.2.2.1 Packet Filtering

Network Routers that do Packet Filtering can decide whether or not to pass a packet based on its source IP address, destination IP address and IP port number. This is highly effective but difficult to configure properly, though products such as Cisco Works can help by displaying a graphical picture of the Network. Packet Filtering is used by the WAN Routers in the Campuses.

9.7.4.2.2.2 Application Gateways

Application Gateways are provided by computer systems specifically introduced between two networks to control the traffic between them. They handle TCP/IP traffic, and monitor all the traffic flowing over a particular connection. They thus have the ability to filter traffic at the application level, and are not restricted merely to its IP addressing details. They take the form of miniature versions of the application. For example, an FTP Firewall consists of a mini FTP service running within the Firewall. These devices are usually used in conjunction with a Router.

They have the ability to re-address TCP/IP traffic, so that outgoing traffic appears to have originated with the Firewall, rather than at the internal host or client.

However, Application Gateways have the disadvantage that the user must know it exists, and connect to it before making any outside connection.

9.7.4.2.2.3 Transparent Application Gateways

These products provide *transparency*, allowing applications to connect to addresses on the other side of the Firewall without being aware of its existence (unless, of course, the Firewall refused the connection).

9.7.4.2.2.4 Stateful Packet Filters

This technology builds on the basic Packet Filtering method. It attempts to make sense out of higher-level protocols, and adapt filtering rules to accommodate protocol-specific needs (e.g. handling simulated connections for connectionless protocols such as NFS). It can also be applied to UDP, and has the effect of setting up a type of Virtual Session.

9.7.4.2.2.5 Network Address Translation

This conceals internal IP addresses (i.e. those within the controlled Domain) from the outside world. It maintains the integrity of the internal addressing scheme, mapping external IP addresses onto valid addresses for full access.

Dynamic Mode address translation allows external users to access the controlled environment, but only via a single IP address. This IP address is associated with any packets sent from the controlled environment to the outside world, and as it does not correspond to any specific internal resource it provides nothing for an external server to “hack”.

Static Mode address translation provides a one-to-one mapping between the internal resources and external IP addresses, but the actual IP address is never exposed on the network.

9.7.4.2.3 Structure

Component	Platforms
Checkpoint Firewall Security Software (Gateway)	Firewall Management Server Firewall Module - 1
Enterprise Centre Firewall Management Software	Firewall Management Server

9.7.4.2.4 Firewall-1

The Firewall-1 product from Checkpoint Software Technologies Ltd provides remote user access control with strong authentication, including the optional use of SecurID tokens. It supports Network Address Translation (NAT), and is transparent to users. It maintains communication and application derived state and context information which is stored and updated dynamically.

Firewall-1 supports three network interfaces: two that it arbitrates between, and a *De-Militarised Zone* (DMZ), which is a secure network attached directly and only to the firewall. Using a DMZ means that all traffic to and from the systems on the secure network must go through the Firewall.

Firewall-1 is used within Horizon at those points where an application level Firewall is required.

9.7.4.2.5 Enterprise Centre

Firewall-1 supports an *Enterprise Centre* that supports firewall configuration via a Graphical User Interface. This runs on the Authentication Server.

Resilience is provided by the use of pairs of Firewalls, with one in each pair acting as the Primary and the other as the Backup. These share state information, so the Backup is able to take of the network monitoring activities should the Primary (or its network connections) fail.

[NWD] lists the addresses and application access types used in each Firewall.

9.8 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 8	User Interfaces	Describes the user interface standards used in Horizon.
Next	Chapter 10	Platforms	Describes the various platform types used to support the Horizon services.
FTMSE	TD/DES/107	File Transfer Managed Service at CSR+	Describes the interface presented by the FTMS
FW	TD/DES/038	Firewall Requirements	Covers the use of Firewalls, though much of its text is now subsumed into [NWD]. The only substantial text not covered in both is the description of Firewall technology from which the description above is derived.
KMPROXY	TSC/CRY/069	KM Proxy Detailed Design	Describes the Proxy service, running in the VPN Exception Servers, that handles lost or missing VPN Keys.
NWARCH	TD/ARC/002	Network Architecture	Contains an initial description of the network architecture (primarily the ISDN network); now somewhat out of date.
NWD	TD/ARC/059	Network Infrastructure High Level Design - NR2	Contains full details of the network design for CSR and CSR+
VPNHLD	RS/DES/046	VPN High Level Design	Describes the way in which the VPN service is provided at the Campuses and in the Outlets, and the ways in which the network traffic is balanced across the available servers.

Chapter 10 - Platforms

10.1 Scope

This Chapter describes the various classes of Platform, the software regime under which they run, and the principal applications that they support. Details of the actual hardware and software versions used are given in the [PD] series of documents.

Platforms include all hardware components: data storage devices, processors, network connections, terminals and printers. They also include the way that operating systems, including transaction processing software, manage this hardware and use it to support the components of the business solution that are mounted on the Platforms.

10.2 Platforms Reference Architecture

Platforms can be viewed at three different levels, a shown in the following diagram. A "capsule" is the minimum component of an application that must run within a single platform.

- Hardware
- Operating System
- Applications

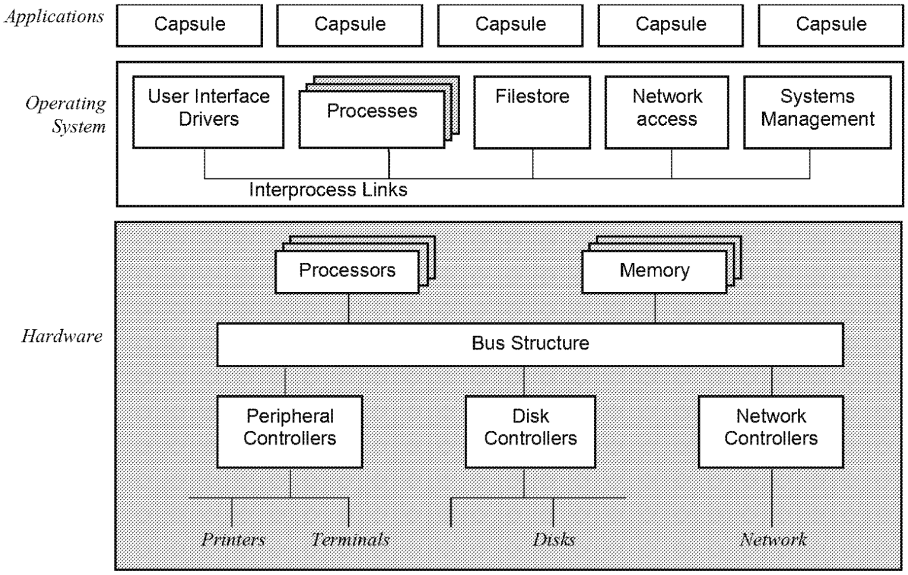

Figure 10.1 - Platforms Reference Model

10.3 STRATEGIC ISSUES

Chapter 4 “Overview” identifies a large number of physical platforms within the Horizon architecture. In the interests of simplicity, these use the minimum possible number of different hardware and operating system types.

Commodity (i.e. Intel-based) Platforms, running Microsoft NT, are used wherever this is feasible in terms of functionality, reliability and performance. Where this is not feasible, UNIX servers are used. Sequent servers are used for high-performance RDBMS servers, and cheaper SUN Solaris servers for other UNIX applications.

This diagram illustrates a hierarchy of Platform classes. The assumption is that each member “inherits” the properties of its class unless specifically stated otherwise.

The remainder of this Chapter follows the structure implicit in this diagram.

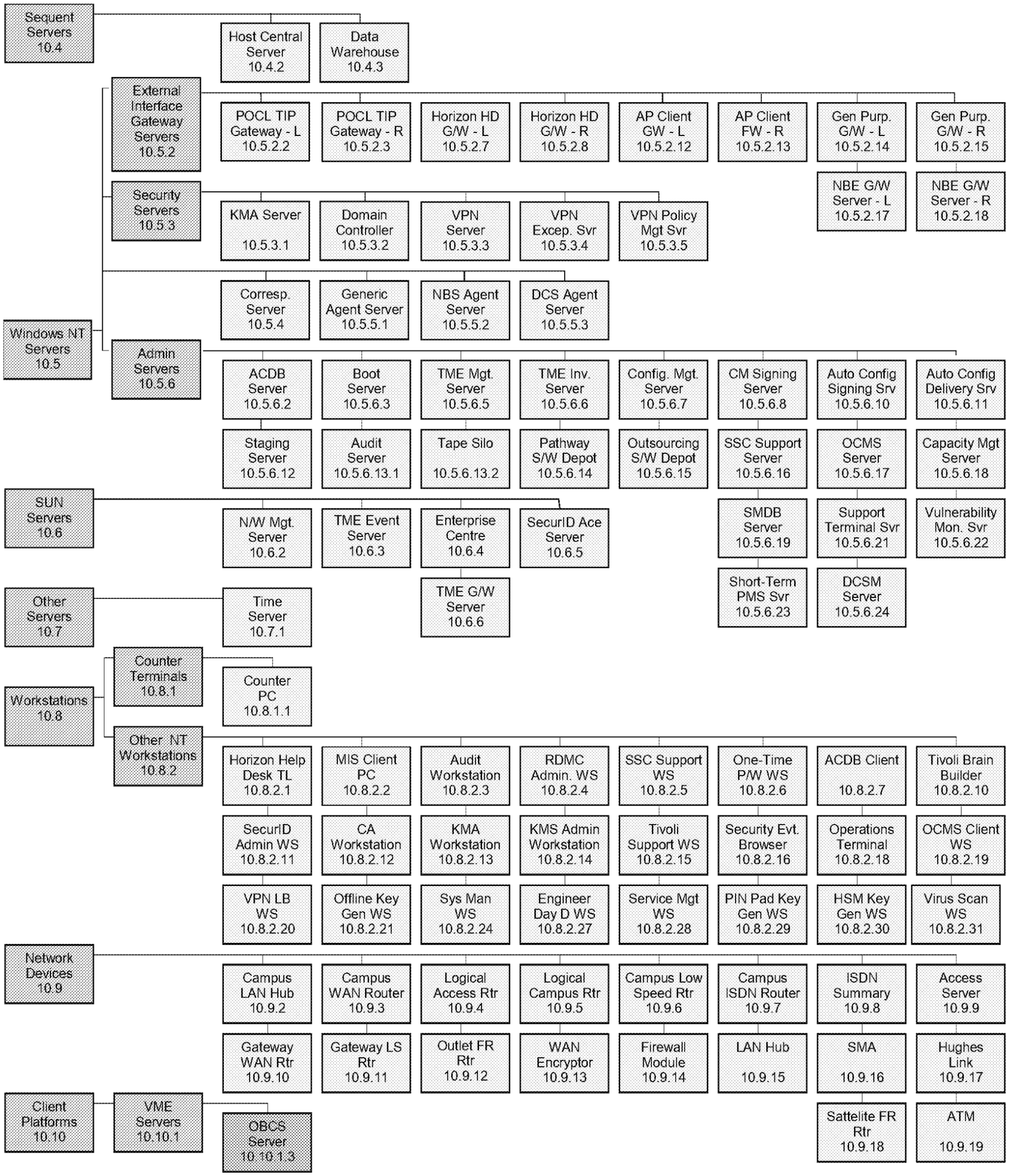
Sequent Servers 10.4
Host Central Server 10.4.2
Data Warehouse 10.4.3
External Interface Gateway Servers 10.5.2
POCL TIP Gateway - L 10.5.2.2
POCL TIP Gateway - R 10.5.2.3
Horizon HD G/W - L 10.5.2.7
Horizon HD G/W - R 10.5.2.8
AP Client GW - L 10.5.2.12
AP Client FW - R 10.5.2.13
Gen Purp. G/W - L 10.5.2.14
Gen Purp. G/W - R 10.5.2.15
NBE G/W Server - L 10.5.2.17
NBE G/W Server - R 10.5.2.18
Security Servers 10.5.3
KMA Server 10.5.3.1
Domain Controller 10.5.3.2
VPN Server 10.5.3.3
VPN Excep. Svr 10.5.3.4
VPN Policy Mgt Svr 10.5.3.5
Corresp. Server 10.5.4
Generic Agent Server 10.5.5.1
NBS Agent Server 10.5.5.2
DCS Agent Server 10.5.5.3
Windows NT Servers 10.5
Admin Servers 10.5.6
ACDB Server 10.5.6.2
Boot Server 10.5.6.3
TME Mgt. Server 10.5.6.5
TME Inv. Server 10.5.6.6
Config. Mgt. Server 10.5.6.7
CM Signing Server 10.5.6.8
Auto Config Signing Srv 10.5.6.10
Auto Config Delivery Srv 10.5.6.11
Staging Server 10.5.6.12
Audit Server 10.5.6.13.1
Tape Silo 10.5.6.13.2
Pathway S/W Depot 10.5.6.14
Outsourcing S/W Depot 10.5.6.15
SSC Support Server 10.5.6.16
OCMS Server 10.5.6.17
Capacity Mgt Server 10.5.6.18
SMDB Server 10.5.6.19
Support Terminal Svr 10.5.6.21
Vulnerability Mon. Svr 10.5.6.22
Short-Term PMS Svr 10.5.6.23
DCSM Server 10.5.6.24
SUN Servers 10.6
N/W Mgt. Server 10.6.2
TME Event Server 10.6.3
Enterprise Centre 10.6.4
SecurID Ace Server 10.6.5
TME G/W Server 10.6.6
Other Servers 10.7
Time Server 10.7.1
Workstations 10.8
Counter Terminals 10.8.1
Counter PC 10.8.1.1
Other NT Workstations 10.8.2
Horizon Help Desk TL 10.8.2.1
MIS Client PC 10.8.2.2
Audit Workstation 10.8.2.3
RDMC Admin. WS 10.8.2.4
SSC Support WS 10.8.2.5
One-Time P/W WS 10.8.2.6
ACDB Client 10.8.2.7
Tivoli Brain Builder 10.8.2.10
SecurID Admin WS 10.8.2.11
CA Workstation 10.8.2.12
KMA Workstation 10.8.2.13
KMS Admin Workstation 10.8.2.14
Tivoli Support WS 10.8.2.15
Security Evt. Browser 10.8.2.16
Operations Terminal 10.8.2.18
OCMS Client WS 10.8.2.19
VPN LB WS 10.8.2.20
Offline Key Gen WS 10.8.2.21
Sys Man WS 10.8.2.24
Engineer Day D WS 10.8.2.27
Service Mgt WS 10.8.2.28
PIN Pad Key Gen WS 10.8.2.29
HSM Key Gen WS 10.8.2.30
Virus Scan WS 10.8.2.31
Network Devices 10.9
Campus LAN Hub 10.9.2
Campus WAN Router 10.9.3
Logical Access Rtr 10.9.4
Logical Campus Rtr 10.9.5
Campus Low Speed Rtr 10.9.6
Campus ISDN Router 10.9.7
ISDN Summary 10.9.8
Access Server 10.9.9
Gateway WAN Rtr 10.9.10
Gateway LS Rtr 10.9.11
Outlet FR Rtr 10.9.12
WAN Encryptor 10.9.13
Firewall Module 10.9.14
LAN Hub 10.9.15
SMA 10.9.16
Hughes Link 10.9.17
Sattelite FR Rtr 10.9.18
ATM 10.9.19
Client Platforms 10.10
VME Servers 10.10.1
OBCS Server 10.10.1.3

Figure 10.2 - Platform Class Hierarchy

10.4 SEQUENT SERVERS

These are used for running high-performance Oracle database applications. There are two types of Sequent server:

- Host Central Servers, used to run the principal business applications where there is a need for the power and scalability of an Oracle database
- Data Warehouse Server, which acts as a repository for a large amount of financial and service-related information and which supports a number of applications principally used for Pathway's internal business purposes

Variants of these are used for testing purposes.

10.4.1 General

10.4.1.1 Sequent as an Oracle Platform

The Sequent Servers run a number of large Oracle Database applications. Relational Databases do not inherently provide fast response times. To meet the workload it is necessary to use a Platform in which Oracle have invested a considerable amount of tuning work, and which has the Oracle "seal of approval" based on competitive benchmarks.

Workload considerations are not the only ones that apply. For resilience reasons, as discussed in Chapter 13 "Availability", it is sensible to adopt a strategy whereby the active Host Central Server and Data Warehouse server can operate in conjunction with similar systems at a standby site, linked by a high-speed communications network that enables the data held on the "live" system to be immediately available at the standby site. EMC disks, which can be used with the Sequent servers, provide this facility.

10.4.1.2 Sequent Hardware Architectures

10.4.1.2.1 Symmetric Multi Processor Systems

In simple computer system, increased power is provided by faster *Central Processing Units* (CPUs), more memory and/or faster disks. When this is insufficient, a number of processors are linked so that they share memory and disks. This is known as *Symmetric Multi Processing* (SMP). In general, an SMP system offers a scaling factor of around 1.8: two linked processors can offer the same power as 1.8 similar but independent processors, three processors around the same power as 2.7 and so on. The scaling factor is reasonably linear up to the maximum number of processors supported by the architecture, which is usually imposed by the bandwidth of the system Bus.

10.4.1.2.2 Clustered Systems

To go beyond the power of an SMP system, *Clustered Systems* link a number of SMP systems (each called a Node) so that they can share filestore but not memory. Each node contains a single UNIX instance, with message passing between nodes to carry out any necessary co-ordination. High-speed switches enable each Node to access the the shared disks. Various techniques are used to share the workload between nodes. These need, for example, to partition an Oracle database so that each node only accesses its own part of it. Alternatively, they need to provide locking techniques so that each node can gain exclusive access to some part of the database for a brief period of time.

Clustering gives a significant improvement in system throughput, but not to the same degree as that provided by adding processors to an SMP system. It also provides improves system resilience, as each node provides a fallback for the others, and (at a certain cost) the system can include a standby node provided merely to be able to step in should any node fail. In general, this involves restarting any services that were running on the failed node. This shows the structure of a clustered system.

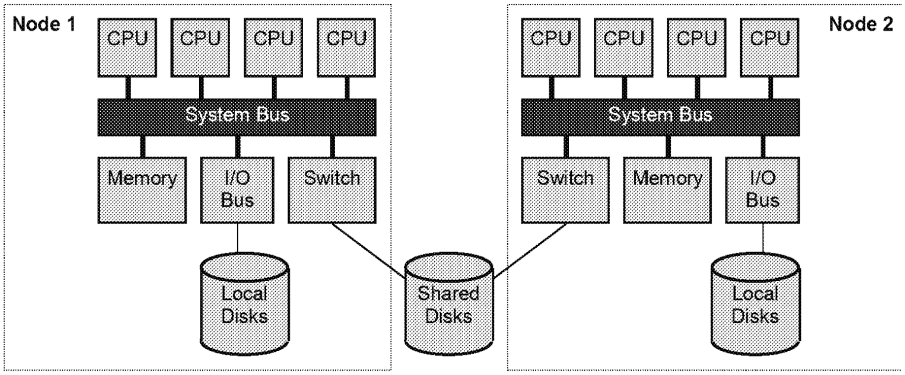

Figure 10.3 - Clustered System

10.4.1.2.3 Non-Uniform Memory Addressing (NUMA)

A further development is to share memory between processors in a way that removes the limits imposed by Clustering. This connects nodes by a mechanism that is slower than the main system bus. A processor can see all the memory attached to any of the other nodes. However, access times to any other than its own memory is considerably slower (*non-uniform*), though clever caching techniques can obviate some of the performance loss that this would otherwise cause.

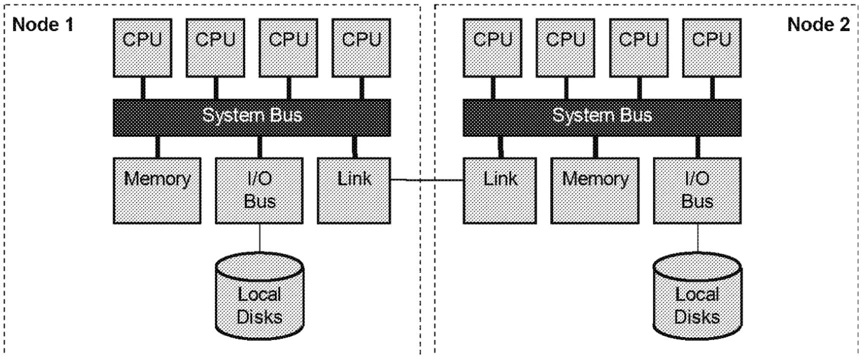

Figure 10.4 - NUMA Technology

This technology can provide a considerable reasonably linear performance boost, but depends on the applications that run on it being constrained to operate primarily within one node. The system presents a single UNIX system image, and sophisticated process scheduling is required to ensure that processes always return to the processor where they last run. For example, Oracle Parallel Server is being enhanced by Oracle to support NUMA architectures. This enhancement is being exploited by Sequent.

10.4.1.2.4 NUMA-Q

Sequent's interception of NUMA technology is called *NUMA-Q*. It uses up to four Pentium Pro or Xeon processors within a single card (known as a Quad), each sharing a common memory of up to 4 GB, and using standard SMP techniques. Each processor incorporates a high degree of internal caching. The resulting single board is known by Intel as their *Single High Volume Server* (SHVS).

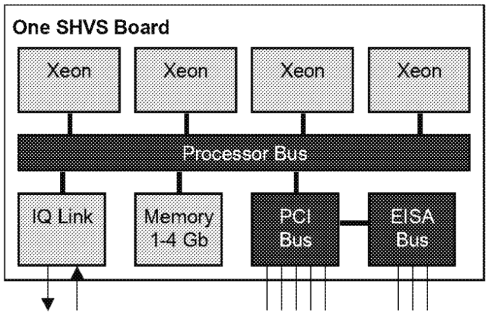

Figure 10.5 - Sequent's NUMA-Q Quad Architecture

In theory up to 63 Quads can be linked together, giving a total storage capacity of up to 100 Tb. The links are via the Sequent-provided IQ-Link cards, which provide a 1 Gbps bandwidth between nodes. These links support a coherent Cache that effectively provides a shared memory between all the Nodes, though with the access time limitations mentioned above.

Sequent's NUMA-Q nodes normally contain at least two QUAD boards. A NUMA-Q node is not a clustered system in the sense described above. It provides a single system image, and thus if one Quad breaks it is necessary to take down the entire system in order to repair it.

10.4.1.3 Fibre Channel Interconnection

NUMA-Q disks can be accessed via *Fibre Channel Interconnection*. This allows disks tobe shared between a number of NUMA-Q Quads, as shown here.

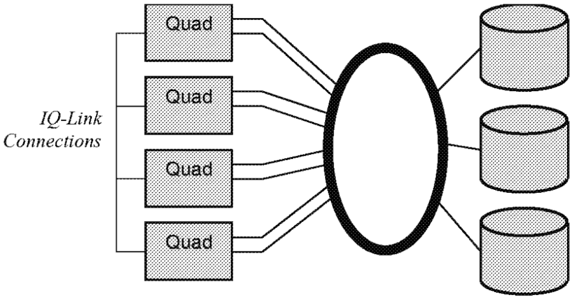

Figure 10.6 - NUMA-Q Use of Fibre Channel Interconnect

Dynix includes a version of UNIX Volume Manager that provides dynamic mapping from logical volumes to physical volumes depending on what routes are available. Primarily this is via the PCI interface from the Quad. Either PCI card may be used. I*n extremis,* a Quad can access its disks via the IQ-Link interface and another Quad.

It is possible to "cluster" NUMA-Q systems by linking them through the filestore as with a conventional clustered system.

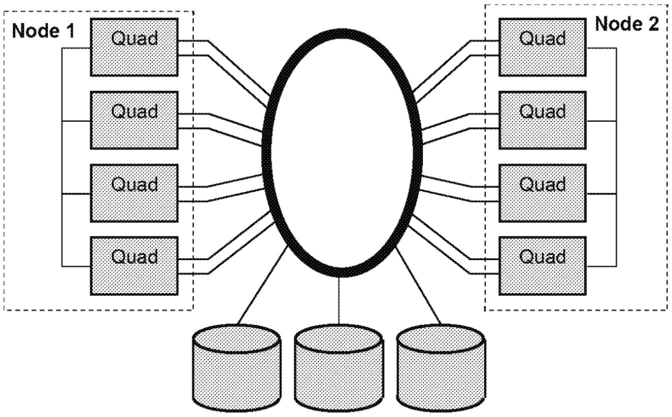

Figure 10.7 - Clustering NUMA-Q Nodes

This only supports clustering within a single site, as the Fibre links are limited at present to around 20 Km.

Two Nodes are used at each Campus, one running the Host central applications and the other the Data Warehouse and MIS applications. Routine failover for either node is to the other node.

Additional measures are taken to provide for site disaster recovery, as described below.

10.4.1.4 Host Storage Strategy

10.4.1.4.1 Disk Hardware

The disaster resilience strategy for the Host Central Servers, as described in Chapter 13 “Availability”, involves replicating data between the two sites. Thus, following a site failure, the servers at the other site can quickly take over the entire workload. A single EMC disk array is used in each Campus. As well as the Host Central Server databases, this array also holds data required by the following applications.

- Key Management Application (KMS)
- Outlet Change Management Service (OCMS)
- Auto-Configuration Database Service (ACDB)
- Debit Card Service (DCS)

Each array supports internal disk mirroring, with automated disk recovery from the mirror using a hot standby disk in the event of a single disk failure.

Further disk arrays are used for test purposes. These are earlier EMC 3230 arrays, connected via a SCSI-to-Fibre bridge.

10.4.1.4.2 EMC Disk Replication

This is covered in more detail in Chapter 13 "Availability". It uses EMC's SRDF technology to replicate data between the EMC disk array at each Campus. The replicated data is used mainly by the Host Central Servers.

10.4.1.5 Sequent Operating System Strategy

Sequent’s variant of UNIX is called *Dynix*. It is optimised to handle large relational database workloads on SMP and nodal system. However, IBM (who now own Sequent) are decommitting from future developments to Dynix, and Pathway is reconsidering the strategic direction for Host platforms. It is likely that these will move to a Solaris based architecture at some point in the future.

10.4.1.5.1 Dynix Structure

Component	Platforms
Alexandria Backup Librarian Software	Data Warehouse Server Host Central Server
Alexandria Backup Toolkit	Data Warehouse Server Host Central Server
Dynix/ptx CD-ROM Media	Data Warehouse Server
Dynix/ptx Operating System	Data Warehouse Server Host Central Server
Fibre Channel Bridge Software (FCBR)	Data Warehouse Server Host Central Server
Fibre Channel Host Adapter Software	Data Warehouse Server Host Central Server
NTP for Sequent (Network Time Protocol)	Data Warehouse Server Host Central Server
NUMA-Q Virtual Console System (VCS)	Data Warehouse Server Host Central Server
Patch Base	Data Warehouse Server Host Central Server
ptx/Basecomms	Data Warehouse Server Host Central Server
ptx/INSTALL	Data Warehouse Server Host Central Server
ptx/LAN	Data Warehouse Server Host Central Server
ptx/NFS	Data Warehouse Server Host Central Server
ptx/On-Line Diagnostic Software	Data Warehouse Server Host Central Server
ptx/PDC	Data Warehouse Server
ptx/SPDRIVERS	Data Warehouse Server Host Central Server
ptx/SVM	Data Warehouse Server Host Central Server
ptx/TCP/IP	Data Warehouse Server Host Central Server
ptx/Windows	Data Warehouse Server Host Central Server

10.4.1.5.2 Secure Sequent Build

A "secure Sequent build" is created and maintained by PIT, and is updated at each Release.

10.4.1.6 Campus Configurations

A two-Node NUMA-Q system is installed at each Campus. One Node runs the Host Central Server applications, and the other the Data Warehouse applications. Each node acts as a standby for the other. The other Campus acts as a disaster standby site, and provides the capability to act as a test site.

10.4.2 Host Central Server

Purpose These run the Host applications. At any one time, all applications run at one Campus; in the event of Host failure or loss of a Campus the entire workload is transferred to the other Campus.

Type Sequent NUMA-Q E301 or later

Property	*Value*
Connection type	100baseT
CPU Speed	400 MHz
CPU Type	NUMA-Q
Device	DLT 4000 4-drive 48-cartridge standalone library
Disk size	4.3 Gb
Disk type	Fibre connected EMC 3430 Symmetrix disk array of 300 Gb mirrored, with SRDF connection to the other Campus
Memory	4 Gb
Operating System	Dynix V4.4.8
Port Number	RDMC:62004
Port Number	APS:62003
Port Number	TPS:62002
Port Number	OBCS:62001
Scheduler	Maestro
VLAN	3,4 Host Systems LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	bvnb01
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Wigan Campus	1	<<<	bvnw01

Application	*Component*
Access Control and User Administration	COSMAN Access Control Manager
Automated Payments Service	APR Application
	APS Database
	APS Host Application
	Database Links
BMC Patrol Systems Management	BMC Patrol Agent
	BMC Patrol Console
	BMC Patrol Knowledge Module
	BMC Patrol Knowledge Module for APS
	BMC Patrol Knowledge Module for Dynix Base
	BMC Patrol Knowledge Module for Hytec FTF
	BMC Patrol Knowledge Module for Hytec Sonnet
	BMC Patrol Knowledge Module for LFS
	BMC Patrol Knowledge Module for Maestro
	BMC Patrol Knowledge Module for OBCS
	BMC Patrol Knowledge Module for Oracle
	BMC Patrol Knowledge Module for TPS
	BMC Patrol to Tivoli Event Filter
Build & Installation Processes	Host Backup and Recovery
	Host Failover Management
	Host Installation Routines
	Host Shell Configuration
	Host Shell Test Tools
	Secure Sequent Build
Dynix Operating System Software	Alexandria Backup Librarian Software
	Alexandria Backup Toolkit
	Dynix/ptx Operating System
	Fibre Channel Bridge Software (FCBR)
	Fibre Channel Host Adapter Software
	Fibre Channel Switch Software
	NTP for Sequent (Network Time Protocol)
	NUMA-Q Virtual Console System (VCS)
	Patch Base
	ptx/Basecomms
	ptx/EFS
	ptx/INSTALL
	ptx/LAN
	ptx/NFS
	ptx/On-Line Diagnostic Software
	ptx/SPDRIVERS
	ptx/SVM
	ptx/TCP/IP
	ptx/Windows
EMC Disk Array Driver Software	EMC Symmetrix Manager
	Remote Data Facility Software Licence
	Symmetrix Manager Base Component Software Licence
	Symmetrix Manager SRDF Facility Host S/W Licence
File Transfer Management Service	FTMS Core Application for Unix
Hytec Sonnet Support Software	BMC Patrol Knowledge Module for Hytec FTF
	Hytec Sonnet with ADI, FTF
Logistics Feeder Service	LFS Database
	LFS Host Application

Maestro Scheduler (TWS)	Maestro Master Console International
	Tivoli Maestro Host (Unix)
Management Information Service	Database Links
Network Banking Service	Data Reconciliation Service (DRS) Host Application
	Database Links
	DRS Database
Oracle Relational Database Software	Oracle - PL/SQL
	Oracle - Pro*C
	Oracle Developer 2000
	Oracle Parallel Query Option
	Oracle RDBMS for Sequent
	Oracle Server
	Oracle Server Manager
	Oracle SQL*Net for Sequent
	Oracle SQL*Plus
	Oracle TCP/IP Adapter for Sequent
	Oracle Tools
	Oracle Xa Libraries
Order Book Control Service	Database Links
	OBCS Database
	OBCS Host Application
Performance Measurement System	Metron Athene Acquire - Dynix Performance Management
Proxima LogManagerKM	LogManage KM
Reference Data Management Service	RDDS Database
	RDDS Host Application
	RDMC Database
	RDMC Host Application
	RDMC POCL Reference Data
Systems Management Environment	MANSEQ
Transaction Management System	Host Agent Control
Transaction Processing Service	Database Links
	TPS Database
	TPS Host Application

10.4.3 Data Warehouse Server

Purpose Holds information used to support Pathway management processes, including those necessary to assess conformance to the SLAs. Input to the Data Warehouse comes from the Host Central Server. This is retained for up to four months before being

Type Sequent NUMA-Q E300

Property	*Value*
Connection type	100baseT
CPU Speed	400 MHz
CPU Type	NUMA-Q
CPUs	4
Device	DLT 4000 4-drive 48-cartridge standalone library
Memory	1 Gb
Operating System	Dynix V4.4.8
Port Number	63001
Ports	48
Scheduler	Maestro
VLAN	3,4 Host Systems LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	dwhb01
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Wigan Campus	1	<<<	dwhw01

Application	*Component*
Access Control and User Administration	COSMAN Access Control Manager
BMC Patrol Systems Management	BMC Patrol Agent
	BMC Patrol Console
	BMC Patrol Knowledge Module
	BMC Patrol Knowledge Module for Dynix Base
	BMC Patrol Knowledge Module for Maestro
	BMC Patrol Knowledge Module for Oracle
	BMC Patrol to Tivoli Event Filter
Build & Installation Processes	Datawarehouse Server Installation Routines
	Secure Sequent Build

Dynix Operating System Software	Alexandria Backup Librarian Software Alexandria Backup Toolkit Dynix/ptx CD-ROM Media Dynix/ptx Operating System Fibre Channel Bridge Software (FCBR) Fibre Channel Host Adapter Software Fibre Channel Switch Software NTP for Sequent (Network Time Protocol) NUMA-Q Virtual Console System (VCS) Patch Base ptx/Basecomms ptx/EFS ptx/INSTALL ptx/LAN ptx/NFS ptx/On-Line Diagnostic Software ptx/PDC ptx/SPDRIVERS ptx/SVM ptx/TCP/IP ptx/Windows
EMC Disk Array Driver Software	Symmetrix SymmManager Symmetrix TimeFinder
Maestro Schedule Maestro Scheduler (TWS)	Maestro Schedule - Data Warehouse Maestro Master Console International Tivoli Maestro Host (Unix)
Management Information Service	MIS Application MIS Datawarehouse Archiving MIS Datawarehouse Backup & Recovery MIS Datawarehouse Build MIS Datawarehouse Processing
archived.	MIS Datawarehouse Reference Data MIS Datawarehouse Restore MIS Datawarehouse Scheduling MIS Datawarehouse Setaside Tablespaces MIS Datawarehouse Tablespaces MIS Datawarehouse TPS
Oracle Relational Database Software	Oracle - PL/SQL Oracle - Pro*C Oracle Advanced Replication Option Oracle Parallel Query Option Oracle RDBMS for Sequent Oracle Server Oracle Server Manager Oracle SQL*Net for Sequent Oracle SQL*Plus Oracle TCP/IP Adapter for Sequent Oracle Xa Libraries
Performance Measurement System	Metron Athene Acquire - Dynix Performance Management
Systems Management Environment	MANSEQ
Transaction Management System	Agent Control Product (DW)

10.5 WINDOWS NT SERVERS

10.5.1 General

"Commodity" Intel-based Compaq servers are used for the majority of server requirements. From S30, all new NT Server requirements will be met by Fujitsu Siemens servers.

10.5.1.1 Hardware Architecture

From S30, Campus servers are taken from the Fujitsu Siemens server range appropriate at the time of purchase.

10.5.1.2 Disks

Most NT servers use internal disk drives. However, it is possible to link these servers to external disk arrays, and in particular to the EMC disks used to support the Sequent-based Host Central Servers. SRDF facilities are used to synchronise this array with a similar array in the other Campus. Where there is a need to synchronise two Windows NT servers' filestores across the inter-Campus link, they can use part of the EMC disk array, connected via special SCSI controllers. This is subject to detailed sizing of the EMC arrays.

10.5.1.3 NT Operating System

Microsoft's Windows NT is the commodity operating system of choice for Intel-based servers. It is Pathway's chosen server operating system for Intel systems. The current strategy is to use Windows NT Version 4.0 with (from BI2) Service Pack 6a and a range of security hot fixes.

Windows 2000 and Windows XP are now available. Windows NT is no longer available from Microsoft and will cease to be supported in the foreseeable future. At BI3, some specialised new platforms are implemented on Windows 200 (W2K). It is likely that, at an appropriate point, all Campus servers will be moved to W2K (or Windows XP).

Systems are configured with a Regional setting of UK.

10.5.1.3.1 Structure

Component	Platforms
Microsoft FTP	DCS Management Server Network Banking FTMS Remote Gateway SSC Support Workstation
Microsoft NT 4.0 Resource Kit	KMA Server KMS Admin Workstation
Microsoft NT 4.0 Server Tools	KMS Admin Workstation
Microsoft NT Server	ACDB Server Agent Server AP Client Gateway - Local AP Client Gateway - Remote Audit Server Auto Configuration Delivery Server Auto Configuration Signing Server Boot Server CA Workstation Capacity Management Server CM Signing Server Configuration Management Server Correspondence Server Domain Controller - Local Domain Controller - Remote Engineer's Day D Laptop General Purpose FTMS Gateway - Local
Microsoft NT Server	General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote KMA Server KMS Admin Workstation OCMS Server Outsourcing Software Depot POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote SMDB Server SSC Support Server Staging Server TME Inventory Server TME Management Server - 1

	VPN Exception Server VPN Policy File Management Server VPN Server
Microsoft NT Workstation	ACDB Client Workstation Atalla Card Loader Workstation Audit Workstation CA Workstation Counter PC Horizon Help Desk Terminal KMA Workstation MIS Client Workstation MIS Support Workstation OCMS Client Offline Key Generation Workstation One Time Password Workstation PIN Pad Key Generation Workstation PIN Pad Proving Workstation RDMC Administrator Workstation SecurID Admin Workstation Short-term Performance Database Server SSC Support Workstation Systems Management Access Workstation Tivoli Support Workstation VPN Loopback Workstation Vulnerability Monitoring Workstation
Microsoft Windows Scripting Host	Audit Server DCS Management Server SMDB Server SSC Support Server
NotePad (part of NT)	SSC Support Workstation
Performance Monitor (from NT Resource Kit)	SSC Support Workstation
POSIX Subsystem	SSC Support Workstation
Remote Console NT Resource Kit	Correspondence Server
Robocopy	Audit Server OCMS Server SMDB Server SSC Support Server
Time Service (Windows NT Resource Kit)	ACDB Client Workstation ACDB Server Agent Server
Time Service (Windows NT Resource Kit)	AP Client Gateway - Local AP Client Gateway - Remote Audit Server Audit Workstation Boot Server Capacity Management Server CM Signing Server Correspondence Server DCS Agent Server DCS Management Server Domain Controller - Local Domain Controller - Remote General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote KMA Server KMA Workstation KMS Admin Workstation MIS Client Workstation MIS Support Workstation NBS Agent Server Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway OCMS Client OCMS Server Outsourcing Software Depot POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote RDMC Administrator Workstation SecurID Admin Workstation Short-term Performance Database Server SSC Support Server SSC Support Workstation

	VPN Exception Server VPN Loopback Workstation VPN Policy File Management Server VPN Server
Windows NT Service Pack 6a - High Encryption + Hot	ACDB Client Workstation ACDB Server Agent Server AP Client Gateway - Local AP Client Gateway - Remote Atalla Card Loader Workstation Audit Server Audit Workstation Auto Configuration Delivery Server Auto Configuration Signing Server Boot Server CA Workstation Capacity Management Server CM Signing Server Correspondence Server Counter PC DCS Agent Server DCS Management Server Domain Controller - Local Domain Controller - Remote Engineer's Day D Laptop General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote Horizon Help Desk Terminal KMA Server KMA Workstation KMS Admin Workstation MIS Client Workstation MIS Support Workstation NBS Agent Server Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway OCMS Client OCMS Server Offline Key Generation Workstation One Time Password Workstation Outsourcing Software Depot PIN Pad Key Generation Workstation PIN Pad Proving Workstation POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote RDMC Administrator Workstation SecurID Admin Workstation Short-term Performance Database Server SMDB Server SSC Support Server SSC Support Workstation Staging Server Systems Management Access Workstation Tivoli Support Workstation TME Inventory Server TME Management Server - 1 VPN Exception Server VPN Loopback Workstation VPN Policy File Management Server VPN Server Vulnerability Monitoring Workstation

10.5.1.3.2 NT Secure Build

A “secure build” is used to provide common security features across all NT platforms,and is updated at each Release.

10.5.1.4 Internet Explorer

This is Microsoft's general-purpose Web Browser. It is used on Counter PCs to display receipts and other forms prior to printing. It is used on varions Campus servers and workstations, either because it is the only available way to view Help data, or because the workstation has access to web-based data such as the Tivoli Inventory Server.

Component	Platforms
Microsoft Internet Explorer (Minimum Install)	ACDB Client Workstation ACDB Server AP Client Gateway - Remote Audit Server Audit Workstation Correspondence Server Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation KMS Admin Workstation OCMS Client OCMS Server RDMC Administrator Workstation SecurID Admin Workstation Short-term Performance Database Server SMDB Server SSC Support Server SSC Support Workstation Systems Management Access Workstation

10.5.1.5 Microsoft FTP

This is delivered as part of NT and is used on certain servers for file transfer purposes.

10.5.2 External Interface Gateway Servers

A range of Gateway servers is used for communication with external bodies. These support the FTMS, which transfers Flat Files to and from external Clients. Some of these servers carry out software encryption of the transferred files, as directed by their configuration files.

10.5.2.1 Standards

There are two variants of most Gateway Servers: one in the Campus and one for the remote site. There are minor differences in the configurations of these. For example, a Server installed in the Campus has two LAN cards and is connected to both Campus LANs. Servers installed on remote sites have only one LAN card that is connected to an Pathway supplied Cisco Router.

10.5.2.2 POCL TIP Gateway Server - Local

Purpose Half of a pair of servers used to transfer data between Pathway and POCL. One server is located at each Campus. They communicate with a remote gateway server at Huthwaite, or an identical backup system at Isleworth.

Type Compaq ProLiant 5000 6/200 Model 2

Property	*Value*
CPU Type	Pentium Pro
CPUs	2
Device	Diskette 3.5" 1.44 Mb

Disk size	14 x 4.3 Gb
Memory	128 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Resilience	Compaq Resilience Option
Scheduler	Maestro
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	PBORMT015
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Wigan Campus	1	<<<	PWIRMT050
Wigan Campus	1	<<<	PWIRMT050-SEC

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build POCL TIP Local Gateway Server Installation Routines
Crypto Code	CAPU Check Handler Core Signing Functions (CSF) Crypto Keystore Service (CKS) File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - CAPUs (Initial) via Build or Tivoli Crypto Keys - CRL via Automatic Channel Crypto Keys - CRL via Manual Crypto Keys - PWY TIPPR (Black) via PMKM Crypto Keys - PWY TIPPR (Red) via PMKM Crypto Keys - PWY TIPPU PKC via Build
Debit Card System File Transfer Management Service Hummingbird Communications Software Logistics Feeder Service	FTMS DCS to TIP MID/TID Local Connection Configuration FTMS Core Application Hummingbird NFS Maestro Solo FTMS LFS to SAPADS Local Connection Configuration FTMS SAPADS to LFS Local Connection Configuration
Maestro Schedule Maestro Scheduler (TWS) Microsoft Windows NT	Maestro Schedule Tivoli Maestro Agent for NT Platforms Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Reference Data Management Service	Network Associates AV Suite - Server FTMS RDB to RDMC Local Connection Configuration FTMS RDB to RDT Local Connection Configuration FTMS RDMC to RDB Local Connection Configuration FTMS RDT to RDB Local Connection Configuration
Sapher Layer7 SecurID Access Control Software Systems Management Environment	Layer7 SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
Transaction Processing Service	FTMS TIP to TPS Local Connection Configuration FTMS TPS to TIP Local Connection Configuration
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.3 POCL TIP Gateway Server - Remote

Purpose Used on POCL site to transfer data from the POCL Reference Data and to receive data from the Pathway TPS system.

Type Compaq ProLiant 5000 Model 6/200

Property	*Value*
CPU Speed	200 MHz
CPU Type	Pentium Pro
CPUs	2
Device	Diskette 3.5" 1.44 Mb
Disk size	14 x 4.3 Gb
Disk size	9 Gb

Memory	128 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Resilience	Compaq Resilience Option

Site	*Qty*	*Installed*	*Platform Name*
POCL Huthwaite	1	<<<	BHUPTG124-SEC
POCL Huthwaite	1	<<<	PHUPTG124
Test - B&TC2 Volumes & Integration Rig	1	<<<	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build POCL TIP Remote Gateway Server Installation Routines
Crypto Code	Core Signing Functions (CSF) File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - CAPUs (Initial) via Build or Tivoli Crypto Keys - POCL TIPPR (Black) via PMKM Crypto Keys - POCL TIPPR (Red) via PMKM Crypto Keys - POCL TIPPU PKC via Build
Debit Card System File Transfer Management Service Logistics Feeder Service	FTMS DCS to TIP MID/TID Remote Connection Configuration FTMS Core Application FTMS LFS to SAPADS Remote Connection Configuration FTMS SAPADS to LFS Remote Connection Configuration
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Performance Measurement System Reference Data Management Service	Network Associates AV Suite - Server Metron Athene Acquire - NT Performance Management Agent FTMS RDB to RDMC Remote Connection Configuration FTMS RDB to RDT Remote Connection Configuration FTMS RDMC to RDB Remote Connection Configuration FTMS RDT to RDB Remote Connection Configuration
Sapher Layer7 SecurID Access Control Software Systems Management Environment	Layer7 SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
Transaction Processing Service	FTMS TIP to TPS Remote Connection Configuration FTMS TPS to TIP Remote Connection Configuration
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.4 POCL APS Gateway Server – Local

This platform was removed at S11R

10.5.2.5 POCL APS Gateway Server – Remote

This platform was removed at S11R

10.5.2.6 POCL APS Backup Gateway – Remote

This platform was removed at S11R

10.5.2.7 Horizon Help Desk Gateway – Local

Purpose Installed at Campuses. Handles transfer of help desk statistics to Data Warehouse.

Type Compaq DeskPro 4000 Model 5166

Property	*Value*
Device	Diskette 3.5" 1.44 Mb
Memory	64 Mb

Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOHDG134
Wigan Campus	1	<<<	MWIHDG084

Application	*Component*
Adaptec Drivers Build & Installation Processes	Adaptec SCSI Driver for 7800 family Generic NT Platform Install Routines Horizon HelpDesk Local Gateway Server Installation Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
File Transfer Management Service Horizon Help Desk	FTMS Core Application FTMS BT to MIS Local Connection Configuration FTMS MITEL to MIS Local Connection Configuration FTMS SORBUS to MIS Local Connection Configuration
Hummingbird Communications Software Maestro Schedule Maestro Scheduler (TWS) Microsoft Windows NT	Hummingbird NFS Maestro Solo Maestro Schedule Tivoli Maestro Agent for NT Platforms Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Performance Measurement System SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Server Metron Athene Acquire - NT Performance Management Agent SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.8 Horizon Help Desk Gateway – Remote

Purpose This is a Pathway managed server, located at the Horizon Helpdesk in STE09. It is used to reliably transfer statistical information between the HSHD and the Data Warehouse.It uses the standard Pathway FTMS software.

Type Compaq DeskPro 4000 Model 6200

Property	*Value*
Device	Diskette 3.5" 1.44 Mb
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
ISD SMC Stevenage 09	1	<<<	MSTHDG135

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines Horizon HelpDesk Remote Gateway Server Installation NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Eicon Driver Software File Transfer Management Service Horizon Help Desk	Eicon ISDN DIVA Basic Rate Card FTMS Core Application FTMS BT to MIS Remote Connection Configuration FTMS MITEL to MIS Remote Connection Configuration FTMS SORBUS to MIS Remote Connection Configuration
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Performance Measurement System SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Server Metron Athene Acquire - NT Performance Management Agent SecurID Agent for NT MANEVENT

	MANEVENT Filter Server
	MANNTEP
	MANSENTRY FTMS
	MANSENTRYCFG FTMS
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.9 Automated Payments Client Gateway - Local

Purpose Used to transfer files between Pathway and AP client sites. Each is provided with 2 LAN adapters for connection to the 2 Campus LANs. The FTMS service provides file transfer between the "AP Client Gateway – Local" PC and the "AP Client Gateway – Remote" P

Type Compaq DeskPro EP Desktop

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOLAP01
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWILAP01

Application	*Component*
Automated Payments Service	FTMS AP Client Local Connection Configuration
Build & Installation Processes	AP Client Gateway Local Installation Routines
	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Verifying Functions (CVF)
	Crypto Keystore Service (CKS)
	File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - FTPPR (Black) via Diskette
	Crypto Keys - FTPPR (Red) via Build
File Transfer Management Service	FTMS Core Application
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Windows NT	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANSENTRY FTMS
	MANSENTRYCFG FTMS
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.10 Automated Payments Client Gateway - Remote

Purpose Installed on an AP Client site. Handles file transfer to and from Campuses. Hardware and driver upgrades indicated mark points where the specification changes for new installations; no existing machines were actually upgraded.

Type Compaq DeskPro EP Desktop

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
ACP, London	2	<<<	MLORAP01..02
AON, Caterham	2	<<<	MCARAP01..02
British Gas Trading, Staines	2	<<<	MSNRAP01..02
CCM (BBC), Huthwayte	2	S06R	MHURAP01..02
DPC (BT) AP Client Site, Bletchley	2	S06R	MBLRAP01..02
DPC (BT), Derby	2	<<<	MDERAP01..02
DVLA, Swansea	2	<<<	MSWRAP01..02
DVLNI, Coleraine	2	<<<	MCORAP01..02
ESP, Hull	2	<<<	MHLRAP01..02
First Rate, Hounslow	2	S11R	MHORAP01..02
Girobank, Bootle	2	<<<	MBORAP01..02
Girobank, Leicester	2	<<<	MLERAP01..02
Hampshire County Cncl & Southampton City	2	<<<	MWHRAP01..02
Knowsley Borough Council, Knowsley	2	<<<	MKNRAP01..02
Mid Kent Water, Snodland	2	<<<	MSDRAP01..02
National Savings, Blackpool	2	<<<	MBPRAP01..02
Northern Ireland Electricity, Sheffield	2	<<<	MSHRAP01..02
Oxford Social Services, Oxford	2	<<<	MOXRAP01..02
Quantrill, Canary Wharf	2	<<<	MCWRAP01..02
Quantum, Newcastle	2	<<<	MNERAP01..02
Royal Sun Alliance, Birmingham	2	<<<	MBMRAP01..02
Scottish & Southern Energy, Havant	2	<<<	MHVRAP01..02
Standard Life Insurance, Edinburgh	2	<<<	MEDRAP01..02
SWALEC and Welsh Water, Bridgend	2	<<<	MBDRAP01..02
TALEXUS, Felixstowe	2	<<<	MFXRAP01..02
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	
TV Licensing, Preston	2	<<<	MPRRAP01..02
Yorkshire Electricity, Leeds	2	<<<	MLDRAP01..02

Application	*Component*
Automated Payments Service	FTMS AP Client Remote Connection Configuration
Build & Installation Processes	AP Client Gateway Remote Installation Routines Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Crypto Code	Core Signing Functions (CSF) Crypto Keystore Service (CKS) File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - AP Client Remote Crypto Keys - FTPPU via Build
Eicon Driver Software	Eicon Client ISDN Driver
File Transfer Management Service	FTMS Core Application
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.11 General Purpose FTMS Gateway – Local

Purpose Installed at the Campuses. Handles File transfers to internal ICL sites such as Stevenage and Manchester.

Type Compaq DeskPro EP Desktop

Property	*Value*
CPU Type	NUMA-Q
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOFLG01
Wigan Campus	1	<<<	MWIFLG01

Application	*Component*
Build & Installation Processes	General Purpose FTMS Gateway Local Installation Routines Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
File Transfer Management Service	FTMS Core Application FTMS General Purpose Local Configurations
Hummingbird Communications Software Maestro Schedule Maestro Scheduler (TWS) Microsoft Windows NT	Hummingbird NFS Maestro Solo Maestro Schedule Tivoli Maestro Agent for NT Platforms Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Order Book Control Service Outlet Change Management Service Performance Measurement System Reference Data Management Service SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Server FTMS OBCS to UKSS Local Connection Configuration FTMS OCMS to UKSS Local Connection Configuration Metron Athene Acquire - NT Performance Management Agent FTMS RDMC to UKSS Local Connection Configuration SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.12 General Purpose FTMS Gateway – Remote

Purpose Installed at internal ICL sites to handle file transfers from the Campuses that are driven by FTMS. Communicates with the Campuses via ISDN

Type Compaq DeskPro EP Desktop

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Fujitsu Services Stevenage STE04/10/14	1	<<<	MSTFRG01
ISD SMC MAN 05, Manchester	1	<<<	MMAFRG01
ISD SMC Stevenage 09	1	<<<	MSEFRG01

Application	*Component*
Build & Installation Processes	General Purpose FTMS Gateway Remote Installation Routines Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Eicon Driver Software	Eicon Client ISDN Driver Eicon DIVA Client for Windows NT4.0 Eicon ISDN DIVA Basic Rate Card
File Transfer Management Service	FTMS Core Application FTMS General Purpose Local Configurations FTMS General Purpose Remote Configurations
Maestro Scheduler (TWS) Microsoft Windows NT	Tivoli Maestro Agent for NT Platforms Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes

Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Order Book Control Service	FTMS OBCS to UKSS Remote Connection Configuration
Outlet Change Management Service	FTMS OCMS to UKSS Remote Connection Configuration
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Reference Data Management Service	FTMS RDMC to UKSS Remote Connection Configuration
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.2.13 POCL Standby Gateway – Remote

Purpose Located at Huthwaite. Provides the file transfer part of the facility for full restoration of service between the Pathway Campuses and POCL, in the event of failure of the main interface at Huthwaite.

Type Proliant 1850R PIII, 500, 64Mb Model 1

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
PON Comdisco, Isleworth	1	<<<	PIWPTG01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Secure Build
Crypto Code	Core Signing Functions (CSF) Crypto Keystore Service (CKS) File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - POCL TIP Remote Gateway Crypto Keys - POCL TIPPR (Black) via PMKM Crypto Keys - POCL TIPPR (Red) via PMKM
File Transfer Management Service	FTMS Core Application
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Reference Data Management Service	FTMS RDB to RDMC Remote Connection Configuration FTMS RDMC to RDB Remote Connection Configuration
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT MANNTEP MANSENTRY FTMS MANSENTRYCFG FTMS MANTOOLS
Transaction Processing Service	FTMS TIP to TPS Remote Connection Configuration FTMS TPS to TIP Remote Connection Configuration

10.5.2.14 Network Banking FTMS Local Gateway

Purpose Located at Campuses. Handles file transfers to and from the NBE

Type Compaq Server

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	BI3	
Wigan Campus	2	BI3	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	Maestro Unattend
	NBE FTMS Gateway Local Installation Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Verifying Functions (CVF)
	Crypto API for Network Banking
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - FTPPR (Black) via Diskette
	Crypto Keys - FTPPR (Red) via Build
File Transfer Management Service	FTMS Core Application
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Key Management Service	Key Store Service
	KM Client Agent
	KM Common Functions
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Windows NT	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Network Banking Service	FTMS NWB Local Configurations
	NBS Bulk File Processes
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANSENTRY FTMS
	MANSENTRYCFG FTMS
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Client
	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server

10.5.2.15 Network Banking FTMS Remote Gateway

Purpose Installed at NBE site and standby site. Handled file transfers to and from the NBE

Type Compaq Server

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty Installed*	*Platform Name*
IBM Warwick	2	BI3
IBM, Greenford	1	BI3

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	Maestro Unattend
	NBE Gateway Server Remote Installation Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Signing Functions (CSF)
	Crypto Keystore Service (CKS)
	File Sign/Verify Library (glued)
File Transfer Management Service	FTMS Core Application
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Windows NT	Microsoft FTP
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server

Network Banking Service	FTMS NWB Remote Configuration
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANSENTRY FTMS
	MANSENTRYCFG FTMS
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.3 Security Servers

10.5.3.1 KMA Server

Purpose Generates all required crypto Key Values, and stores and distributes Key information.

Type Compaq ProLiant 5500 6/400 Model 2

Property	*Value*
Connection type	100baseT
CPU Speed	400 MHz
CPU Type	Pentium III
CPUs	2
Device	ComScire Random Number Generator
Device	Diskette 3.5" 1.44 Mb
Disk size	6 Gb
Disk size	2 x 9 Gb on EMC 3430
Memory	256 Mb
NT Service	Dial-in
NT Service	KMA
NT Service	Maestro
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	24,25 KMA LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOKMS01
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIKMS01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	KMA Server Installation Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	CAPU Check Handler
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	Entropy Generation Application (EGA)
	PMMC Common Library
	TeamWARE Crypto (TWC)
Crypto Keys	Crypto Keys - (KIPR)KMAK
	Crypto keys - (KMA Key)TK via SQL
	Crypto Keys - CAPU Checks via Automatic Channel
	Crypto Keys - CRL via zip drive
	Crypto Keys - DLLKA/B from L&G via Diskette
	Crypto Keys - NVPN set via diskette
	Crypto Keys - TK via Manual
	Crypto Keys - VPN CRL via PMKM
EMC Disk Array Driver Software	EMC Symmetrix manager Control Utilities
Key Management Service	Key Generator (DSA)
	Key Generator (L&G)
	Key Generator (Red Pike)

	Key Management Application (KMA)
	Key Store Service
	KM Client Agent
	KM Common Functions
	KM Interactive Channel Service
	KMA Agents Common
	KMA Common Functions
	KMA Database
	KMA Server Application
Legato Application and Driver Software	Legato Networker ClientPak for Windows NT
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft SQL Server	ActiveX Data Objects (ADO)
	Microsoft SQL Server
Microsoft Visual Studio	Microsoft Visual Studio Runtime
Microsoft Windows NT	Microsoft NT 4.0 Resource Kit
	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
QNG Device Drivers	QNG Device Driver
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANSENTRY KMA
	MANSENTRYCFG KMA
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TeamWARE Crypto	TeamWARE Crypto (TWC)
Transaction Management System	NT Agent Control
TRIAGE Audit Software	Triage Monitoring Client

10.5.3.2 Domain Controller

10.5.3.2.1 Domain Controller - Local

Purpose Handles Windows NT authentication. Connected to both Campus LANs. There are hardware variants of this.

Type Compaq DeskPro 6000 Model 6200

Property	*Value*
CPU Speed	300
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BBOBOPSS02
Bootle Campus	1	<<<	BBOBVPN02
Bootle Campus	1	<<<	BBOPWYKMS01
Bootle Campus	1	<<<	BBOPWYKMS02
Bootle Campus	1	<<<	PBOBOPSS01
Bootle Campus	1	<<<	PBOBVPN01
Bootle Campus	1	<<<	PBOPWYFTMS01
Bootle Campus	1	<<<	PBOPWYSMC01
Bootle Campus	1	<<<	PBOWSLAM01
Bootle Campus	1	BI2C	PBOPWYDCS01
Bootle Campus	1	BI3	PBOPWYPUB01
Bootle Campus	1	S30	BBODCSSERV01
Release 2 Test Rig	1	<<<	
Release 2 Test Rig	1	<<<	
Test - APDU (2 rigs)	2	S30	
Test - B&TC Application Target	2	S30	
Test - B&TC Application Target	2	S30	
Test - B&TC1 Integration	2	S30	
Test - B&TC2 Volumes & Integration Rig	6	<<<	
Test - B&TC2 Volumes & Integration Rig	4	S30	
Test - B&TC5 Testing Support	2	S30	
Test - B&TC7 PET/UTC	1	BI3	

Test - B&TC7 PET/UTC	2	S30	
Test - IPDU System Test (INF1)	3	BI3	
Test - IPDU System Test (INF1)	2	S30	
Test - LST Main Rig	2	BI3	
Test - LST Main Rig	2	S30	
Test - LST2 Second Rig	1	S30	
Test - PTU	7	BI3	
Test - REL1 Release Rig	2	<<<	
Test - REL1 Release Rig	2	S30	
Wigan Campus	1	<<<	BWIPWYDCS02
Wigan Campus	1	<<<	BWIPWYFTMS01
Wigan Campus	1	<<<	BWIPWYKMS01
Wigan Campus	1	<<<	BWIPWYSMC01
Wigan Campus	1	<<<	BWIWOPSS01
Wigan Campus	1	<<<	BWIWSLAM01
Wigan Campus	1	<<<	BWIWVPN02
Wigan Campus	1	<<<	PWIPWYKMS01
Wigan Campus	1	<<<	PWIWOPSS01
Wigan Campus	1	<<<	PWIWVPN01
Wigan Campus	1	BI3	BWIPWYPUB01
Wigan Campus	1	S30	BWIDCSSERV01

Application	*Component*
Build & Installation Processes	Domain Controller Installation Routines Generic Common File Installation Routines Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.3.2.2 Domain Controller - Remote

Purpose Handles Windows NT authentication on remote sites.

Type Compaq DeskPro 6000 Model 6300

Property	*Value*
CPU Speed	300
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	1	<<<	BBRBRASUP02
CS Bracknell	1	<<<	BBRCORPWY01
CS Bracknell	1	<<<	BBRFELUSRS01
CS Bracknell	1	<<<	BBRPWYDCS01
CS Bracknell	1	<<<	PBRBRASUP01
CS Bracknell - Secure Area	1	<<<	BBRPWYHQ01
ISD Belfast Bridgeview	1	<<<	BBEPWYDCS03
ISD Belfast Trident House	1	<<<	BBEPWYDCS02
ISD SMC MAN 05, Manchester	1	<<<	BSTPWYSMC01
ISD SMC Stevenage 09	1	<<<	BSTHDHORIZON02
ISD SMC Stevenage 09	1	<<<	PSTHDHORIZON01
ISD, Lytham St Annes	1	<<<	BLYPWYSMC01
Pathway at Feltham	1	<<<	BFEPWYDCS01
Pathway at Feltham	1	<<<	PFECORPPWY01
Pathway at Feltham	1	<<<	PFEFELUSRS01
Pathway at Feltham	1	<<<	PFEPWYHQ01

Application	*Component*
Build & Installation Processes	Domain Controller Installation Routines Generic Common File Installation Routines

	Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
SecurID Access Control Software Systems Management Environment	SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.3.3 VPN Server

Purpose Handles VPN traffic to and from Outlets and encrypts/decrypts it as appropriate

Type Compaq DeskPro EP Desktop -> DL360 at BI2

Property	*Value*
CPU Speed	200 MHz
Disk size	1.2 Gb
Memory	64 Mb
NT Service	VPN Management Service
NT Service	EWYC Watcher
NT Service	VPN Remote Management Service (RMS)
NT Service	Policy Management Client (PMC)
NT Service	Tivoli
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	18,19 VPN Crypt LAN
VLAN	16,17 VPN Clear LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	12	<<<	MBOVPN01..12
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	8	<<<	
Test - B&TC2 Volumes & Integration Rig	8	BI2C	
Test - IPDU System Test (INF1)	1	BI2C	
Test - LST Main Rig	2	BI2C	
Test - PIT	1	BI2C	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	12	<<<	MWIVPN01..12

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build VPN Server Installation Routines
Crypto Keys	Crypto Keys - (NVPN)PIN via Automatic Channel Crypto Keys - (NVPN)PIN via PMKM Crypto Keys - VPN CRL via Automatic Channel Crypto Keys - VPN CRL via PMKM Crypto Keys - VPN PIN via Manual
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System SecurID Access Control Software Systems Management Environment	Metron Athene Acquire - NT Performance Management Agent SecurID Agent for NT EACRR-Client MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY VPN Server MANSENTRYCFG VPN Server MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software Utimaco Safeguard VPN Software	Triage Monitoring Client Utimaco SG VPN

	VPN Red Pike Driver
Virtual Private Network	VPN EWYC Watcher Application VPN PMC Pin Reader Application VPN Policy Management Client Application VPN Remote Management Client Application VPN Remote Management Service Application VPN Server Configuration

10.5.3.4 VPN Exception Server

Purpose Handles VPN connections from newly installed Counters, or those where the Post Office Manager has lost the PMMC or PIN

Type Compaq EP DeskPro 6600

Property	*Value*
CPU Speed	200 MHz
Disk size	1.2 Gb
Memory	64 Mb
NT Service	Policy Management Client (PMC)
NT Service	KMProxy
NT Service	Tivoli
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	18,19 VPN Crypt LAN
VLAN	16,17 VPN Clear LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOVEX01
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIVEX01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build VPN Exception Server Configuration VPN Exception Server Installation Routines
Crypto Keys	Crypto Keys - VPN CRL via Automatic Channel Crypto Keys - VPN CRL via PMKM Crypto Keys - VPN Server
Key Management Service Microsoft SQL Server Microsoft Visual Studio Microsoft Windows NT	KM Proxy Server Microsoft SQL Server Client Microsoft Visual C++ Runtime DLLs Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System SecurID Access Control Software Systems Management Environment	Metron Athene Acquire - NT Performance Management Agent SecurID Agent for NT MANEVENT MANEVENT Filter Server MANNTEP MANSENTRY VPNEX MANSENTRYCFG VPNEX MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software Utimaco Safeguard VPN Software	Triage Monitoring Client Utimaco SG VPN VPN Red Pike Driver
Virtual Private Network	VPN PMC Pin Reader Application VPN Policy Management Client Application VPN Remote Management Client Application VPN Remote Management Service Application

10.5.3.5 VPN Policy File Management Server

Purpose Central co-ordination VPN Policy File changes during migration, rollout and steady state changes.

Type Compaq DeskPro EP 6600 Desktop

Property	*Value*
NT Service	PMS
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	18,19 VPN Crypt LAN
VLAN	16,17 VPN Clear LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOVPM01
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIVPM01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Microsoft Visual Studio	Microsoft Visual C++ Runtime DLLs
Microsoft Windows NT	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANSENTRY VPNPM
	MANSENTRYCFG VPNPM
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client
Utimaco Safeguard VPN Software	Utimaco SG VPN
Virtual Private Network	VPN Config Application
	VPN PMC Pin Reader Application
	VPN Policy Management Server Application
	VPN Policy Management Server Configuration

10.5.4 Correspondence Server

Purpose Forms the main interface between the Agent Applications and the Counter. The Riposte Messaging System holds all information required by the applications' Counter components. Servers are organised in Clusters of four.

Type Compaq ProLiant DL360

Property	*Value*
CPU Speed	550 MHz
CPU Type	Pentium III
CPUs	4
Disk size	9 x 18 Gb in EMC 3430 Cabinet
Memory	512 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Riposte ID	999981 n/a
Riposte ID	999982 n/a
Riposte ID	999980 n/a
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	4	<<<	MBOCOR01..04
Bootle Campus	4	BI2C	MBOCOR11..14
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	8	<<<	
Test - B&TC2 Volumes & Integration Rig	4	<<<	
Test - LST Main Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	
Test - REL1 Release Rig	2	<<<	

Wigan Campus	4	<<<	MWICOR01..4
Wigan Campus	4	BI2C	MWICOR11..14

Application	*Component*
Adaptec Drivers	Adaptec 2944UW Firmware BIOS Upgrade
	Adaptec SCSI Driver for 7800 family
Audit Facilities	Audit Agent
Build & Installation Processes	Correspondence Server Installation Routines
	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Windows NT	Microsoft NT Server
	Remote Console NT Resource Kit
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Outlet Monitoring Service	TMS Outlet Monitor Agents
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Riposte Utilities	Riposte Utilities from Escher
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	EACRR-Client
	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
Transaction Management System	Agent Management Utilities
	Agent Performance Monitor Libraries
	Cluster Lookup Service (LUC)
	Correspondence Agents Common
	TMS Distrib
	TMS Library
	TMS Outlet Monitor Agents
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server

10.5.5 Agent Server

Purpose Provides the interface between the Host system and the Correspondence Servers. Agent applications act as clients to both, by 'pulling' information from one and 'pushing' it to the other. Every server can run any combination of agent processes.

Type Compaq ProLiant 1850R PIII 600

Property	*Value*
Device	Diskette 3.5" 1.44 Mb
Memory	64 Mb
NT Service	TMSOMDBHBHarvester <n>
NT Service	TMSNBConf <h> <n>
NT Service	KMRx
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Page File	256 Mb
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	4	<<<	MBOAGE01..04
Release 2 Test Rig	2	<<<	
Test - B&TC2 Volumes & Integration Rig	8	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	4	<<<	MWIAGE01..04

Application	*Component*
Automated Payments Service	APS Agents
Build & Installation Processes	Agent Server Installation Routines
	Generic NT Platform Install Routines

	Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Crypto Code	CAPU Check Handler Core Signing Functions (CSF) Crypto Keystore Service (CKS) Cryptographic Functions API PMMC Common Library
Crypto Keys	Crypto Keys - APPU PKC via automatic channel Crypto Keys - CAPU Set via Tivoli Crypto Keys - CRL via Automatic Channel Crypto Keys - SA KEK via Diskette Crypto Keys - SAPR via Build Crypto Keys - SAPU PKC via Build
Debit Card System Key Management Service	DCS Confirmation Agents Key Store Service KM Client Agent KM Common Functions KMC Automatic Channel - Server-side KMS Agents
Logistics Feeder Service Maestro Schedule Maestro Scheduler (TWS) Management Information Service Microsoft SQL Server Microsoft Windows NT	LFS Agent Maestro Schedule Tivoli Maestro Agent for NT Platforms Data Warehouse Agents Microsoft SQL Server Client Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Banking Service Oracle Relational Database Software	NBS Confirmation Agents Oracle for Windows NT4 Networking Products Oracle Net for Windows NT (previously SQL*Net)
Order Book Control Service Outlet Monitoring Service Performance Measurement System Reference Data Management Service Riposte Desktop Riposte Utilities Sapher Layer7 SecurID Access Control Software Systems Management Environment	OBCS Agents TMS Outlet Monitor Agents Metron Athene Acquire - NT Performance Management Agent Reference Data Agents WebRiposte Common - Software Unsigned by Escher Riposte Utilities from Escher Layer7 SecurID Agent for NT EACRR-Client MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management Tivoli Agent/Host Recovery
Transaction Management System	Agent Performance Monitor Libraries Cluster Lookup Service (LUC) Counter Monitoring Agent General Agents Multiple Riposte Library TMS Library TMS Outlet Monitor Agents User Lock Request Library
Transaction Processing Service TRIAGE Audit Software WebRiposte	TPS Agent Triage Monitoring Client WebRiposte Client WebRiposte Data Centre - Software Unsigned by Escher WebRiposte Message Server

10.5.5.1 NBS Agent Server

Purpose Runs the NBS Authorisation Agent and NBS Expedited Confirmation Agent

Type Compaq ML350

Property	*Value*
CPU Speed	1.5 GHz
CPU Type	Pentium 4
CPUs	2

Device	Internal crypto co-processor
Footprint	5U
Memory	256 Mb
NT Service	TMSNBXConf <h> <n>
NT Service	TMSNBAuth <h> <s> <n>
NT Service	KMRx
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Ports	4
VLAN	NBS Internal LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	4	BI3	MBONBA01..04
Release 2 Test Rig	1	BI3	
Test - B&TC7 PET/UTC	3	BI3	
Test - IPDU System Test (INF1)	3	BI3	
Test - LST Main Rig	1	BI3	
Test - PTU	7	BI3	
Wigan Campus	4	BI3	MWINBA01..04

Application	*Component*
Build & Installation Processes	Agent Server Installation Routines
	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Signing Functions (CSF)
	Crypto API for Network Banking
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
Crypto Keys	Crypto Keys - (NBTDO)TK via Automatic Channel
	Crypto Keys - APPU PKC via automatic channel
	Crypto Keys - CAPU Set via Tivoli
	Crypto Keys - CRL via Automatic Channel
	Crypto Keys - SA KEK via Diskette
	Crypto Keys - SAPR via Build
	Crypto Keys - SAPU PKC via Build
	Crypto Keys - TK via Manual
Key Management Service	Key Store Service
	KM Client Agent
	KM Common Functions
	KM Dist Receiver Mon Dispatcher
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft SQL Server	Microsoft SQL Server Client
Microsoft Windows NT	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Banking Service	NBS Authorisation Agents
Oracle Relational Database Software	Oracle for Windows NT4 Networking Products
	Oracle Net for Windows NT (previously SQL*Net)
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	EACRR-Client
	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
	Tivoli Agent/Host Recovery
Transaction Management System	Agent Performance Monitor Libraries
	Cluster Lookup Service (LUC)
	General Agents
	Multiple Riposte Library
	User Lock Request Library
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Client
	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server

10.5.5.2 DCS Agent Server

Purpose Handles the DCS Agents

Type Fujitsu Siemens Primergy F200

Property	*Value*
Device	Internal crypto co-processor
Disk Partition	T: - EMC Mirror Partition
Disk Partition	S: - EMC Primary Partition
Disk Partition	M: - MID/TID Data Files
Disk Partition	D: - Pathway Applications
Disk Partition	C: - System Disk
Filestore	Encrypted
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty Installed*	*Platform Name*
Bootle Campus	4	S30
Test - B&TC2 Volumes & Integration Rig	2	S30
Wigan Campus	4	S30

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Signing Functions (CSF)
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	TeamWARE Crypto (TWC)
Crypto Keys	Crypto Keys - (NBTDO)TK via Automatic Channel
	Crypto Keys - APPU PKC via automatic channel
	Crypto Keys - CAPU Set via Tivoli
	Crypto Keys - CRL via Automatic Channel
	Crypto Keys - SA KEK via Diskette
	Crypto Keys - SAPU PKC via Build
	Crypto Keys - TK via Manual
Debit Card System	DCS Authorisation Agents
EMC Disk Array Driver Software	EMC Symmetrix manager Control Utilities
Key Management Service	Key Store Service
	KM Client Agent
	KM Common Functions
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft SQL Server	Microsoft SQL Server Client
Microsoft Visual Studio	Microsoft VB Runtime DLLs
Microsoft Windows NT	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Oracle Relational Database Software	Oracle for Windows NT4 Networking Products
	Oracle Net for Windows NT (previously SQL*Net)
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Retail Logic Solve/SE and Solve/PFG	Solve/SE Client for Windows NT
	Solve/SE de option for NT
	Solve/SE dt option for NT
	Solve/SE Host Application
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	EACRR-Client
	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
	Tivoli Agent/Host Recovery
TeamWARE Crypto	TeamWARE Crypto (TWC)
Transaction Management System	Agent Performance Monitor Libraries
	Cluster Lookup Service (LUC)
	General Agents
	Multiple Riposte Library
	User Lock Request Library
TRIAGE Audit Software	Triage Monitoring Client

WebRiposte	WebRiposte Client WebRiposte Data Centre - Software Unsigned by Escher WebRiposte Message Server

10.5.6 Administration Servers

A number of servers are provided to assist in the management and administration of the system.

10.5.6.1 ACDB Server

Purpose Supports auto-configuration of newly installed Counter PCs. Backup machine configuration may differ from that listed.

Type Compaq ProLiant 2500r 6/200

Property	*Value*
CPU Speed	200 MHz
CPU Type	Pentium Pro
Disk size	7 x 4.3 Gb
Memory	256 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOACF01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIACF01

Application	*Component*
Auto-configuration	ACDB Server Application ACDB Server Executables ACF with In-line SIPU Auto Configuration Database SQL Mirroring
Build & Installation Processes	Autoconfig DB Server Installation Routines Generic NT Platform Install Routines Maestro Unattend NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft SQL Server	Microsoft SQL Server
Microsoft Visual Studio	Microsoft VB Runtime DLLs
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.2 Boot Server

Purpose Connected to by newly installed Counter PCs and supplies the data needed to enable them to re-connect to the Auto Configuration Servers. Connects to Isolated Boot

Type Compaq DeskPro 4000 Model 5200

Property	*Value*
Connection type	ISDN BRI
Connection type	Frame Relay
Connection type	100baseT
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	PBOBOO01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	PWIBOO01

Application	*Component*
Auto-configuration	Boot Server Application
	Boot Server Service for NDIS Driver
	DayD Boot Server Application
	Eicon Diehl Boot Service for NDIS Driver
	FAD Boot Search Application
Build & Installation Processes	Boot Server Installation Routines
	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Crypto Keystore Service (CKS)
Crypto Keys	Crypto Keys - IPOK Set via Diskette
Eicon Driver Software	Eicon C23 PSTN Modem
	Eicon Client ISDN Driver
	Eicon Diehl S2M ISDN Driver
	Eicon S2M Diva Server PRI PCI 0M
Microsoft Windows NT	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.3 TME Management Server

Purpose Master TMR

Type Compaq DL580

Property	*Value*
Footprint	4U
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	Tivoli Management LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BMASTER002 (MBOTVM01)
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	WSYSMASTER002

Application	*Component*
Microsoft Windows NT	Microsoft NT Server
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Systems Management Environment	Brain Builder
	MANEVENT
	MANNTEP
	MANTRC - Tivoli Remote Console Management
Tivoli Management Environment	TMR

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

10.5.6.4 TME Inventory Server

Purpose Contains inventory information needed for Software Distribution, plus the Operational Management Database which is used for support purposes and accessed via

Type Compaq ProLiant 5000R Model 6/200 with 1 Gb RAM

Property	*Value*
CPU Speed	200 MHz
CPU Type	Pentium Pro
Device	4 x 16 Gb TurboDAT Drive
Disk size	6 x 4.3 Gb
Footprint	7U
Memory	1 Gb
NT Service	Config_Watcher
NT Service	ACDB Watcher
Operating System	Microsoft NT Server with Service Pack 3
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BSYSINV01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	WSYSINV01

Application	*Component*
Microsoft Windows NT	Microsoft NT Server Windows NT Service Pack 6a - High Encryption + Hot Fixes
Oracle Relational Database Software	Oracle Server for Windows NT Oracle Web Server
Systems Management Environment	ACDB Feeder Auto-Targeting Aiming Device (ATAD) Auto-Targeting Engine (ATE) Brain Builder MANEVENT MANNTEP Operational Management Database (OMDB)

10.5.6.5 Configuration Management Server

Purpose Secure Change Management server based at Feltham and running PVCS. Software goes from here to the CM Signing Server for distribution.

Type Compaq DeskPro 4000 Model 5200

Property	*Value*
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	<<<	BBRCOM01
Pathway at Feltham	1	<<<	PFECOM01

Application	*Component*
Build & Installation Processes	NT Common File Set
Microsoft Windows NT	Microsoft NT Server
Software Signing	PVCS Server

10.5.6.6 CM Signing Server

Purpose Signs software for distribution via Tivoli. It is the only connection between the Feltham LAN and the Campus network at Wigan where the Tivoli master system is

Type Compaq DeskPro 4000 Model 5200

Property	*Value*
Device	Diskette 3.5" 1.44 Mb
Memory	64 Mb

Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	1	<<<	BBRCMS01
Pathway Feltham Secure Area	1	<<<	PFECMS01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Build & Installation Processes	CKS install CM Signing Server CM Signing Server Installation Routines Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Crypto Code	Core Signing Functions (CSF) Crypto Keystore Service (CKS)
Crypto Keys	Crypto Keys - (SIPR)TK via Automatic Channel Crypto Keys - SICERT via Build Crypto Keys - SIPR (Black) via Build Crypto Keys - SIPR (Red) via PMKM Crypto Keys - SIPU PKC via Build
Microsoft Windows NT	Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Software Signing	Signing Service
Systems Management Environment	MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.7 Auto Configuration Signing Server

Purpose Software to be installed in new Counter PCs is fed to this from the ACDB Server. It is digitally signed and passed to a staging area owned by ICL ISD. They have the same specification as the CM Signing Servers but use different shares.

Type Compaq DeskPro 4000 Model 6/200

Property	*Value*
Device	Diskette 3.5" 1.44 Mb
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOACS01
Wigan Campus	1	<<<	MWIACS01

Application	*Component*
Auto-configuration	ACF
Build & Installation Processes	CKS install CM Signing Server CM Signing Server Installation Routines NT Common File Set NT Secure Build
Crypto Code	Core Signing Functions (CSF) Crypto Keystore Service (CKS)
Crypto Keys	Crypto Keys - (SIPR)TK via Automatic Channel Crypto Keys - SICERT via Build Crypto Keys - SIPR (Black) via Build Crypto Keys - SIPR (Red) via PMKM Crypto Keys - SIPU PKC via Build
Microsoft Windows NT	Microsoft NT Server Windows NT Service Pack 6a - High Encryption + Hot Fixes
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Software Signing	Signing Service
Systems Management Environment	MANEVENT

	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.8 Auto Configuration Delivery Server

Purpose Stages software deliveries to new Counter PCs. These connect to a share on this server.The server is operated by ISD on Pathway's behalf. Although Pathway supplies the hardware, the software and the running of the service is the responsibility of ISD.

Type Compaq ProLiant 1600R 6/300

Property	*Value*
Footprint	4U
Level 2 Cache	256 Kb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	Tivoli Management LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BSYSDEL01 (MBOTVM08)
Wigan Campus	1	<<<	WSYSDEL01 (MWITVM08)

Application	*Component*
Build & Installation Processes	NT Common File Set
Microsoft Windows NT	Microsoft NT Server
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Systems Management Environment	ACDB Watcher
	Brain Builder
	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
Tivoli Management Environment	TMR
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.9 Staging Server

Purpose Holds boot data needed by newly installed Outlet PCs, and provides backup for software in the event of a fatal problem. Without such a source, ISD will not be able to rebuild the servers in time to fulfil SLAs.

Type Compaq ProLiant 1600 6/450

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOSTG01
Wigan Campus	1	<<<	MWISTG01

Application	*Component*
Build & Installation Processes	NT Common File Set
Crypto Code	Cryptographic Functions API
Microsoft Windows NT	Microsoft NT Server
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Systems Management Environment	MANEVENT Filter Server
	MANTOOLS
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.10 Audit Server

10.5.6.10.1 Audit Server Platform

Purpose Handles archiving and restore of audit and other archive data

Type Compaq ProLiant 7000 6/200

Property	*Value*
CPU Speed	200 MHz
CPUs	2
Device	DLT tape decks with auto-feed hopper
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOARC01
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - IPDU System Test (INF1)	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIARC01

Application	*Component*
Audit Facilities	Audit Checksum Database
	Audit Data Retrieval Agent
	Audit Server Application
	FTMS ASB to ASW Local Connection Configuration
	FTMS ASB to ASW Remote Connection Configuration
	FTMS ASW to ASB Local Connection Configuration
	FTMS ASW to ASB Remote Connection Configuration
Build & Installation Processes	Audit Server Configuration File
	Audit Server Installation Routines
	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Core Signing Functions (CSF)
	Crypto Keystore Service (CKS)
	File Encrypt/Decrypt Library (glued)
Crypto Keys	Crypto Keys - Audit Server
EMC Disk Array Driver Software	EMC Disk Storage Management System for NT
File Transfer Management Service	FTMS Core Application
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Legato Application and Driver Software	DLT7000 Drivers for Windows Intel Platforms
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Office	Microsoft Access
Microsoft Open Database Connectivity	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft SQL Server	ActiveX Data Objects (ADO)
	Microsoft NT Runtime for DAO
	Microsoft Open Database Connectivity (ODBC) Driver
	Microsoft SQL Server
Microsoft Visual Studio	Microsoft VB Runtime DLLs
Microsoft Windows NT	Microsoft NT Server
	Microsoft Windows Scripting Host
	Robocopy
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Oracle Relational Database Software	Oracle Server for Windows NT
	Oracle Table Re-Load Utility
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Riposte Message Server	Riposte Message Server Import
Riposte Utilities	Riposte Integrity Checker
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server

	MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management Riposte Archiving Agent
Transaction Management System	Audit Data Retrieval Agent Cluster Lookup Service (LUC)
TRIAGE Audit Software WebRiposte	Triage Monitoring Client WebRiposte Data Centre - Software Unsigned by Escher WebRiposte Message Server
WinZip	WinZip

10.5.6.10.2 Audit Data Repository

From BI3, the Audit Server is provided with a Tape Silo that optimises the management of DLTs and speeds up the audit retrieval process.

All audit information is copied to the Audit Server and is written to bulk storage media from there. Where this imposes unacceptable network traffic, it is feasible to write audit data directly to the Tape Silo from other Platforms. The platforms involved are:

- Key Management Server
- Host Central Server

10.5.6.11 Pathway Software Depot

Purpose Holds software from PCMS prior to its installation in the Bracknell Test Rigs

Type tbs

Property	***Value***
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	***Qty Installed***	***Platform Name***
SSC, Bracknell	3	<<<

Application	***Component***
Build & Installation Processes Crypto Code	NT Common File Set Core Signing Functions (CSF) Core Verifying Functions (CVF) Cryptographic Functions API
Crypto Keys	Crypto Keys - CAPUs (Initial) via Build or Tivoli Crypto Keys - CRL via Automatic Channel Crypto Keys - SIPU PKC via Automatic Channel
Key Management Service	Key Store Service KM Client Agent
Sapher Layer7 Software Signing Systems Management Environment	Layer7 SI Verifying Functions (SVF) MANEVENT MANEVENT Filter Server MANNTEP MANTOOLS
WebRiposte	WebRiposte Client WebRiposte Message Server

10.5.6.12 Outsourcing Software Depot

Purpose Conceptual name for the ISD platforms that hold software from PVCS until it is released for installation on the live estate.

Type Compaq ProLiant 1600 Model 266

Property	***Value***
NT Service Operating System Riposte ID VLAN	KMRx Microsoft NT Server 4.0 with Service Pack 6a 999982 n/a 1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	NT Common File Set
	OSD Depot Installation Routines
Crypto Code	Core Signing Functions (CSF)
	Core Verifying Functions (CVF)
	Cryptographic Functions API
	File Sign/Verify Library (glued)
Crypto Keys	Crypto Keys - CAPUs (Initial) via Build or Tivoli
	Crypto Keys - CRL via Automatic Channel
	Crypto Keys - SIPU PKC via Automatic Channel
Key Management Service	KM Client Agent
	KM Common Functions
	KM Dist Receiver Mon Dispatcher
Microsoft Visual Studio	Microsoft Visual C++ Runtime DLLs
Microsoft Windows NT	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Sapher Layer7	Layer7
Software Signing	SI Verifying Functions (SVF)
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Client
	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server

10.5.6.13 SSC Support Server

Purpose Provides the SSC with client access to archived files and message stores. The servers are accessed from SSC Workstations on a private LAN in BRA0. In normal operations one server is active and the other acts as a reserve.

Type Compaq ProLiant 1850R PIII 500 M1

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Scheduler	Maestro
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOSSC01
Wigan Campus	1	<<<	MWISSC01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
	SSC Support Server Installation Routines
Crypto Code	File Encrypt/Decrypt Library (glued)
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Maestro Schedule	Maestro Schedule
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Windows NT	Microsoft NT Server
	Microsoft Windows Scripting Host
	Robocopy
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server

Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Riposte Utilities	Riposte Integrity Checker
	Riposte Utilities from Escher
SecurID Access Control Software	SecurID Agent for NT
System Support Centre	SSC Support Applications
	WinGrep Search Utility
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server
WinZip	WinZip

10.5.6.14 OCMS Server

Purpose Supports steady state outlet changes.

Type Compaq 1850R PIII 500 M1

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Share Name	D:\transfer\ocms\ukss\in, \received, \out, \sent
Share Name	D:\transfer\ocms\tivoli\out
Share Name	D:\transfer\ocms\acdb\out
VLAN	OCMS LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	MBOOCM01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIOCM01

Application	*Component*
Auto-configuration	SQL Mirroring
Build & Installation Processes	Common File Set
	Generic NT Platform Install Routines
	Maestro Unattend
	NT Platform Fast Track Fixes
	NT Secure Build
	OCMS Server Installation Routines
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Open Database Connectivity	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft SQL Server	ActiveX Data Objects (ADO)
	Microsoft NT Runtime for DAO
	Microsoft Open Database Connectivity (ODBC) Driver
	Microsoft SQL Server
Microsoft Visual Studio	Microsoft VB Runtime DLLs
Microsoft Windows NT	Microsoft NT Server
	Robocopy
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Outlet Change Management Service	OCMS Database
	OCMS Server Application
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.15 Capacity Management Server

Purpose Used for collection and storage of performance management information

Type Siemens Fujitsu Scenix 600 Mini Tower PC

Property	*Value*
Device	DAT TapeDrive
Device	CD-Writer
Disk size	108 Gb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Pathway at Feltham	1	<<<	PBRPERMAN01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	NT Common File Set
	NT Secure Build
File Transfer Management Service	FTMS Core Application
Microsoft Windows NT	Microsoft NT Server
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System	FTMS PMS Local Connection Configuration
	Performance Management Database (PMDB)
	Performance Management Package "Athene"
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS

10.5.6.16 SMDB Server

Purpose Outside the DMZ; holds Service Management data used by support staff

Type Compaq Rack ProLiant ML530 R01

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
ISD SMC Stevenage 09	1	S06	BSEPWYCSM01
ISD SMC Stevenage 09	1	S06	PSEPWYCSM01
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines
	NT Secure Build
EMC Disk Array Driver Software	Symmetrix TimeFinder
Legato Application and Driver Software	DLT7000 Drivers for Windows Intel Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft SQL Server	Microsoft NT Runtime for DAO
Microsoft Windows NT	Microsoft NT Server
	Microsoft Windows Scripting Host
	Robocopy
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Oracle Relational Database Software	Oracle Installer Patch
	Oracle Server for Windows NT
Outlet Monitoring Service	Service Management Database (SMDB)
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
	SMDB Host Application
TRIAGE Audit Software	Triage Monitoring Client

10.5.6.17 Support Terminal Server

Purpose Support SSC staff using terminal server type access to Counter PCs

Type PRIMERGY F250 BU RH XEON 1,8GHz 512kB

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	S30	
Test - B&TC2 Volumes & Integration Rig	1	S30	
Wigan Campus	2	S30	

Application	*Component*
Build & Installation Processes	NT Common File Set
Crypto Code	TeamWARE Crypto (TWC)
Systems Management Environment	MANEVENT Filter Server MANTOOLS
TeamWARE Crypto	TeamWARE Crypto (TWC)

10.5.6.18 Vulnerability Monitoring Workstation

Purpose Runs the WebTrends vulnerability analysis software

Type Fujitsu Workstation

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Pathway Feltham Secure Area	2	BI2C	
Pathway Feltham Secure Area	2	S30	
Test - B&TC2 Volumes & Integration Rig	1	S30	
Test - IPDU System Test (INF1)	1	BI3	
Test - IPDU System Test (INF1)	1	S30	
Test - LST Main Rig	1	BI3	
Test - LST Main Rig	1	S30	
Test - PTU	1	BI3	

Application	*Component*
Build & Installation Processes	NT Common File Set
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Systems Management Environment	MANEVENT Filter Server MANTOOLS

10.5.6.19 Short-Term PMS Database Server

Purpose This is the access point for the Performance Management Service (PMS), and stores performance data collected from the platforms being monitored.

Type Compaq ProLiant ML370R01

Property	*Value*
Device	DAT TapeDrive
Device	CD-Writer
Disk size	36 Gb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	1	S06	BBRPERFMAN01
CS Bracknell	1	S06	PBRPERFMAN01

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Secure Build
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)

Microsoft SQL Server	SQL+
Microsoft Windows NT	Microsoft NT Workstation
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Performance Measurement System	Performance Management Package "Athene"
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TextPad	TextPad
TRIAGE Audit Software	Triage Monitoring Client
Virtual Private Network	VPNConfig
WinZip	WinZip

10.5.6.20 DCS Management Server

Purpose Generates Payment Files and sends them to the MA. Receives EMIS files and sends them to the DRS.

Type Fujitsu Siemens Primergy F200

Property	***Value***
Device	Internal crypto co-processor
Disk Partition	T: - EMC Mirror Partition
Disk Partition	S: - EMC Primary Partition
Disk Partition	M: - MID/TID Data Files
Disk Partition	D: - Pathway Applications
Disk Partition	C: - System Disk
Filestore	Encrypted
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	1	S30	
Test - B&TC2 Volumes & Integration Rig	2	S30	
Wigan Campus	1	S30	

Application	***Component***
Build & Installation Processes	Generic NT Platform Install Routines
	Maestro Unattend
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	TeamWARE Crypto (TWC)
Debit Card System	DCS Bulk File Agents
	MID/TID Allocation Database
	MID/TID Allocation Service Application
EMC Disk Array Driver Software	EMC Symmetrix manager Control Utilities
File Transfer Management Service	FTMS Core Application
Key Management Service	Key Store Service
	KM Client Agent
	KM Common Functions
Maestro Scheduler (TWS)	Tivoli Maestro Agent for NT Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Open Database Connectivity	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft SQL Server	ActiveX Data Objects (ADO)
	Microsoft NT Runtime for DAO
	Microsoft Open Database Connectivity (ODBC) Driver
	Microsoft SQL Server
Microsoft Visual Studio	Microsoft VB Runtime DLLs
Microsoft Windows NT	Microsoft FTP
	Microsoft Windows Scripting Host
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Server
Oracle Relational Database Software	Oracle for Windows NT4 Networking Products
	Oracle Net for Windows NT (previously SQL*Net)
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Retail Logic Solve/SE and Solve/PFG	Solve/PFG Payment File Generation for NT

	Solve/SE SPF Edit Utility
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Sapher Layer7	Layer7
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Server
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
	Tivoli Agent/Host Recovery
TeamWARE Crypto	TeamWARE Crypto (TWC)
Transaction Management System	Agent Performance Monitor Libraries
	Cluster Lookup Service (LUC)
	Multiple Riposte Library
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Client
	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server

10.6 SUN SERVERS

10.6.1 Operating Systems

Solaris is a variant of Unix supported by SUN.

10.6.1.1 Structure

Component	Platforms
NTP for Solaris (Network Time Protocol)	Firewall Management Server Firewall Module - 1 SecurID ACE Server
Solaris English Media Kit	Firewall Management Server Firewall Module - 1 SecurID ACE Server
Solaris Operating System	SecurID ACE Server TME Event Server - 1 TME Event Server - 2

10.6.1.2 Secure Solaris Build

As with the other operating systems used in Horizon, a “secure Solaris build” is created and maintained by PIT.

10.6.2 Standards

Hardware	Type	Sun	
Operating System		Solaris 2.6.1	
Capsules	Time Services	NTP version 3.5f	From the Internet

Table 10.5 - Sun Common Configuration

10.6.3 Network Management Server

Purpose Runs HP OpenView, CISCO Works and CISCO View. It provides a GUI interface for management and configuration of Routers and Firewalls. Also used to give Telnet access to the Routers and Firewalls when the graphical tools are unsuitable. Also runs TACACS.

Type SUN Ultra 1 Model 170E Server

Property	*Value*
CPU Speed	166 MHz
CPU Type	Ultra SPARC
Disk size	3 x 2.1 Gb
Memory	256 Mb
Monitor	20" "
Operating System	Solaris 2.6
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	<<<	
Wigan Campus	2	<<<	

Application	*Component*
Access Control and User Administration	Terminal Access Controller Access Control System (TACACS)
Auto-configuration	AutoConfig ISDN Router Configuration Script Generator
Build & Installation Processes	Secure Solaris
HP OpenView Network Management	CISCO Works 3.2/Solaris - HP OpenView
	CISCOView
	CISCOView for Tivoli
	HP OpenView Network Node Manager
	HP OpenView to Tivoli Event Adapter

10.6.4 TME Event Server

Purpose Collects, analyses and displays Tivoli event information.

Type Sun Ultra Enterprise 2/1170 Server (plus earlier variants)

Property	*Value*
Footprint	3U
Memory	128 Mb
Monitor	14" "
Operating System	Solaris 2.6
VLAN	Tivoli Management LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BTEC001
Bootle Campus	1	<<<	BTEC002
Bootle Campus	1	<<<	BTEC003
Bootle Campus	1	BI3	BETEC01
Bootle Campus	1	<<<	BMASTEC001
Wigan Campus	3	<<<	WTEC001..3
Wigan Campus	1	BI3	WETEC01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	WMASTEC001

Application	*Component*
Sun Solaris	Solaris Operating System
Systems Management Environment	MANSOEP
Tivoli Management Environment	TEC
	TMR

10.6.5 Firewall Management Server

Purpose Manages Firewall configurations

Type SUN Ultra Workstation

Property	*Value*
Operating System	Solaris 2.6
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	btlmgr01
Wigan Campus	1	<<<	wimgr01

Application	*Component*

Build & Installation Processes	Enterprise Centre Installation Routines Firewall Module Installation Routines Firewall-1 Configuration Secure Solaris
Firewall Management Software	Checkpoint Firewall Security Software (Gateway) Enterprise Centre Firewall Management Software
Sun Solaris	NTP for Solaris (Network Time Protocol) Solaris English Media Kit
Systems Management Environment	MANSOEP

10.6.6 SecurID Ace Server

Purpose Handles SecurID Authentication

Type Sun Ultra Workstation

Property	*Value*
Operating System	Solaris 2.6
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	btlfent01
Wigan Campus	1	<<<	wigfent01

Application	*Component*
Build & Installation Processes	Secure Solaris SecurID ACE Server Installation Routines
SecurID Access Control Software	SecurID ACE/Server
Sun Solaris	NTP for Solaris (Network Time Protocol) Solaris English Media Kit Solaris Operating System
Systems Management Environment	MANSOEP MANTOOLS

10.6.6.1 TME Gateway Server

Purpose Provides Tivoli management facilities for a range of managed end points.

Type Sun Netra

Property	*Value*
Footprint	1U
VLAN	Tivoli Management LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	BI1C	BCGW01
Bootle Campus	1	BI1C	BLGW01
Bootle Campus	10	BI1C	BPGW01..10
Bootle Campus	1	BI3	
Bootle Campus	8	BI3	
Bootle Campus	1	S30	
ISD Development & Test	2	BI3	
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	7	BI3	
Test - B&TC2 Volumes & Integration Rig	4	S30	
Test - IPDU System Test (INF1)	1	BI3	
Test - IPDU System Test (INF1)	2	S30	
Test - LST Main Rig	1	BI3	
Test - LST Main Rig	1	S30	
Test - PIT	1	S30	
Test - PTU	1	BI3	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	BI1C	WCGW01
Wigan Campus	1	BI1C	WLGW01
Wigan Campus	10	BI1C	WPGW01..10
Wigan Campus	8	BI2R	
Wigan Campus	1	BI3	
Wigan Campus	1	S30	

Application	*Component*

Systems Management Environment	Brain Builder MANSOEP MANTOOLS MANTRC - Tivoli Remote Console Management
Tivoli Management Environment	TMR

10.7 OTHER SERVERS

10.7.1 Network Time Server

Purpose Dedicated Network server. Broadcasts an accurate time signal over the Campus LAN.

Type TrueTime Network Time Server

Property	*Value*
Device	GPS Antenna
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.8 WORKSTATIONS

The workstation requirement is dominated by the population of around 40,000 Counter PCs, installed in around 19,000 Post Offices throughout the UK.

A number of other Workstations are used for a wide range of purposes, mostly within Pathway's management.

As with servers, the primary concern is value for money, with security a close second. Thus the hardware Platform chosen for all workstations is Intel-based, and the operating system is Windows NT Workstation. The latter is extremely similar to the Windows NT Server used for the commodity server systems, but cheaper and with fewer facilities.

As mentioned, security is a major concern in the choice of Windows NT. The operating system has been shown to be able to achieve an ITSEC C2 security rating. However, it cannot achieve this "out of the box", and hence all Windows NT systems used must be specifically built and configured to achieve the highest achievable levels of security. Chapter 16 "Security" discusses this in more detail.

10.8.1 Counter Terminals

Around 40,000 *Counter PCs* will be installed in over 19,000 Outlets and used by non-computer literate staff. These systems must be inexpensive, robust, easy to use and easy to install and configure. There are four basic configuration types, listed in full in [CNTD].

- Single Counter PCs (CC/S/G/1)
- Gateway PCs in Multi-Counter Outlets (CC/S/G/M)
- Counter PCs in Multi-Counter Outlets (CC/S/C)
- Mobile Counters

These contain all or most of the components listed here

Purpose Supports POCL Counter staff.

Type Fujitsu ErgoPro x365/400

Property	*Value*
CD-ROM	No
Connection type	Ethernet 10baseT/100baseT
Connection type	10baseT
Connection type	ISDN BRI
CPU Speed	400 MHz
Device	Smart Card Reader
Device	Swipe Card Reader
Device	Weigh Scales
Device	Tally Roll Printer
Disk size	13 Gb
Diskette	Blanked off "
Filestore	Encrypted
Keyboard	LIFT Financial Keyboard
Memory	128 Mb
Mouse	No
Network Card	8-port serial
NT Service	KMRx
NT Service	AdminCfg
NT Service	Tivoli Remote Execution Service
NT Service	Tivoli Endpoint
NT Service	TECNet Adapter
NT Service	Listener
NT Service	KeyStore
NT Service	Riposte
NT Service	AdminSet
NT Service	Riposte Training Service
NT Service	Call Monitor
NT Service	VPNConfig
NT Service	Tivoli
NT Service	TMSPOAcknowledge
NT Service	Downloader
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
Page File	200 Mb

Site	*Qty*	*Installed*	*Platform Name*
Eight-Counter Outlets	1	<<<	
Eighteen-Counter Outlets	1	<<<	
Eleven-Counter Outlets	1	<<<	
Fifteen-Counter Outlets	1	<<<	
Five-Counter Outlets	1	<<<	
Four-Counter Outlets	1	<<<	
Fourteen-Counter Outlets	1	<<<	
Nine-Counter Outlets	1	<<<	
Nineteen-Counter Outlets	1	<<<	
Release 2 Test Rig	1	<<<	
Seven-Counter Outlets	1	<<<	
Seventeen-Counter Outlets	1	<<<	
Six-Counter Outlets	1	<<<	
Sixteen-Counter Outlets	1	<<<	
Ten-Counter Outlets	1	<<<	
Test - REL1 Release Rig	5	<<<	
Thirteen-Counter Outlets	1	<<<	
Three-Counter Outlets	1	<<<	
Twelve-Counter Outlets	1	<<<	
Twenty-Counter Outlets	1	<<<	
Two-Counter Outlets	1	<<<	

Application	*Component*
Access Control and User Administration	Post Office Log On (POLO)
Audit Facilities	Counter File Audit
Auto-configuration	ACF with In-line SIPU Auto Configuration - Counter Counter Downloader Listener PcConfig Rollout Synchronisation (Counter)
Automated Payments Service	APS Counter Application APS SCCache

Build & Installation Processes	Counter Installation Routines
	Eicon Gateway PC ISDN Card Settings
	Escher Counter Configuration
	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
Crypto Code	CAPU Check Handler
	Core Signing Functions (CSF)
	Core Verifying Functions (CVF)
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	PMMC Agent
	PMMC Common Library
	Siemens Metering Counter
	TeamWARE Crypto (TWC)
Crypto Keys	Crypto Keys - (APPR)TK via Automatic Channel
	Crypto Keys - (GDK)TK via Automatic Channel
	Crypto Keys - (NBTDO)TK via Automatic Channel
	Crypto Keys - (NVPN)PIN via Automatic Channel
	Crypto Keys - (NVPN)TK via Automatic Channel
	Crypto Keys - CAPU Checks via Automatic Channel
	Crypto Keys - CRL via Automatic Channel
	Crypto Keys - DLLKA via Interactive Channel
	Crypto Keys - DLLKB via Automatic Channel
	Crypto Keys - EVPN (common) via Build or Tivoli
	Crypto Keys - FEK (Outlet-specific) via Interactive Channel
	Crypto Keys - In-line SAPU PKC via Riposte
	Crypto Keys - KIPU PKC in-line via Interactive Channel
	Crypto Keys - NVPN (Outlet specific) via Interactive Channel
	Crypto Keys - POK (Initial) via BSF
	Crypto Keys - POK (Outlet specific) via Interactive Channel
	Crypto Keys - SIPU PKC via AutoConfig or Tivoli
	Crypto Keys - TK (Outlet specific) via Interactive Channel
	Crypto Keys - VPN CRL via Automatic Channel
Debit Card System	DCS Counter Application
	DCS Counter Recovery Application
Eicon Driver Software	Eicon Client ISDN Driver
	Eicon ISDN DIVA Basic Rate Card
Electronic Point of Sale Service	EPOSS Counter Application
	HTML
	MiMAN
Europa Test Facilities	Europa Installation Test Utilities
Hardware Configurations	LIFT Keyboard with Integral Magnetic card/Smart Card Reader
Horizon Help Desk	Counter Diagnostics
Key Management Service	KM Client Agent
	KM Common Functions
	KM Dist Receiver Mon Dispatcher
	KM Interactive Channel Client
Logistics Feeder Service	LFS Counter Application
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Visual Studio	Microsoft VB Runtime DLLs
	Microsoft Visual C++ Runtime DLLs
Microsoft Windows NT	Microsoft NT Workstation
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Microtouch Screen Driver	Microtouch Screen Driver
Network Banking Service	Magnetic Card Token Manual Input
	Magnetic Card Token Validation Function
	NBS Counter Application
	NBS Counter Application Support
	NBS Counter Recovery Application
Order Book Control Service	OBCS Counter Application
Outlet Monitoring Service	Counter Network Information Monitor
Performance Measurement System	Metron Athene Acquire - NT Performance Management Agent
Reference Data Management Service	Counter Reference Data
Riposte Desktop	Memo View
	Other Riposte Counter Software
	WebRiposte Common - Software Unsigned by Escher
	WebRiposte Counter - Unsigned Riposte Files
	WebRiposte Signed - Software Signed by Escher
Riposte Message Server	Non RDMC Persistent Objects from Escher
Sapher Layer7	Layer7
Software Signing	Counter Tivoli Inventory Signatures
	SI Verifying Functions (SVF)

Specialix	Specialix Driver Software (installation disk image)
SysInternals BlueSave Support Software	Winternals Software BlueSave for Windows NT4.0
Systems Management Environment	AdminCfg
	Counter Application Scheduler
	ISDN Call Monitor
	MANEVENT
	MANEVENT Filter Counter
	MANNTEP
	MANSENTRY Counter
	MANSENTRYCFG Counter
	MANTOOLS
	NT Backup System
	NT Fail Safe Startup System
	Software Distribution - Counter
TeamWARE Crypto	TeamWARE Crypto (TWC)
Transaction Management System	Agent Counter Common
	Counter Configuration Administration
	Counter Shutdown Monitor
	TMS PostOfficeRedirector - Agent
	TMS PostOfficeWait - Agent
	User Lock Request Library
TRIAGE Audit Software	Triage Monitoring Client
Utimaco Safeguard VPN Software	Utimaco SG VPN
	VPN Red Pike Driver
Virtual Private Network	VPN Config Application
	VPN Counter Configuration
	VPNConfig
WebRiposte	Asset Manager Web Services
	Memo View
	WebRiposte Client
	WebRiposte Desktop
	WebRiposte Message Server
WebRiposte Financial Transaction Framework	FT Application Framework Desktop Client
	FT Application Framework Web Services

10.8.2 Other Windows NT Workstations

10.8.2.1 Horizon Help Desk Terminal

Purpose Provides support facilities to Horizon Help Desk operators

Type Fujitsu ErgoPro PC

Property	*Value*
Connection type	Ethernet 10baseT/100baseT
CPU Speed	166 MHz
Device	CD-ROM
Disk size	2.1 Gb
Memory	32 Mb
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty Installed*	*Platform Name*
CS Bracknell	50	<<<
ISD SMC MAN 05, Manchester	50	<<<
ISD SMC Stevenage 09	100	<<<

Application	*Component*
Build & Installation Processes	NT Common File Set
Horizon Help Desk	PowerHelp Client
Microsoft Windows NT	Microsoft NT Workstation
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Order Book Control Service	OBCS Stop List Enquiries
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT Filter Workstation
	MANTOOLS

10.8.2.2 MIS Client Workstation

Purpose Allows analysis of information stored in the Data Warehouse. Mostly based at Bracknell, with a further two PCs located in FEL01 for disaster recovery purposes. All contain the Oracle OLAP clients, along with specific client software for MIS applications.

Type Fujitsu ErgoPro x451 (min.)

Property	*Value*
CD-ROM	Writer
CPU Speed	1.5 GHz
Disk size	40 Gb
Memory	512 Mb
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	3	<<<	WBRBSC01..03
Pathway at Feltham	5	<<<	WFEMIS01..05
Pathway Feltham Secure Area	2	<<<	WFEMIS01..02
SSC, Bracknell	3	BI3	WBRMIS01..03

Application	*Component*
Build & Installation Processes	Generic Common File Installation Routines Generic NT Platform Install Routines MIS Client PC Installation Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Business Objects Hummingbird Communications Software Management Information Service	Business Objects - End User Bundle Hummingbird NFS Maestro Solo Ad Hoc Reporting Universe MIS Business Development Reporting MIS Business Objects MIS Business Objects APR MIS Business Objects Customer Service Reporting MIS Business Objects Universe MIS Common Software MIS Contract Administration MIS Reference Data Maintenance
Microsoft Office	Microsoft Office 97 Professional Microsoft Office 97 SR2
Microsoft Windows NT	Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Network Banking Service Oracle Relational Database Software	Network Associates AV Suite - Workstation DRS Workstation Application Oracle Developer 2000 Oracle Discoverer 2000 Client Oracle Discoverer Meta Layer Oracle Express Objects Workstation Oracle for Windows NT4 Networking Products Oracle Forms (Runtime) for NT Oracle Net for Windows NT (previously SQL*Net)
SecurID Access Control Software System Support Centre	SecurID Agent for NT BSU Help Desk Help Desk Common Files WinOnCD Recording Software
Systems Management Environment	MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS NT Fail Safe Startup System
TRIAGE Audit Software WinZip	Triage Monitoring Client WinZip

10.8.2.3 MIS Support Workstation

Purpose Allows analysis of information stored in the Data Warehouse. Mostly based at Bracknell, with a further two PCs located in FEL01 for disaster recovery purposes.

All contain the Oracle OLAP clients, along with specific client software for MIS applications.

Type Fujitsu ErgoPro x451 (min.)

Property	***Value***
CD-ROM	Writer
CPU Speed	1.5 GHz
Disk size	40 Gb
Memory	512 Mb
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	***Qty Installed***	***Platform Name***
SSC, Bracknell	1	BI3
Test - APDU (2 rigs)	2	<<<
Test - LST Main Rig	1	BI3
Test - PIT	1	<<<

Application	***Component***
Build & Installation Processes	Generic Common File Installation Routines Generic NT Platform Install Routines MIS Client PC Installation Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Business Objects	Business Objects - Designer Bundle Business Objects - End User Bundle
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Management Information Service	Ad Hoc Reporting Universe MIS Business Development Reporting MIS Business Objects MIS Business Objects APR MIS Business Objects Customer Service Reporting MIS Business Objects Universe MIS Common Software MIS Contract Administration MIS Reference Data Maintenance
Microsoft Office	Microsoft Office 97 Professional Microsoft Office 97 SR2
Microsoft Windows NT	Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Network Banking Service	DRS Workstation Application
Oracle Relational Database Software	Oracle Developer 2000 Oracle Discoverer 2000 Client Oracle Discoverer Meta Layer Oracle Express Objects Workstation Oracle for Windows NT4 Networking Products Oracle Forms (Runtime) for NT Oracle Net for Windows NT (previously SQL*Net)
SecurID Access Control Software	SecurID Agent for NT
System Support Centre	BSU Help Desk Help Desk Common Files WinOnCD Recording Software
Systems Management Environment	MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS NT Fail Safe Startup System
TRIAGE Audit Software	Triage Monitoring Client
WinZip	WinZip

10.8.2.4 Audit Workstation

Purpose Provides facilities for audit staff to access the Audit Server in order to retrieve Audit Track data and to either select and prepare Audit Track data for presentation to the POCL and DSS auditors or in support of internal audit activities

Type Compaq DeskPro EN Series 6266 M3200 NT

Property	*Value*
CPU Speed	200 MHz
Device	Internal crypto co-processor
Device	CD-Writer
Disk size	8 Gb
Disk type	Diskette
Memory	64 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	<<<	WBOAUD01..nn
Pathway Feltham Secure Area	2	<<<	WFEAUD01..02
Pathway Feltham Secure Area	5	BI3	wfeaud003..007
Test - B&TC1 Integration	1	S30	
Test - B&TC2 Volumes & Integration Rig	1	<<<	
Test - B&TC5 Testing Support	1	S30	
Test - B&TC7 PET/UTC	1	S30	
Test - IPDU Development	1	S30	
Test - IPDU System Test (INF1)	1	S30	
Test - LST Main Rig	1	S30	
Test - REL1 Release Rig	1	S30	
Wigan Campus	1	<<<	WWIAUD01

Application	*Component*
Adaptec Drivers	Adaptec EasyCD Creator Deluxe Edition
Audit Facilities	Audit Data Retrieval Agent
	Audit Extraction & Filtering Application - Client
	Audit Server Application
Build & Installation Processes	Audit Workstation Installation Routines
	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Keys	Crypto Keys - TK via Manual
Legato Application and Driver Software	DLT7000 Drivers for Windows Intel Platforms
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Office	Microsoft Office 97 Professional
	Microsoft Office 97 SR2
Microsoft SQL Server	Microsoft NT Runtime for DAO
Microsoft Windows NT	Microsoft NT Workstation
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Oracle Relational Database Software	Oracle Discoverer 2000 Client
Riposte Desktop	WebRiposte Common - Software Unsigned by Escher
Riposte Utilities	Riposte Utilities from Escher
SecurID Access Control Software	SecurID Agent for NT
System Support Centre	Riposte Query UK
Systems Management Environment	MANEVENT
	MANEVENT Filter Workstation
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
Transaction Management System	Audit Data Retrieval Agent
	Cluster Lookup Service (LUC)
TRIAGE Audit Software	Triage Monitoring Client
WebRiposte	WebRiposte Data Centre - Software Unsigned by Escher
	WebRiposte Message Server
WinZip	WinZip

10.8.2.5 RDMC Administrator Workstation

Purpose Used for data entry and Reference Data release authorisation. It also provides a facility for Pathway Customer Services to send messages to some or all installed Outlets. It runs bespoke VB applications which link to the (RDMC) Oracle database.

Type Fujitsu ErgoPro x453 with Windows NT Workstation

Property	*Value*
CPU Speed	166 MHz
Disk size	2.1 Gb

Memory	64 Mb
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	6	<<<	WBRRDM01..06
CS Bracknell	1	BI3	WBRRDM07
Pathway at Feltham	1	<<<	WFERDM01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Automated Payments Service	APS Administration Workstation Setup
	APS User Maintenance
Build & Installation Processes	APS Administration Workstation Setup
	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
	RDMC Admin Workstation Installation Routines
	RDMC Administration Workstation Setup
Hummingbird Communications Software	Hummingbird NFS Maestro Solo
Maestro Scheduler (TWS)	Maestro Remote Console
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Office	Microsoft Office 97 Professional
	Microsoft Office 97 SR2
Microsoft Open Database Connectivity	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft SQL Server	Microsoft Data Access Components (MDAC)
	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft Windows NT	Microsoft NT Workstation
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Oracle Relational Database Software	Oracle Discoverer 2000 Client
	Oracle for Windows NT4 Networking Products
	Oracle Net for Windows NT (previously SQL*Net)
	Oracle ODBC Driver
	Oracle SQL Worksheet
	Oracle SQL*Plus
Reference Data Management Service	Message Submission Application
	RDMC - Change Control Application
	RDMC Access Control
	RDMC Administration Application
	RDMC Interactive Data Loader
	RDMC Release Manager
	RDMC Reports
	RDMC Send
SecurID Access Control Software	SecurID Agent for NT
Systems Management Environment	MANEVENT
	MANEVENT Filter Workstation
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
WinZip	WinZip

10.8.2.6 SSC Support Workstation

Purpose 3rd line support of Horizon hardware in Outlets

Type Fujitsu ErgoPro x453/166

Property	*Value*
CPU Speed	166 MHz
CPU Type	Pentium
Device	CD-Writer
Disk size	2.1 Gb
Memory	32 Mb
Monitor	17" "
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
SSC, Bracknell	25	<<<	SSCBR01..28

Application	*Component*
Adaptec Drivers	Adaptec EasyCD Creator Deluxe Edition
Build & Installation Processes	Generic NT Platform Install Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
	SSC Workstation Installation Routines
Hummingbird Communications Software	eXceed Xclient Software
Microsoft Internet Explorer	Microsoft Internet Explorer (Minimum Install)
Microsoft Office	Microsoft Office 97
Microsoft SQL Server	Microsoft SQL Server Client
Microsoft Visual Studio	Microsoft Visual Basic
Microsoft Windows NT	Microsoft FTP
	Microsoft NT Workstation
	NotePad (part of NT)
	Performance Monitor (from NT Resource Kit)
	POSIX Subsystem
	Time Service (Windows NT Resource Kit)
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Oracle Relational Database Software	Oracle Forms (Runtime) for NT
	Oracle Net for Windows NT (previously SQL*Net)
	Oracle SQL*Plus
Performance Measurement System	Performance Management Analysis Tools
Riposte Desktop	Rconsole
Riposte Utilities	Riposte Tools
SecurID Access Control Software	SecurID Agent for NT
System Support Centre	Archive Viewer
	EndOfDay Reporter
	Expiry Reporter
	Formatted File Utility
	Message Store Utility
	MessageStore Sort Utility
	Pathway Event Viewer
	Riposte Query UK
	Stops Reporter
	WinOnCD Recording Software
Systems Management Environment	MANEVENT
	MANEVENT Filter Workstation
	MANNTEP
	MANTOOLS
	MANTRC - Tivoli Remote Console Management
TextPad	TextPad
TRIAGE Audit Software	Triage Monitoring Client
Virtual Private Network	VPN Remote Management Client Application
WebRiposte	Rconsole
	WebRiposte Client
WinZip	WinZip

10.8.2.7 One Time Password Workstation

Purpose Generates one-time passwords for use by visiting staff at Outlets

Type Fujitsu ErgoPro x453/166

Property	*Value*
CPU Speed	166 MHz
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
ISD SMC Stevenage 09	3	<<<	WSTOSP01

Application	*Component*
Access Control and User Administration	One Time Password Application
	System Integrity Check Application
Microsoft Windows NT	Microsoft NT Workstation
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
Systems Management Environment	NT Fail Safe Code Generator Utility

10.8.2.8 ACDB Client Workstation

Purpose Used to configure the Auto Configuration database.

Type Fujitsu ErgoPro x453/166 PC

Property	*Value*
CPU Speed	166 MHz
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	WBOACC01??
Pathway, Kidsgrove	1	<<<	WKIACC01
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Auto-configuration Build & Installation Processes	ACDB Client Auto Configuration Server Client Installation Routines Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Microsoft Internet Explorer Microsoft Open Database Connectivity Microsoft SQL Server	Microsoft Internet Explorer (Minimum Install) Microsoft Open Database Connectivity (ODBC) Driver Microsoft NT Runtime for DAO Microsoft Open Database Connectivity (ODBC) Driver Microsoft SQL Server Client
Microsoft Visual Studio Microsoft Windows NT	Microsoft VB Runtime DLLs Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Workstation SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.8.2.9 Tivoli Brain Builder

Purpose Used to pre-build the configurations that are downloaded to Counter PCs at Installation. Operated by ISD on ICL's Pathway behalf. Although Pathway supplies the hardware, the software and the running of the service is entirely the responsibility

Type Fujitsu ErgoPro PC x365/400

Property	*Value*
CPU Speed	400 MHz
Disk size	4.3 Gb
Memory	64 Mb
NT Service	Tivoli Brain Builder
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	BRAINBUILDER 4
Wigan Campus	1	<<<	BRAINBUILDER 1

Application	*Component*
Systems Management Environment	Brain Builder MANSYS

10.8.2.10 SecurID Admin Workstation

Purpose Used for remote administration of the SecurID servers at Wigan and Bootle, and for Firewall Monitoring and Security Event Monitoring.

Type Fujitsu ErgoPro x365/360 PC

Property	*Value*
CPU Speed	266 MHz
CPU Type	Pentium
Disk size	4.3 Gb
Memory	64 Mb
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Pathway Feltham Secure Area	2	<<<	WFEACE01..2
Wigan Campus	1	<<<	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build SecurFS CMD Script SecurID Installation Routines
Microsoft Internet Explorer Microsoft Office	Microsoft Internet Explorer (Minimum Install) Microsoft Access Microsoft Office 97 SR2
Microsoft Windows NT	Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Workstation SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS Tivoli Web Browser
TRIAGE Audit Software	Triage Monitoring Client

10.8.2.11 CA Workstation

Purpose Free-standing Workstation used to hold CAPR certificate and to certify Keys from the KMA. Supplied by Utimaco; only the components added by Pathway are identified.

Type Utimaco Cryptware Server

Property	*Value*
Card Reader	Utimaco
CPU Speed	333 MHz
CPU Type	Pentium II
Device	ComScire Random Number Generator
Device	Diskette 3.5" 1.44 Mb
Disk size	4.3 Gb
Disk type	Iomega Jaz drive
Memory	128 Mb
Operating System	Microsoft NT Server 4.0 with Service Pack 6a
Page File	128 Mb

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	<<<	WBRCAW01
Pathway Feltham Secure Area	1	<<<	WFECAW01

Application	*Component*
Build & Installation Processes	CA Workstation Installation Routines CA Workstation VPN Install Generic NT Platform Install Routines NT Secure Build
Crypto Code	Crypto Keystore Service (CKS) Cryptographic Functions API Entropy Generation Application (EGA) PMMC Common Library TeamWARE Crypto (TWC)
Crypto Keys	Crypto Keys - CAPR (Black) via Diskette Crypto Keys - CAPR (Red) via Diskette

	Crypto Keys - CAPU Checks via Automatic Channel
	Crypto Keys - CRL via zip drive
	Crypto Keys - KIPU PKC In-Line via zip drive
	Crypto Keys - VPN Sec Data
IomegaWare Jaz Drive Software	IomegaWare Jaz Drive Software
Key Management Service	Key Generator (Red Pike)
	Key Store Service
	KM Client Agent
	KM Common Functions
	KMA Bundle Handler
	KMA Certification Authority
Microsoft Office	Microsoft Office 2000 SR1
Microsoft Open Database Connectivity	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft SQL Server	Microsoft Open Database Connectivity (ODBC) Driver
Microsoft Visual Studio	Microsoft Visual C++ Runtime DLLs
Microsoft Windows NT	Microsoft NT Server
	Microsoft NT Workstation
	Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Suite - Workstation
PKZIP	PKZIP
QNG Device Drivers	QNG Device Driver
Sapher Layer7	Layer7
TeamWARE Crypto	TeamWARE Crypto (TWC)
Utimaco Safeguard VPN Software	Utimaco Cryptware PKI (CA/RA)
	Utimaco Cryptware Toolkit Runtime
	Utimaco Key Generator
	Utimaco Registration Authority Batch (RAB)
	Utimaco SG VPN

10.8.2.12 KMA Workstation

Purpose Used by Key Custodian for Key management administration.

Type Compaq DeskPro EN Desktop

Property	*Value*
Connection type	100baseT
CPU Speed	333 MHz
Device	ComScire Random Number Generator
Device	Diskette 3.5" 1.44 Mb
Disk size	4.3 Gb
Disk type	Iomega Jaz drive
Memory	128 Mb
Monitor	17" "
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	<<<	WBRKAW01
Pathway Feltham Secure Area	1	<<<	WFEKAW01
Release 2 Test Rig	1	<<<	
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Adaptec Drivers	Adaptec AHA-2940 Ultra PCI Adapter
Build & Installation Processes	Generic NT Platform Install Routines
	KMA Workstation Installation Routines
	NT Common File Set
	NT Platform Fast Track Fixes
	NT Secure Build
Crypto Code	CAPU Check Handler
	Crypto Keystore Service (CKS)
	Cryptographic Functions API
	Entropy Generation Application (EGA)
	PMMC Common Library
	TeamWARE Crypto (TWC)
Crypto Keys	Crypto keys - (KMA Key)TK via SQL
	Crypto Keys - CAPU Checks via Automatic Channel
	Crypto Keys - DLLKA/B from L&G via Diskette
	Crypto Keys - GDK via Diskette
	Crypto Keys - IPOK Set via Diskette
	Crypto Keys - NVPN set via diskette

IomegaWare Jaz Drive Software Key Management Service	IomegaWare Jaz Drive Software Key Generator (DSA) Key Generator (L&G) Key Generator (Red Pike) KM Client Agent KM Common Functions KM Reports KMA Bundle Handler KMA User Interface KMA Workstation Application
Microsoft Internet Explorer Microsoft Office Microsoft SQL Server	Microsoft Internet Explorer (Minimum Install) Seagate Crystal Reports (Professional) ActiveX Data Objects (ADO) Microsoft Data Access Components (MDAC) Microsoft SQL Server Client SQL NetLib
Microsoft Visual Studio	Microsoft VB Runtime DLLs Microsoft Visual Studio Runtime
Microsoft Windows NT	Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software QNG Device Drivers Sapher Layer7 SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Workstation QNG Device Driver Layer7 SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TeamWARE Crypto TRIAGE Audit Software	TeamWARE Crypto (TWC) Triage Monitoring Client

10.8.2.13 KMS Admin Workstation

Purpose Handles management & administration of KMC Database

Type Compaq DeskPro EN Desktop

Property	*Value*
Connection type	10baseT
CPU Speed	333 MHz
Disk size	4.3 Gb
Diskette	Blanked off "
Memory	64 Mb
Monitor	17" "
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	WBOKSA01
CS Bracknell - Secure Area	1	<<<	WBRKSA01
ISD Belfast Bridgeview	1	<<<	WBEKSA01
ISD Belfast Trident House	1	<<<	WBEKSA02
Pathway Feltham Secure Area	2	<<<	WFEKSA01..02
Release 2 Test Rig	1	<<<	
SSC, Bracknell	2	<<<	WBRKSA02..03
Test - B&TC2 Volumes & Integration Rig	2	<<<	
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines KMS Admin Workstation Installation Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Key Management Service Microsoft Internet Explorer Microsoft Office	KM Reports Microsoft Internet Explorer (Minimum Install) Microsoft Office 2000 SR1 Seagate Crystal Reports (Professional)
Microsoft Open Database Connectivity Microsoft SQL Server	Microsoft Open Database Connectivity (ODBC) Driver Microsoft Open Database Connectivity (ODBC) Driver Microsoft SQL Server Client

Microsoft Visual Studio Microsoft Windows NT	Microsoft Visual Studio Runtime Microsoft NT 4.0 Resource Kit Microsoft NT 4.0 Server Tools Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Workstation SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software	Triage Monitoring Client

10.8.2.14 Tivoli Support Workstation

Purpose Part of the Tivoli Managed Service provided by ISD

Type Fujitsu ErgoPro x453

Property	*Value*
CPU Speed	166 MHz

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
ISD SMC MAN 05, Manchester	1	<<<	
ISD SMC Stevenage 09	1	<<<	
ISD, Lytham St Annes	10	<<<	
Release 2 Test Rig	1	<<<	
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*
Build & Installation Processes	Common File Set NT Common File Set Tivoli Workstation Installation Routines
Key Management Service	KM Common Functions KMA Help Desk GUI
Microsoft SQL Server	ActiveX Data Objects (ADO) Microsoft NT Runtime for DAO Microsoft SQL Server Client
Microsoft Visual Studio	Microsoft VB Runtime DLLs Microsoft Visual C++ Runtime DLLs
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Systems Management Environment	Network Associates AV Suite - Workstation MANEVENT Filter Workstation MANNTEP MANTOOLS MANTRC - Tivoli Remote Console Management

10.8.2.15 Operations Terminal

Purpose Remote system operation

Type X-Terminal app. On NT Workstation

Property	*Value*
Monitor	17" "

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	<<<	WBOOPS01..nn
CS Bracknell	2	<<<	Approx. number
ISD Belfast Bridgeview	3	<<<	
ISD Belfast Trident House	18	<<<	WBEOPS01..nn
Wigan Campus	2	<<<	WWIOPS01..02

Application	*Component*
Build & Installation Processes	NT Secure Workstation Build

Network Associates Anti-Virus Software Systems Management Environment	Network Associates AV Suite - Workstation MANEVENT Filter Workstation MANTOOLS

10.8.2.16 OCMS Client

Purpose Used for administration of the Outlet Change management System

Type Compaq DeskPro EN Spacesaver 733

Property	*Value*
Disk Partition	6 Gb
Disk Partition	4 Gb
Disk type	Diskette
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
VLAN	OCMS LAN

Site	*Qty*	*Installed*	*Platform Name*
ISD, Lytham St Annes	1	S06	WLYOCM01
Pathway at Feltham	1	S06	WFEOCM01
Pathway, Kidsgrove	4	S06	WKIOCM01..04
Release 2 Test Rig	1	<<<	
SSC, Bracknell	2	S06	WBROCM01..02
Test - REL1 Release Rig	1	<<<	

Application	*Component*
Build & Installation Processes	Common File Set Generic NT Platform Install Routines NT Common File Set NT Secure Build OCMS Client Installation Routines
Business Objects Microsoft Internet Explorer Microsoft Office Microsoft Open Database Connectivity Microsoft SQL Server	Business Objects - End User Bundle Microsoft Internet Explorer (Minimum Install) Microsoft Excel Microsoft Open Database Connectivity (ODBC) Driver ActiveX Data Objects (ADO) Microsoft Data Access Components (MDAC) Microsoft NT Runtime for DAO Microsoft Open Database Connectivity (ODBC) Driver Microsoft SQL Server Client
Microsoft Visual Studio Microsoft Windows NT	Microsoft VB Runtime DLLs Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software Outlet Change Management Service SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Workstation OCMS Client Application SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS
TRIAGE Audit Software	Triage Monitoring Client

10.8.2.17 VPN Loopback Workstation

Purpose Used for diagnosis of VPN problems. Responds to HPOV "pings".

Type Compaq DeskPro EP 6600 Desktop

Property	*Value*
NT Service	Policy Management Client (PMC)
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a
VLAN	Summary LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	WBOVDW01
Test - REL1 Release Rig	1	<<<	
Wigan Campus	1	<<<	MWIVDW01

Application	*Component*

Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build VPN Loopback Workstation Installation Routines
Crypto Keys	Crypto Keys - (NVPN)PIN via Automatic Channel Crypto Keys - (NVPN)PIN via PMKM Crypto Keys - VPN CRL via Automatic Channel Crypto Keys - VPN PIN via Manual
Microsoft Windows NT	Microsoft NT Workstation Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
SecurID Access Control Software Systems Management Environment	SecurID Agent for NT MANEVENT Filter Workstation MANNTEP MANSENTRY VPNLW MANSENTRYCFG VPNLW MANTOOLS MANTRC - Tivoli Remote Console Management
TRIAGE Audit Software Utimaco Safeguard VPN Software	Triage Monitoring Client Utimaco SG VPN VPN Red Pike Driver
Virtual Private Network	VPN Loopback Workstation Configuration VPN PMC Pin Reader Application VPN Policy Management Client Application

10.8.2.18 Offline Key Generation Workstation

Purpose Provides a Managed Key Service for platforms that are not managed by KMS.

Type Fujitsu ErgoPro

Property	*Value*		
Site	***Qty***	***Installed***	***Platform Name***
CS Bracknell - Secure Area	2	<<<	

Application	*Component*
Crypto Code	Entropy Generation Application (EGA) PMMC Common Library Siemens Metering Offline
Key Management Service	Key Generator (DSA) Key Generator (Red Pike) KM Common Functions Managed Key Service
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
QNG Device Drivers Sapher Layer7	QNG Device Driver Layer7

10.8.2.19 Systems Management Access Workstation

Purpose Used in CS Annexe 2 at BRA 01 to access the ISD Operational Management Database. It provides a Web Browser capability to view and update specific Tivoli data relating to releasing software to the Pathway network of PCs in POCL Outlets.

Type Fujitsu ErgoPro x453

Property	*Value*		
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a		
Site	***Qty***	***Installed***	***Platform Name***
CS Bracknell	1	<<<	

Application	*Component*
Build & Installation Processes	NT Common File Set NT Platform Fast Track Fixes NT Secure Build Systems Management Workstation Installation Routines

Microsoft Internet Explorer Microsoft Windows NT	Microsoft Internet Explorer (Minimum Install) Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus Software	Network Associates AV Server Management Console Network Associates AV Suite - Workstation
Oracle Relational Database Software SecurID Access Control Software Systems Management Environment	Oracle Developer 2000 SecurID Agent for NT MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS

10.8.2.20 Engineer's Day D Laptop

Purpose Used by Engineers for Day D Rectification on Outlets with failed ISDN lines

Type ErgoPro C332 Lifebook

Property	*Value*		
Site	***Qty***	***Installed***	***Platform Name***
Pathway Regional Office, Gloucester	5	S10R	
Pathway Regional Office, Hertford	1	S10R	
Pathway Regional Office, Tunbridge Wells	5	S10R	

Application	*Component*
Auto-configuration Eicon Driver Software	DayD PC Config Eicon C23 PSTN Modem Eicon PCMCIA ISDN Xircom 56 Kb Card
Microsoft Windows NT	Microsoft NT Server Windows NT Service Pack 6a - High Encryption + Hot Fixes
Systems Management Environment	MANEVENT Filter Workstation MANTOOLS

10.8.2.21 Service Management Workstation

Purpose Used to manage the Service Management Server

Type Ergopro

Property	*Value*		
Site	***Qty***	***Installed***	***Platform Name***
Pathway at Feltham	1	S06	

Application	*Component*
Build & Installation Processes Network Associates Anti-Virus Software Systems Management Environment	NT Common File Set Network Associates AV Suite - Workstation MANEVENT MANEVENT Filter Workstation MANNTEP MANTOOLS

10.8.2.22 PIN Pad Key Generation Workstation

Purpose Generates keys for use in HSM cards

Type Fujitsu Siemens PC

Property	*Value*
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	BI3	
Pathway Feltham Secure Area	1	BI2R	WFESKG01
Test - IPDU Development	1	BI3	
Test - LST Main Rig	1	BI3	
Test - PTU	1	BI3	

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

Application	*Component*
Build & Installation Processes	Generic NT Platform Install Routines NT Common File Set NT Platform Fast Track Fixes NT Secure Build
Crypto Code	Core Signing Functions (CSF) Crypto Keystore Service (CKS) Cryptographic Functions API
Crypto Keys	Crypto Keys - APPU PKC via automatic channel Crypto Keys - CAPU Set via Tivoli Crypto Keys - CRL via Automatic Channel Crypto Keys - SA KEK via Diskette Crypto Keys - SAPR via Build
Key Management Service	Key Store Service KM Client Agent KM Common Functions KM Interactive Channel Service
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Sapher Layer7	Layer7
Specialix	Specialix Driver Software (installation disk image)
Systems Management Environment	MANEVENT Filter Workstation MANTOOLS
Transaction Management System	User Lock Request Library

10.8.2.23 Atalla Card Loader Workstation

Purpose Used for manual generation of keys for HSM cards to be inserted in NBS Agent Servers and the KMA Workstation.

Type Fujitsu ErgoPro

Property	*Value*
Operating System	Microsoft NT Server 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	BI3	
Pathway Feltham Secure Area	1	BI2R	WFEACL01

Application	*Component*
Build & Installation Processes	NT Common File Set
Crypto Code	Atalla Key Loading Software Tool
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Systems Management Environment	MANEVENT Filter Workstation MANTOOLS

10.8.2.24 PIN Pad Proving Workstation

Purpose

Type

Property	*Value*
Operating System	Microsoft NT Workstation 4.0 with Service Pack 6a

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell - Secure Area	1	BI3	
Pathway Feltham Secure Area	1	BI2R	WFEPIN01

Application	*Component*
Build & Installation Processes	Common File Set NT Secure Build
Key Management Service	KM Common Functions
Microsoft Windows NT	Microsoft NT Workstation Windows NT Service Pack 6a - High Encryption + Hot Fixes
Sapher Layer7	Layer7
Specialix	Specialix Driver Software (installation disk image)

10.8.2.25 Anti Virus Workstation

Purpose Used prior to BI3 to scan for viruses on platforms that are not yet on SP6a and hence cannot use the preferred Anti-Virus software. Reuses previous Migration Agent Server platforms

Number 2

Platform

Type Operating System	Compaq DeskPro EN Microsoft NT Server with Service Pack 3

Capsules

Maestro Scheduler (TWS) Microsoft Windows NT	Tivoli Maestro Agent for NT Platforms Microsoft NT Server Time Service (Windows NT Resource Kit) Windows NT Service Pack 6a - High Encryption + Hot Fixes
Network Associates Anti-Virus SecurID Access Control Software Systems Management Environment	Network Associates AV Suite - Server SecurID Agent for NT MANEVENT Filter Workstation MANSYS MANTOOLS MANTRC - Tivoli Remote Console Management Tivoli Generic Service Monitor

10.9 NETWORK DEVICES

10.9.1 General

Network Active Devices (Hubs, Routers and Firewalls) are supplied by Cisco. None of these has an attached console in normal working. The only method of direct connection is via Telnet connection from the Network Management System.

These descriptions are included for completeness. In general, each instance of a network device is configured specifically for its position in the network, and it is not possible to generalise about them in the same way as for servers and workstations.

The following members of the Cisco range of Routers and Switches are used.

- Cisco Catalyst 5000 switches, which supports two 100baseT or 100baseFx interfaces, and a modular construction which supports a variety of different types of LAN connections.
- Cisco Catalyst 2900 24-port switches supporting 100baseT
- Cisco 7500 Router family, which supports a variety of LAN and WAN media including 100baseT, ATM and ISDN.
- Cisco 4700 family, which supports a variety of WAN media including Frame Relay and ISDN.
- Cisco 3600 family
- Cisco 2500 family, a fixed function Router with two high-speed ports and one LAN port.
- Cisco 1600 family of low-cost Routers with one high-speed port and a 10baseT or 10base5 connection.

All Routers use the Cisco IOS software

10.9.2 Campus LAN Switches

10.9.2.1 Campus LAN Switch

Purpose Supports high-speed LANs in Campuses and provides VLAN partitioning and sharing across Campuses.

Type Cisco Catalyst 6513 switch

Property	*Value*
Connection type	Ethernet 10baseT/100baseT
VLAN	18,19 VPN Crypt LAN
VLAN	1,2 Campus LAN
VLAN	OCMS LAN
VLAN	Tivoli Management LAN
VLAN	3,4 Host Systems LAN
VLAN	24,25 KMA LAN
VLAN	16,17 VPN Clear LAN
VLAN	FRIACO Management LAN
VLAN	Summary LAN
VLAN	Access LAN
VLAN	FRIACO LAN
VLAN	14,15 Suppliers LAN
VLAN	NBS Internal LAN
VLAN	NBS External LAN
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	BI2R	B_LAN_1
Bootle Campus	1	BI2R	B_LAN_2
Wigan Campus	1	BI2R	W_LAN_!
Wigan Campus	1	BI2R	W_LAN_2

Application	*Component*

10.9.2.2 Campus LAN Hub - 2

Purpose Access Layer Switch

Type Cisco Catalyst 2924 24-port Switch

Property	*Value*
Connection type	100baseT
Ports	24

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	B_LAN_09 (Suppliers)
Bootle Campus	1	<<<	B_LAN_10 (Suppliers)
Bootle Campus	1	<<<	B_LAN_11 (Security)
Bootle Campus	1	<<<	B_LAN_12 (Security)
Bootle Campus	4	<<<	B_LAN_13 (Security)
Bootle Campus	2	<<<	B_LAN_14 (Security)
Wigan Campus	1	<<<	W_LAN_09 (Suppliers)
Wigan Campus	1	<<<	W_LAN_10 (Suppliers)
Wigan Campus	1	<<<	W_LAN_11 (Security)
Wigan Campus	1	<<<	W_LAN_12 (Security)
Wigan Campus	4	<<<	W_LAN_13 (Security)
Wigan Campus	2	<<<	W_LAN_14 (Security)

Application	*Component*

10.9.2.3 Campus LAN Hub - 4

Purpose Logical Campus Layer hubs

Type Catalyst 5500

Property	*Value*

Connection type	100baseT

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	B_LAN_3,5,8 (Clear,
Bootle Campus	1	<<<	B_LAN_4,6,7 (Clear,
Wigan Campus	1	<<<	W_LAN_3,5,8 (Clear,
Wigan Campus	1	<<<	W_LAN_4,6,7 (Clear,

Application	*Component*

10.9.3 Campus WAN Router

Purpose Support high-speed communications between Campuses and to other sites

Type Cisco 7200 Router

Property	*Value*
Connection type	ATM
Connection type	100baseT
VLAN	18,19 VPN Crypt LAN
VLAN	1,2 Campus LAN
VLAN	OCMS LAN
VLAN	Tivoli Management LAN
VLAN	3,4 Host Systems LAN
VLAN	24,25 KMA LAN
VLAN	16,17 VPN Clear LAN
VLAN	FRIACO Management LAN
VLAN	Summary LAN
VLAN	Access LAN
VLAN	FRIACO LAN
VLAN	14,15 Suppliers LAN
VLAN	NBS Internal LAN
VLAN	NBS External LAN
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	R-B7
Bootle Campus	1	<<<	R-B8
Wigan Campus	1	<<<	R-W7
Wigan Campus	1	<<<	R-W8

Application	*Component*
Cisco IOS Software	Cisco 7200 Series IOS IP Only Feature Set

10.9.4 Logical Access Router

Purpose Provides separation of Host and Access network Layers

Type Cisco 7206 six-slot Router

Property	*Value*
Connection type	100baseT
VLAN	Summary LAN
VLAN	18,19 VPN Crypt LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	R-B12
Bootle Campus	1	<<<	R-B13
Wigan Campus	1	<<<	R-W12
Wigan Campus	1	<<<	R-W13

Application	*Component*
Build & Installation Processes	LAR Configuration
Cisco IOS Software	Cisco 7200 Series IOS IP Only Feature Set

10.9.5 Logical Campus Router

Purpose Separates Campus LAN from VPN Servers

Type Cisco 7206 Router

Property	*Value*
Connection type	100baseT
VLAN	16,17 VPN Clear LAN
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	R-B17
Bootle Campus	1	<<<	R-B18
Wigan Campus	1	<<<	R-W17
Wigan Campus	1	<<<	R-W18

Application	*Component*
Build & Installation Processes	LCR Configuration
Cisco IOS Software	Cisco 7500 Series IOS IP only Feature Set
Network Infrastructure	Cisco 13-slot 2 CyBus 1RSP2 1AC Supply

10.9.6 Campus Low Speed Router

10.9.6.1 Campus Low Speed Router - 2 (ISDN/Serial)

Purpose Central low-speed ISDN and Serial support connections to POCL HAPS and AP clients

Type Cisco 4700 Router (ISDN & Serial)

Property	*Value*
Connection type	Serial
Connection type	ISDN PRI
Connection type	100baseT
VLAN	14,15 Suppliers LAN
VLAN	12,13 Secure LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	R-B10
Wigan Campus	1	<<<	R-W10

Application	*Component*
Cisco IOS Software	Cisco 4500/4700 IOS IP Only Feature Set

10.9.6.2 Campus Low Speed Router - 3 (Serial)

Purpose Central low-speed serial support connections to CFM, SSC and Pathway

Type Cisco 4700 Router (Serial)

Property	*Value*
Connection type	Serial
Connection type	100baseT
VLAN	1,2 Campus LAN

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	R-B11
Wigan Campus	1	<<<	R-W11

Application	*Component*
Cisco IOS Software	Cisco 4500/4700 IOS IP Only Feature Set

10.9.6.3 Campus Low Speed Router - 4 (Frame Relay)

Purpose Central Frame Relay connections from non-ISDN Outlets

Type Cisco 4700 Router (Frame Relay)

Property	*Value*
Connection type	Frame Relay

Connection type	100baseT		
Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	1	<<<	R-B15
Bootle Campus	1	<<<	R-B16
Wigan Campus	1	<<<	R-W15
Wigan Campus	1	<<<	R-W16

Application	***Component***
Build & Installation Processes	Router Configuration for Data Centres
Cisco IOS Software	Cisco 4500/4700 IOS IP Feature Set

10.9.7 Campus ISDN Summarisation Router

Purpose Provides a summarisation layer for the ISDN Routers. There is one of these for every four ISDN Routers

Type Cisco 7206 Router

Property	***Value***
Connection type	100baseT
VLAN	Access LAN
VLAN	Summary LAN

Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	1	<<<	Sum_B_2
Bootle Campus	1	<<<	Sum_B_4
Bootle Campus	1	<<<	Sum_B_6
Wigan Campus	1	<<<	Sum_W_1
Wigan Campus	1	<<<	Sum_W_3
Wigan Campus	1	<<<	Sum_W_5

Application	***Component***

10.9.8 Access Server

Purpose Supports incoming calls via PSTN

Type Cisco AS5210 with 48 modems

Property	***Value***
Connection type	PSTN
Connection type	100baseT
Ports	48

Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	1	<<<	A-B1
Bootle Campus	1	<<<	A-B2
Wigan Campus	1	<<<	A-W1
Wigan Campus	1	<<<	A-W2

Application	***Component***
Cisco IOS Software	Cisco 5200 Series IOS Software

10.9.9 Gateway WAN Router

10.9.9.1 Gateway WAN Router - 1

Purpose Supports communication with Clients and Suppliers over dedicated links

Type Cisco 4700 Router

Property	***Value***
Connection type	Serial
Connection type	100baseT

Site	***Qty***	***Installed***	***Platform Name***

Pathway at Feltham	1	<<<	R-Fe1
Pathway at Feltham	1	<<<	R-Fe2
Pathway at Feltham	1	<<<	R-Fe3
Pathway Feltham Secure Area	1	<<<	
POCL Huthwaite	2	<<<	R43,R44
PON Comdisco, Isleworth	2	<<<	
SSC, Bracknell	1	<<<	R-Br1
SSC, Bracknell	1	<<<	R-Br4
SSC, Bracknell	1	<<<	R-Br5

Application	*Component*
Cisco IOS Software	Cisco 4500/4700 IOS IP Only Feature Set Cisco 5200 Series IOS Software

10.9.10 Gateway Low Speed Router

10.9.10.1 Gateway Low Speed Router - 1

Purpose Supports dedicated 2 Mbps links within ICL

Type Cisco 2501 Router

Property	*Value*
Connection type	Serial
Connection type	100baseT

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	3	<<<	
ISD Belfast Bridgeview	2	<<<	R-Be2
ISD Belfast Trident House	2	<<<	R-Be1
ISD SMC Stevenage 09	2	<<<	R-St1,2
ISD, Lytham St Annes	2	<<<	R-Ly1,2

Application	*Component*
Cisco IOS Software	Cisco 2500 IOS Enterprise Feature Set

Purpose Supports communications with Clients and Suppliers over ISDN links

Number 2

Platform

Type	Cisco 2503 (ISDN & Serial)
Connection type	ISDN BRI
Connection type	Serial
Connection Type	100baseT

10.9.10.2 Gateway Low Speed Router - 2

Purpose Supports dedicated 2 Mbps links within Fujitsu Services

Number 11

Platform

Type	Cisco 2501 Router
Connection type	Serial
Connection type	100baseT

Capsules

Cisco IOS Software	Cisco 2500 IOS Enterprise Feature Set

10.9.10.3 Gateway Low Speed Router - 3

Purpose Communication with Regional Offices

Type Cisco 1603 Router

Property	*Value*
Connection type	ISDN BRI
Connection type	100baseT

Site	*Qty*	*Installed*	*Platform Name*
Pathway Regional Office, Gloucester	1	<<<	R-Bi1
Pathway Regional Office, Hertford	1	<<<	R-Sa1
Pathway Regional Office, Tunbridge Wells	1	<<<	R-Tu1

Application	*Component*
Cisco IOS Software	Cisco 1600 IOS IP Feature Set

10.9.10.4 Gateway Low Speed Router - 4

Purpose Pathway Kidsgrove

Type Cisco 3620 2-slot Modular Router

Property	*Value*
Connection type	Serial
Connection type	ISDN PRI
Connection type	100baseT

Site	*Qty*	*Installed*	*Platform Name*
Pathway, Kidsgrove	1	<<<	R-Ki1

Application	*Component*
Cisco IOS Software	Cisco 3620 IP only

10.9.10.5 Gateway Low Speed Router - 6

Purpose Used at MAN 05 Horizon Systems Help Desk

Type Cisco 3620 Router

Property	*Value*
Connection type	100baseT

Site	*Qty*	*Installed*	*Platform Name*
ISD SMC MAN 05, Manchester	2	<<<	

Application	*Component*
Cisco IOS Software	Cisco 2600 IOS Enterprise Feature Set

10.9.11 Outlet Frame Relay Router

Purpose Installed in Frame Relay connected Outlets to support connection to the Campuses

Number 50

Platform

Type	Cisco 1601
Connection type	Frame Relay
Connection type	100baseT

Capsules

Cisco IOS Software	Cisco 1600 IOS IP Feature Set

10.9.12 WAN Encryptor

10.9.12.1 WAN Encryptor (high speed)

Purpose Support RAMBUTAN encryption on Megastream links

Type Zergo ED2000RTS encryptor

Property	*Value*
Connection type	Serial

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	10	<<<	
ISD SMC MAN 05, Manchester	2	<<<	
Pathway at Feltham	3	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.9.12.2 WAN Encryptor (low speed)

Purpose Supports RAMBUTAN encryption of Kilostream links

Type Zergo ED600RTS

Property	*Value*
Connection type	Serial

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	8	<<<	
CS Bracknell	1	<<<	
CS Bracknell	1	<<<	
ISD Belfast Bridgeview	2	<<<	
ISD Belfast Trident House	2	<<<	
ISD SMC Stevenage 09	2	<<<	
ISD, Lytham St Annes	2	<<<	
Pathway Feltham Secure Area	1	<<<	
SSC, Bracknell	2	<<<	
Wigan Campus	9	<<<	

Application	*Component*

10.9.13 Firewall Module

10.9.13.1.1 Firewall Module - 1

Purpose Provides firewall protection

Type SUN Ultra 10/300 Workstation with Firewall-1 Software

Property	*Value*
Operating System	Solaris 2.6

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	<<<	F-B1,2
Bootle Campus	2	BI3	F-B3,4
Pathway at Feltham	1	<<<	F-Fe1
Pathway Feltham Secure Area	1	<<<	
SSC, Bracknell	1	<<<	F-Br1
Wigan Campus	2	<<<	F-W1,2
Wigan Campus	2	BI3	F-W3,4

Application	*Component*
Build & Installation Processes	Firewall Module Installation Routines Firewall-1 Configuration Secure Solaris
Firewall Management Software	Checkpoint Firewall Security Software (Gateway)
Sun Solaris	NTP for Solaris (Network Time Protocol) Solaris English Media Kit
Systems Management Environment	MANSOL

10.9.13.1.2 Firewall Module - 2

Purpose DMZ Firewall

Type Cisco PIX 515UR

Property	*Value*		
Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	4	BI2R	F-B5,6
Bootle Campus	2	S30	
Test - B&TC2 Volumes & Integration Rig	2	S30	
Test - B&TC7 PET/UTC	1	S30	
Test - IPDU Development	1	S30	
Test - LST Main Rig	1	S30	
Test - REL1 Release Rig	1	S30	
Wigan Campus	4	BI2R	F-W5,6
Wigan Campus	2	S30	
Application	***Component***		

10.9.13.2 Firewall Load Balancer

Purpose Used to balance firewall traffic between the two sets of firewalls within a DMZ.

Type Cisco CSS11050

Property	*Value*		
Site	***Qty***	***Installed***	***Platform Name***
Bootle Campus	2	BI2R	
Wigan Campus	2	BI2R	
Application	***Component***		

10.9.14 LAN Hub

10.9.14.1 LAN Hub 4-port

Purpose Supports localised 10baseT Ethernet LANs

Type 3Com OfficeConnect Hub TP4

Property	*Value*		
Connection type	10baseT		
Ports	4		
Site	***Qty***	***Installed***	***Platform Name***
Four-Counter Outlets	1	<<<	
Pathway Feltham Secure Area	2	<<<	
PON Comdisco, Isleworth	2	<<<	
Three-Counter Outlets	1	<<<	
Wigan Campus	10	<<<	
Application	***Component***		

10.9.14.2 LAN Hub 8-port

Purpose Local LANs within Outlets and elsewhere

Type 3Com OfficeConnect Hub 8/TPO

Property	*Value*		
Connection type	10baseT		
Ports	8		
Site	***Qty***	***Installed***	***Platform Name***
Eight-Counter Outlets	1	<<<	
Eighteen-Counter Outlets	3	<<<	
Eleven-Counter Outlets	2	<<<	
Fifteen-Counter Outlets	3	<<<	
Five-Counter Outlets	1	<<<	

Fourteen-Counter Outlets	2	<<<	
Nine-Counter Outlets	2	<<<	
Nineteen-Counter Outlets	3	<<<	
Pathway Regional Office, Gloucester	1	<<<	
POCL Huthwaite	2	<<<	
Seven-Counter Outlets	1	<<<	
Seventeen-Counter Outlets	3	<<<	
Six-Counter Outlets	1	<<<	
Sixteen-Counter Outlets	3	<<<	
Ten-Counter Outlets	2	<<<	
Thirteen-Counter Outlets	2	<<<	
Twelve-Counter Outlets	2	<<<	
Twenty-Counter Outlets	3	<<<	

Application	*Component*

10.9.14.3 LAN Hub 12-port

Purpose LAN hub for larger sites

Type 3Com SuperStack II 12-port Hub

Property	*Value*
Connection type	10baseT
Ports	12

Site	*Qty*	*Installed*	*Platform Name*
ISD Belfast Bridgeview	1	<<<	
ISD Belfast Trident House	2	<<<	
ISD SMC MAN 05, Manchester	2	<<<	
ISD SMC Stevenage 09	2	<<<	
ISD, Lytham St Annes	2	<<<	
Pathway Regional Office, Hertford	1	<<<	
Pathway Regional Office, Tunbridge Wells	1	<<<	

Application	*Component*

10.9.14.4 LAN Hub 24-port

10.9.14.4.1 LAN Hub 24-port - 1

Purpose LAN hub for even larger sites

Type 3Com Superstack II

Property	*Value*
Connection type	10baseT
Ports	24

Site	*Qty*	*Installed*	*Platform Name*
CS Bracknell	1	<<<	
Pathway at Feltham	2	<<<	
Pathway, Kidsgrove	2	<<<	
SSC, Bracknell	6	<<<	

Application	*Component*

10.9.14.4.2 LAN Hub 24-port - 2

Purpose LAN Hub

Type Cisco 24-port Catalyst Switch

Property	*Value*
Connection type	10baseT
Ports	24

Site	*Qty*	*Installed*	*Platform Name*
ISD SMC MAN 05, Manchester	2	<<<	

Application	*Component*

10.9.15 Synchronous Multiplexor Add-Drop

10.9.15.1.1 Synchronous Multiplexor Add-drop I

Purpose Link to Energis high-speed network

Type SMA

Property	*Value*
Connection type	SDH

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.9.15.1.2 Synchronous Multiplexor Add-drop II

Purpose Energis links into Campus

Type SMA

Property	*Value*
Connection type	SDH

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.9.16 Satellite Frame Relay Router

Purpose Installed at Hughes Telecomms site at Milton Keynes

Type Cisco 3660

Property	*Value*

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.9.17 ATM Switch

Purpose Provides ATM switching and hence enables SRDF circuits to be multiplexed across the Inter-Campus ATM circuits.

Type ForeRunner ATM Switch

Property	*Value*

Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	<<<	
Wigan Campus	1	<<<	

Application	*Component*

10.9.18 Outward Call Router

Purpose Introduced at BI3 to provide a continued outward call capability to Outlets for support purposes

Type Cisco 5350 Router

Property	*Value*		
Footprint	1U		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	3	BI2R	
Wigan Campus	3	BI2R	
Application	*Component*		

10.9.19 FRIACO Feed Router

Purpose Provies access into the Horizon Campus network for Outlet traffic that is carried across he Energis FRIACO network

Type Supplied by and owned by Energis

Property	*Value*		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	BI2R	
Wigan Campus	2	BI2R	
Application	*Component*		

10.9.20 RADIUS Server

Purpose Authenticates calls delivered to the Campuses via FRIACO

Type

Property	*Value*		
VLAN	FRIACO Management LAN		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	3	BI2R	
Wigan Campus	3	BI2R	
Application	*Component*		
Build & Installation Processes	Generic NT Platform Install Routines NT Platform Fast Track Fixes		

10.9.21 Cisco Secure Router

Purpose Monitors data transfers through the LSN

Type Compaq DL360 Server

Property	*Value*		
VLAN	FRIACO Management LAN		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	1	BI2R	
Wigan Campus	1	BI2R	
Application	*Component*		

10.9.22 Cisco Syslog Router

Purpose	Logs data transfers through the LSNs
Type	Compaq DL360R01 Server

Property	*Value*		
VLAN	FRIACO Management LAN		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	BI2R	
Wigan Campus	2	BI2R	
Application	*Component*		

10.9.23 L2TP Network Server Router (LNS)

Purpose	Provides the interface between the Energis-owned FRIACO Feed Router, and the Campus LAN.
Type	Cisco 7200 Router

Property	*Value*		
VLAN	FRIACO LAN		
VLAN	Access LAN		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	12	BI2R	
Wigan Campus	12	BI2R	
Application	*Component*		

10.9.24 NBE WAN Router

Purpose	Used for communication with NBE
Type	Cisco 7206 Router

Property	*Value*		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	BI2R	
Wigan Campus	2	BI2R	
Application	*Component*		

10.9.25 DCS Access LAN Router

Purpose	Used for ISDN and X.25 communication with Streamline Merchant Services
Type	Cisco 2561

Property	*Value*		
Site	*Qty*	*Installed*	*Platform Name*
Bootle Campus	2	S30	
Test - B&TC2 Volumes & Integration Rig	2	S30	
Test - B&TC7 PET/UTC	1	S30	
Test - IPDU Development	1	S30	
Test - LST Main Rig	1	S30	
Test - REL1 Release Rig	1	S30	
Wigan Campus	2	S30	
Application	*Component*		
Network Infrastructure	Cisco 13-slot 2 CyBus 1RSP2 1AC Supply		

10.10 Client Platforms

10.10.1 VME Servers

There are no Pathway-owned VME servers. However, there is a requirement to pass data to and from VME systems owned by the DSS Benefit Agency. As this data transfer uses software supplied by Pathway, it is apposite to describe here the Platform environment on which this software runs.

10.10.1.1 ESNS VME Server

Purpose DSS mainframe supporting the OBCS(D) service. Horizon data is held in a secure area managed by VME HSO.

Type ICL SX 580

Property	*Value*
Operating System	VME with HSO

Site	*Qty*	*Installed*	*Platform Name*
DSS ACC, Washington	1	<<<	

Application	*Component*
BMC Patrol Systems Management	BMC Patrol Knowledge Module for Hytec VME FTF Proxy
OBCS DSS Application	DSS ESNS Service DSS OBCS Service OAS Common Routines OAS Controlling Procedures OAS Housekeeping OAS Installation OAS Inward File Processing OAS Outward File Processing OAS Stand Alone Utilities

10.10.2 OS/390 Servers

10.10.2.1 Network Banking Engine (NBE)

Purpose Provides an interface for Network Banking transactions and hides from Pathway the differences between the various banks.

Type IBM S/390 mainframe

Property	*Value*

Site	*Qty*	*Installed*	*Platform Name*
IBM Warwick	2	BI3	
IBM, Greenford	1	BI3	

Application	*Component*
Network Banking Service	NBE Server Application

10.11 Further Reading

Ref	Document	Title	Comments
Previous	Chapter 9	Networking Services	Describes the networking services which support the Horizon services
Next	Chapter 11	Application Development	Describes the application development and Release control processes used
CNTD	BP/DES/003	Counter Hardware Design Specification	Describes the various Counter PC specifications

LIFT	D06A-9999-B057/01	Financial Keyboard Specification	Describes the Lift keyboard used in Outlets
NUMAQ		NUMA-Q 2000 Framework Strategy	Sequent's recommended strategy for Pathway's data centre Host hardware configurations
SCO	TD/DES/048	Riposte Mirroring for Single Counter Outlets at Release 2	Describes the processes for handling the exchangeable disk in Single Counter PCs

Chapter 11 - Application Development

11.1 SCOPE

This Chapter discusses the methods used to develop Applications that are to run within the Horizon architecture, and the constraints imposed on application design and development.

A fundamental requirement of Horizon is the ability to develop new applications, and integrate them into the system, in response to new business opportunities, in a speedy and cost effective manner.

Chapter 5 "Application Architecture" describes the architecture to which any new Application must conform. This Chapter describes the way in which a new Application is justified, specified, designed, developed and released into the Live Estate. It largely reflects current custom and practice, though note that many of the processes mentioned are under review and may change in the context of a revised Contract between Pathway and PO Ltd.

11.2 APPLICATION DEVELOPMENT REFERENCE MODEL

This illustrates the components of an application development strategy.

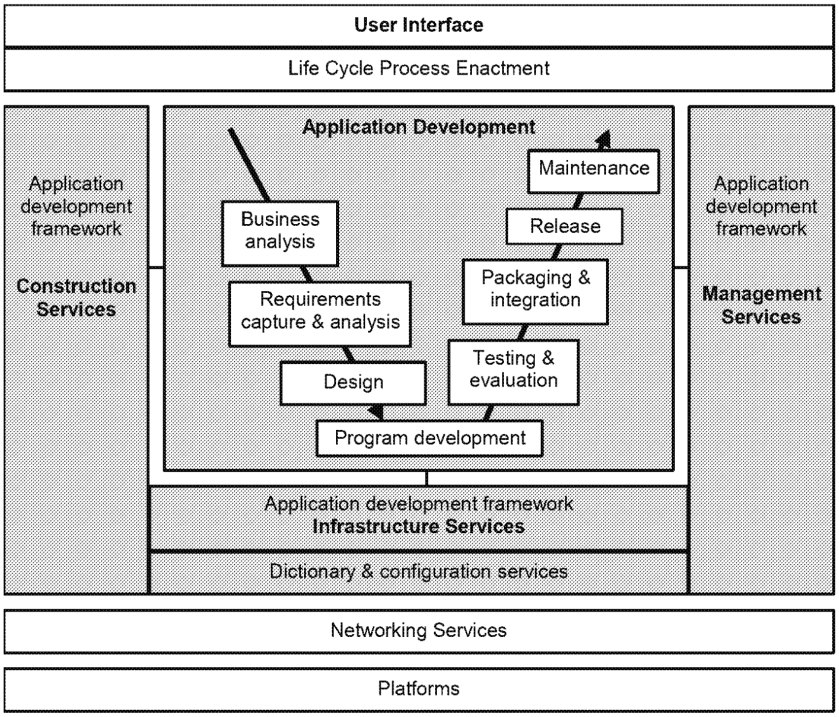

Figure 11.1 - Application Development Reference Model

11.3 APPLICATION DEVELOPMENT IN PATHWAY

This sub-section contains general rules that must be applied to all Application developments, and taken into account by all external procurements.

This diagram relates the reference model to the processes involved within Pathway. It defines a number of processes that are elaborated in subsequent sub-sections.

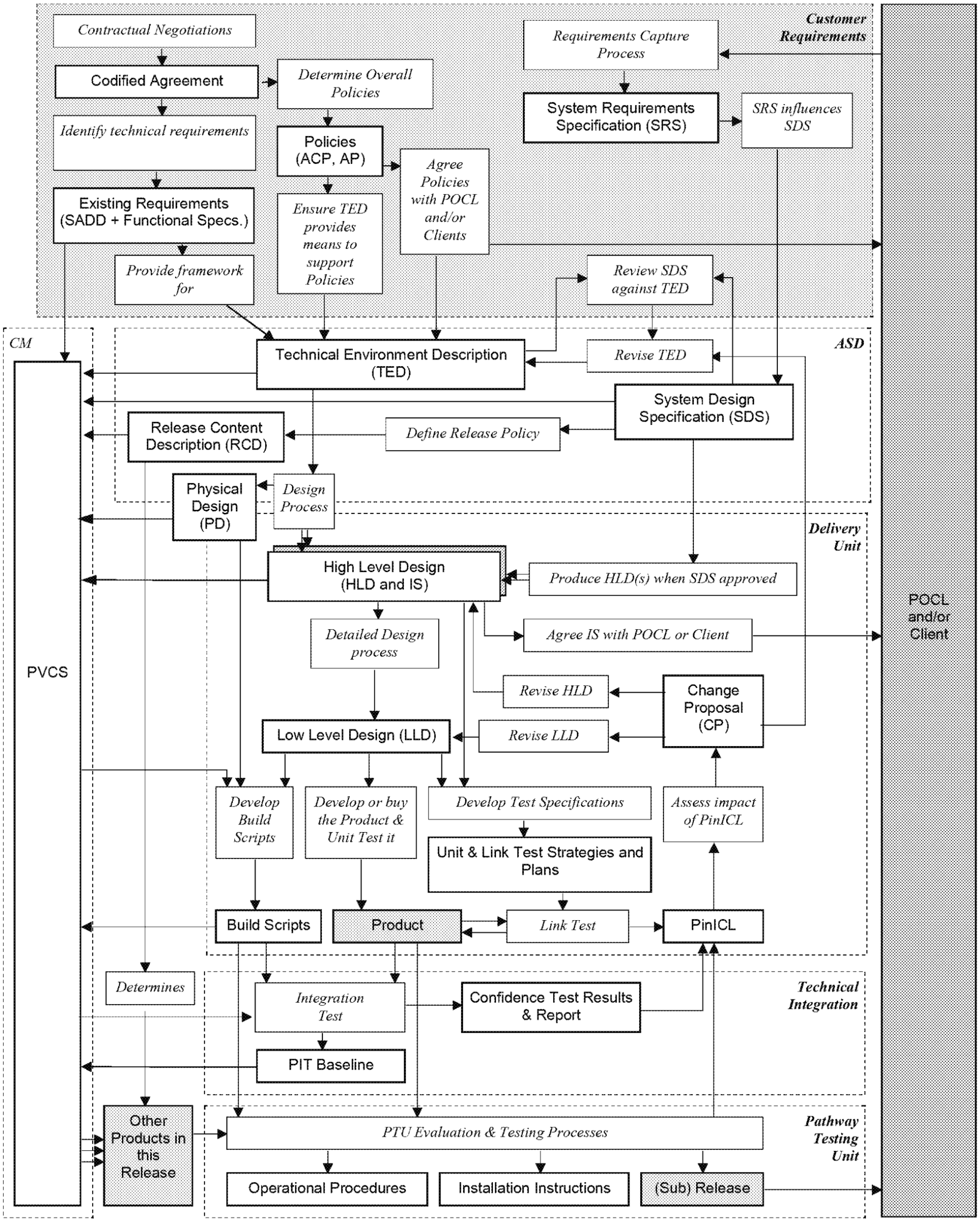
Customer Requirements
Contractual Negotiations
Codified Agreement
Determine Overall Policies
Requirements Capture Process
System Requirements Specification (SRS)
SRS influences SDS
Identify technical requirements
Policies (ACP, AP)
Agree Policies with POCL and/or Clients
Existing Requirements (SADD + Functional Specs.)
Ensure TED provides means to support Policies
Provide framework for
Review SDS against TED
CM
ASD
Technical Environment Description (TED)
Revise TED
System Design Specification (SDS)
Release Content Description (RCD)
Define Release Policy
Physical Design (PD)
Design Process
Delivery Unit
High Level Design (HLD and IS)
Produce HLD(s) when SDS approved
Detailed Design process
Agree IS with POCL or Client
PVCS
Revise HLD
Change Proposal (CP)
Low Level Design (LLD)
Revise LLD
POCL and/or Client
Develop Build Scripts
Develop or buy the Product & Unit Test it
Develop Test Specifications
Assess impact of PinICL
Unit & Link Test Strategies and Plans
Build Scripts
Product
Link Test
PinICL
Determines
Integration Test
Confidence Test Results & Report
Technical Integration
PIT Baseline
Other Products in this Release
PTU Evaluation & Testing Processes
Pathway Testing Unit
Operational Procedures
Installation Instructions
(Sub) Release

Figure 11.2 – Release Development Processes

This model has been modified in line with the recent Development Directorate organisation, but needs some further work to ensure it fully reflects the new Pathway processes..

11.4 BUSINESS ANALYSIS

There are two classes of Business Analysis: those relating to the services identified in the Contract, and those that relate to services identified subsequently.

11.4.1 Initial Customer Requirements

Most existing *Requirements* are expressed in the Codified Agreement. Many of these contained "agreements to agree" which needed to be refined and elaborated before application development could begin. This was the responsibility of the *Customer Requirements* team.

The outcome of this analysis is documented in the [SADD]. That document has contractual significance and represents an agreed definition of the services to be provided to PO Ltd and its Clients.

The Customer Requirements team is also responsible for the development of a set of *policies* which determine the way in which the services is to be provides. These cover areas such as Access Control and Audit.

11.4.2 New Business Development

Further requirements arise from new business opportunities identified by PO Ltd. These are negotiated with Pathway in a framework constrained by the time taken to carry out the development, and its costs. They may require changes to the the existing Horizon architecture. Any potential change to the system, or any requirement for a new application, need to be measured against the existing architecture.

A number of techniques are used to make it simple and speedy to introduce new generic Applications. As an example, it is feasible to introduce a new APS Client solely by use of Reference Data. Similarly, it is feasible to introduce new EPOSS products by the use of Reference Data, especially where the product is bar coded. There is no need to introduce menu buttons for bar coded products, and this considerably simplifies the Counter Application design.

11.5 REQUIREMENTS CAPTURE & ANALYSIS

Both the Contract and the [SADD] are text-based documents, as are a number of requirements documents derived from these (e.g. the [ATFS]). Similarly, requirements articulated by PO Ltd are captured by Pathway in a *System Requirement Specification* (SRS).

11.5.1 System Design Specification

Requirements documented in an SRS need to be assessed in terms of their impact on the existing system. The first stage is the development, by or for ASD, of a *System Design Specification* (SDS) for the development. The SDS reflects the business needs for the development, and its agreed requirements. It establishes the fit of the development with the existing architecture, or identifies areas where the architecture will need to be extended. It provides sufficient information to enable Pathway management to develop a rough outline of its costs and business return.

11.6 APPLICATION DESIGN

11.6.1 High Level Design

An application *High Level Design* (HLD) is produced once it is decided to undertake the development. It takes the development process a stage further and specifies the development's components, where these are sourced from, and any special development or configuration needs.

11.6.1.1 Interface Specifications

Where the development requires an interaction with PO Ltd or a PO Ltd Client, it is also necessary to develop a *Technical* or *Application Interface Specification* (TIS or AIS). This defines the nature of the external interface, the Platforms required to support it, and the file transfer formats and volumes. This document must be agreed with the appropriate Client.

11.6.1.2 Low Level Design

Following on from this is the *Low Level Design Process*, carried out by the Delivery Unit, which culminates in the production of the necessary *Low Level Design* (LLD) documents.

Chapter 5 "Application Architectures" describes the structure of any new application. A new application includes components running on a number of different Platforms, using different design paradigms and different design tools. In addition, a number of design issues need to be taken into account in any new application.

11.6.1.3 Platform Design

Design processes may thus also require changes to the *Platform Physical Designs* that describe the nature of each Platform and the Capsules that run on it.

11.6.2 External Interface Design

Wherever possible the interface to an external body is via serial files that are transferred via the FTMS. This is described in Chapter 5 "Application Architecture". Design work involves identifying the files to be transferred in which direction, their contents and formats, integrity requirements (e.g. whether digital signing is required) and others. Most of this information is used to configure the FTMS instance used for the application.

11.6.3 Host Application Design

A set of detailed application and database design standards are given in [HADDIS]. Those that are specific to the use of Oracle databases are summarised in Chapter 7 "Information Management". The more general design standards are summarised in this sub-section.

11.6.3.1 Object Orientation

Applications must be designed to be self-contained, and only communicate via pre-defined, documented interfaces that are not dependent on the application's physical implementation.

11.6.3.2 Scheduling

Maestro is Horizon's strategic job scheduler. All applications that run as discrete batch jobs should be written in such a way that they are compatible with the requirements of Maestro.

11.6.3.3 Defensive Programming

Database applications should be designed and built defensively, so that they can handle any type of unexpected conditions in a controlled manner. Unexpected conditions include:

- Invalid data which has been erroneously input into the database
- Logical inconsistencies between database objects
- Error responses to valid DML requests

All SQL statements must be coded on the assumption that they may fail. Any such exception condition should be logged to the Module's exception table. If it is deemed serious enough, the application should roll back all uncommitted updates (*before* logging the exception) and exit gracefully.

11.6.3.4 Archiving

Archiving is a term used here to cover the hiving off to a different storage medium of data that no longer needs to be held in an immediately accessible form. It thus covers the removal of historical data from a database to off-line storage such as magnetic tape or optical disk.

Each application is responsible for defining its own archiving strategy, which in effect amounts to specifying the tables that are to be archived. These must include:

- The audit related tables discussed above
- Tables representing data transferred to and from the Agent Layer, represented by the Client Interface Tables application component in Chapter 5 "Application Architectures", which are required for contractual reasons.

Standards for database archiving are given in [HADDIS].

11.6.3.5 Handling of Reference Data

Host applications, like Counter applications, can be closely controlled by the use of Reference Data. This is usually contained within the application's own schema in tables which contain a relatively small number of rows.

Any such data must be delivered to the application via the Reference Data Management System (RDMS) which ensure that it has been properly validated and properly released. It also ensures that changes to Reference Data are co-ordinated with similar changes to other applications.

11.6.3.6 Backup and Recovery

All data used by Host applications must be regularly backed up so that there is no realistic possibility of data ever being lost should a media or system failure occur.

11.6.3.7 Consistency Checking

Applications should provide facilities to enable the logical and physical consistency of their data to be checked, and these facilities should be run on a regular basis.

11.6.4 Agent Design

Chapter 5 "Application Architectures" defines the various types of Agent applications, and the interfaces that they use. New Agents need to be designed to fit into this context.

Key constraints are:

- Support transactional integrity, where possible. Riposte does not always make this possible, and hence Agents must be designed that Riposte messages will never be lost but may be duplicated.
- Support multi-threading, to optimise the use of the limited number of Agent Servers.

11.6.5 Counter Application Design

The construction of Counter applications is also covered by Chapter 5 "Application Architectures". Key issues include the following.

- Conformance to the Horizon Style Guide ([STYLE]), and its hierarchy of Menus and Buttons.
- Use of Reference Data

11.6.6 General Design Issues

A number of design considerations need to be applied to all application layers. They apply particularly to Third party products, which may be procured for purposes not covered by any of the above.

11.7 APPLICATION CONSTRUCTION

Construction is a loose term, and covers everything from writing code to procuring a large Sequent server.

Different tools and test facilities are used for different components of the application architecture.

11.7.1 Host Application Construction

All Host applications are based on Oracle.

11.7.1.1 Schema Design

Oracle Developer 2000 is used to develop Oracle applications.

11.7.1.2 Programming Languages

C++ is the language of choice for Host applications, with the Pro*C extensions to C++ forming the interface to Oracle. The choice of C++ is because:

- It is a mature language which is reliable and widely known
- It provides the best performance for interfacing with Oracle, as well as with most other RDBMSs
- It is used elsewhere in the system

C++ is used for the KMS application.

11.7.2 Agent Application Construction

These are developed for Pathway by A&TC Enterprise Solutions, and are generally written in C. Agents have access to the Riposte APIs, and to a number of libraries that help to simplify the developed code.

11.7.3 Counter Application Construction

11.7.3.1 Riposte

Riposte is in general a "soft" development environment, in which applications are primarily driven by messages stored in the Counter's persistent store. Escher provide a toolkit which may be used to prototype these applications and subsequently to integrate them into the Counter desktop. Facilities are provided within this to define Impulses, and the actions to be taken when they occur, and a number of other such features.

Riposte is a full 32-bit application environment making extensive use of Microsoft's ActiveX technology.

Riposte Help information is held as Internet-type HTTP files, and displayed by Internet Explorer.

11.7.3.2 Visual Basic

Applications that form part of the Riposte Desktop are developed using Visual Basic. They have access to the Riposte functions that are implemented as OCXs. Applications are designed using object-oriented techniques. Standard mechanisms are defined for handling menus, icons and Buttons.

Both NBS and DCS are developed using methods derived from Escher's Financial Transaction Framework. This consists of a core component, with the bulk of the application logic defined by "scripts" that are held in Reference Data. The scripts call application components that are developed using VB.

The vast majority of Pathway platforms use the VB 5 runtime libraries. The exception is the Operational Change Management System server. This uses VB 6 runtime.

11.7.3.3 C

Counter Agents, like Agent Layer Agents, are written in *C*.

11.7.4 Third Party Products

11.7.4.1 Selection and Upgrade of Commodity Products

Horizon makes significant use of third party *Commodity Products* where appropriate. These range from platform operating systems to specific applications. Any such product needs to be procured and used according to the following guidelines.

- It should be installed on the minimum number of platforms needed to carry out its required functions
- Where the product is licences or can be configured in a number of different ways, the minimum configuration or lowest-cost variant able to meet the required functions should be used
- When a product ceases to be of use on a particular platform (for example because the platform itself is retired), consideration should be given to moving the licence to another platform
- Where sensible, licences used for test rigs should be transferred to live platforms when no longer needed in test
- Products should be upgraded at suitable intervals, according to the programme's Commodity Software Upgrade Strategy, to ensure that wherever possible the versions used are supported by their suppliers and will continue to be supported for a reasonable period

11.7.4.2 Commodity Products Used

Some third party products (e.g. Dynix, NT) are described and listed at appropriate points in other Chapters of this Document. Those that are not described elsewhere are as follows.

11.7.4.2.1 ADAP - Adaptec Drivers

Notes Various drivers supplied by Adaptec
Supplier Adaptec

Component	Platforms
Adaptec 2944UW Firmware BIOS Upgrade Adaptec AHA-2940 Ultra PCI Adapter Adaptec EasyCD Creator Deluxe Edition	Correspondence Server KMA Workstation Audit Workstation SSC Support Workstation
Adaptec SCSI Driver for 7800 family	Correspondence Server Horizon Help Desk Gateway - Local

11.7.4.2.2 CISCO - Cisco IOS Software

Notes Contains the Cisco IOS components installed on Routers and other network components
Supplier Cisco

Component	Platforms
Cisco 1600 IOS IP Feature Set	Gateway Low Speed Router - 3
Cisco 2500 IOS Enterprise Feature Set	Gateway Low Speed Router - 2
Cisco 2600 IOS Enterprise Feature Set	Gateway Low Speed Router - 6
Cisco 3620 IP only	Gateway Low Speed Router - 4
Cisco 4500/4700 IOS IP Feature Set	Campus Low Speed Router - 4 (Frame Relay)
Cisco 4500/4700 IOS IP Only Feature Set	Campus Low Speed Router - 2 (ISDN/Serial)
	Campus Low Speed Router - 3 (Serial)
	Gateway WAN Router - 1
	Gateway WAN Router - 2

Cisco 5200 Series IOS Software	Access Server Gateway WAN Router - 1
Cisco 7200 Series IOS IP Only Feature Set	Campus WAN Router Logical Access Router
Cisco 7500 Series IOS IP only Feature Set	Logical Campus Router

11.7.4.2.3 EICON - Eicon Driver Software

Notes Driver software used for Eicon ISDN cards

Supplier Eicon

Component	**Platforms**
Eicon C23 PSTN Modem	Boot Server Engineer's Day D Laptop
Eicon Client ISDN Driver	AP Client Gateway - Remote Boot Server Counter PC General Purpose FTMS Gateway - Remote
Eicon Diehl S2M ISDN Driver	Boot Server
Eicon DIVA Client for Windows NT4.0	General Purpose FTMS Gateway - Remote
Eicon ISDN DIVA Basic Rate Card	Counter PC General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Remote
Eicon PCMCIA ISDN Xircom 56 Kb Card	Engineer's Day D Laptop
Eicon S2M Diva Server PRI PCI 0M	Boot Server

11.7.4.2.4 EMC - EMC Disk Array Driver Software

Notes Drivers used to manage EMC Disk Arrays

Supplier EMC

Component	**Platforms**
EMC Disk Storage Management System for NT	Audit Server
EMC Symmetrix Manager	Host Central Server
EMC Symmetrix manager Control Utilities	DCS Agent Server DCS Management Server KMA Server
Remote Data Facility Software Licence	Host Central Server
Symmetrix Manager Base Component Software Licence	Host Central Server
Symmetrix Manager SRDF Facility Host S/W Licence	Host Central Server
Symmetrix SymmManager	Data Warehouse Server
Symmetrix TimeFinder	Data Warehouse Server SMDB Server

11.7.4.2.5 EUR - Europa Test Facilities

Notes Software used on the Counter PCs to carry out a hardware test on installation

Supplier Europa

Component	**Platforms**
Europa Installation Test Utilities	Counter PC

11.7.4.2.6 HB - Hummingbird Communications Software

Notes NFS Software

Supplier Hummingbird

Component	**Platforms**
Hummingbird NBS Maestro Solo	(all FTMS platforms)
eXceed Xclient Software	SSC Support Workstation

11.7.4.2.7 JAZ - IomegaWare Jaz Drive Software

Notes

Supplier Iomega

Component	**Platforms**

IomegaWare Jaz Drive Software	CA Workstation KMA Workstation

11.7.4.2.8 LEG - Legato Application and Driver Software

Notes DLT Tape driver and management facilities

Supplier Legato

Component	**Platforms**
DLT7000 Drivers for Windows Intel Platforms	Audit Server Audit Workstation SMDB Server
Legato Networker ClientPak for Windows NT	KMA Server

11.7.4.2.9 LM - Proxima LogManagerKM

Notes

Supplier Proxima

Component	**Platforms**
LogManage KM	Host Central Server

11.7.4.2.10 MTO - Microtouch Screen Driver

Notes

Supplier Microtouch

Component	**Platforms**
Microtouch Screen Driver	Counter PC

11.7.4.2.11 ODBC - Microsoft Open Database Connectivity

Notes

Supplier Microsoft

Component	**Platforms**
Microsoft Open Database Connectivity (ODBC) Driver	ACDB Client Workstation Audit Server CA Workstation DCS Management Server KMS Admin Workstation OCMS Client OCMS Server RDMC Administrator Workstation

11.7.4.2.12 PKZIP

Notes File Compression software. Could be replaced by WINZIP.

Supplier PKWare Inc

Component	**Platforms**
PKZIP	CA Workstation

11.7.4.2.13 QNG - QNG Device Drivers

Notes Drivers for Random Number Generators

Supplier ComScire

Component	**Platforms**
QNG Device Driver	CA Workstation KMA Server KMA Workstation Offline Key Generation Workstation

11.7.4.2.14 RL - Retail Logic SOLVE/SE

Notes

Supplier Retail Logic

Component	**Platforms**
Solve/PFG Payment File Generation for NT	DCS Management Server
Solve/SE Client for Windows NT	DCS Agent Server
Solve/SE de option for NT	DCS Agent Server
Solve/SE dt option for NT	DCS Agent Server
Solve/SE Host Application	DCS Agent Server
Solve/SE SPF Edit Utility	DCS Management Server

11.7.4.2.15 SONNET - Hytec Sonnet Support Software

Notes

Supplier Hytec

Component	**Platforms**
BMC Patrol Knowledge Module for Hytec FTF	Host Central Server
Hytec Sonnet with ADI, FTF	Host Central Server

11.7.4.2.16 SPEC - Specialix

Notes Multi-port Serial Driver software for Counters

Supplier Specialix

Component	**Platforms**
Specialix Driver Software (installation disk image)	Counter PC PIN Pad Key Generation Workstation PIN Pad Proving Workstation

11.7.4.2.17 SYSI - SysInternals BlueSave Support Software

Notes Captures data generated by a "BlueScreen of Death" (BSOD) and formats it for transmission to the Campus

Supplier SysInternals

Component	**Platforms**
Winternals Software BlueSave for Windows NT4.0	Counter PC

11.7.4.2.18 TWC - TeamWARE Crypto

Notes Used on Counter PCs to encrypt the Counter filestore. No longer supported by Fujitsu, and support is provided solely within Pathway.

Supplier Fujitsu Siemens

Component	**Platforms**
TeamWARE Crypto (TWC)	CA Workstation Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation Support Support Access Server

11.7.4.2.19 TXP - TextPad

Notes

Supplier Software Solutions

Component	**Platforms**
TextPad	Short-term Performance Database Server SSC Support Workstation

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

11.7.4.2.20 VS - Microsoft Visual Studio

Notes

Supplier Microsoft

Component	**Platforms**
Microsoft VB Runtime DLLs	ACDB Client Workstation ACDB Server Audit Server Counter PC DCS Agent Server DCS Agent Server DCS Management Server KMA Workstation OCMS Client OCMS Server Tivoli Support Workstation
Microsoft Visual Basic Microsoft Visual C++ Runtime DLLs	SSC Support Workstation CA Workstation Counter PC Outsourcing Software Depot Tivoli Support Workstation VPN Exception Server VPN Policy File Management Server
Microsoft Visual Studio Runtime	KMA Server KMA Workstation KMS Admin Workstation

11.7.4.2.21 WINZIP

Notes Visual application for compressing and expanding files

Supplier WinZip

Component	**Platforms**
WinZip	Audit Server Audit Workstation MIS Client Workstation MIS Support Workstation RDMC Administrator Workstation Short-term Performance Database Server SSC Support Server SSC Support Workstation

11.8 PRODUCT TESTING & EVALUATION

Unit Testing takes place once the product is developed or procured, and ensures that the product conforms to its functional and other requirements. It is carried out by the Delivery Unit. Any problems encountered during testing are documented in PinICLs, which are passed to the affected Department. PinICLs may give rise to a *Change Proposal* (CP) to any or all of the TED, the HLD or the *Low Level Design* (LLD).

Link Testing verifies that the product interworks with other major components.

11.9 TECHNICAL INTEGRATION

This sub-section discusses the ways in which developments are aggregated and integrated to form systems that can be released into live use to meet the Pathway contractual requirements.

11.9.1 Product Breakdown Structure

The formal name for this analysis is the *Product Breakdown Structure*, and it relates to project assembly life cycles from handover to activation in a live system.

Integration involves testing the product with other products with which it needs to interwork, and proving that it operates within the Horizon infrastructure. In general, integration applies to a complete Release. Problems identified at this stage are also documented as PinICLs.

11.9.2 The Approach to Technical Integration

Horizon contains many physical products and combinations of products Configuration management of these is based on identifying, recording, and capturing (for later recovery and use) each version or variant of:

- products delivered into and used within the project, whether used directly in the live operational system or not
- the main sub-components of these products, where the sub-components will be used on different Platforms, in different Builds, or for different purposes such as different Build, integration, test and operational phases. In line with OPEN*framework* standards, these are described in this Document as *Capsules*
- defined combinations of instances of these Capsules, known hereinafter as Builds

This basic product information is complemented by identifying, recording, and capturing (for later recovery and use):

- information about how the product is configured for use
- the configuration operations (if any) required to activate each Capsule
- supporting product related data
- a range of dependency information
- a range of usage information.

Assembly operations are carried out in an order determined by the product inter-dependencies.

This model is also based upon identification methods for:

- products and Capsules
- logical Platforms
- logical sites (e.g. Outlets, Campuses, Support Sites)
- operational Platform types (e.g. all the particular instances of a given logical Platform)
- operational sites (e.g. all Outlets, all Campuses)
- Builds
- Releases (BI2, S20, BI3)

11.9.3 Basic model

The basic model adopted at this stage is as follows.

- Define a self-consistent set of Capsule versions (and if necessary variants) which comprise each *product stream*
- Define the Capsules which constitute each *working Build*
- Define the clean Builds which constitute each *Release*

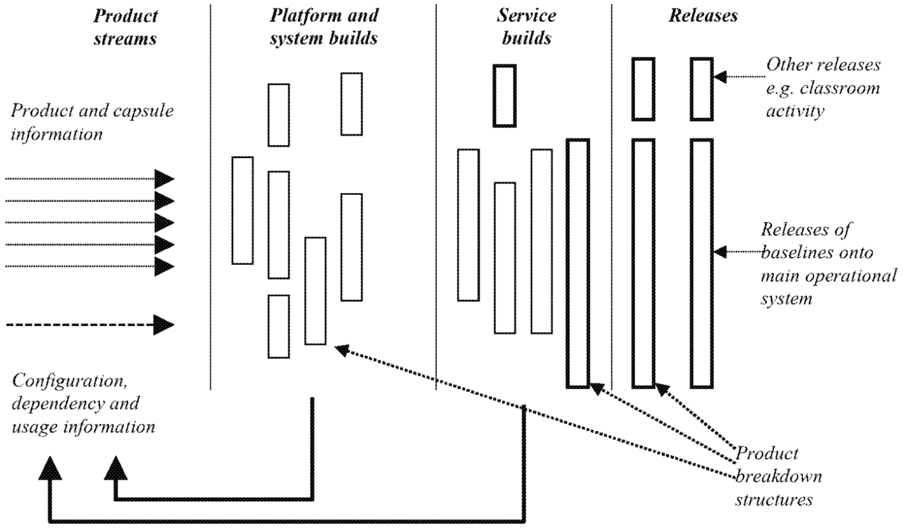
Product streams
Platform and system builds
Service builds
Releases
Product and capsule information
Other releases e.g. classroom activity
Releases of baselines onto main operational system
Configuration, dependency and usage information
Product breakdown structures

Figure 11.3 - Basic model

The terminology used in this Diagram follows that of OPENframework, and Chapter 10, but not necessarily that used elsewhere in Pathway at present.

This representation is simplified, so does not include detail such as fast track routes for high priority fixes, nor pre-release testing of operational fixes.

Heavy outlining is used to indicate major baselines although many earlier Builds will also in general be Baselined for operational benefit.

11.9.4 Product Version Management

Product deliverable version management and variant management are based on:

- Capsules
- operations carried out on Capsules
- configuration information for those operations (Build scripts, installation scripts, configuration files)
- dependency information

11.9.4.1 Capsules

A Capsule is the indivisible Build object for assembling and managing a Platform Build. Typically, it consists of a set of configuration items (such as individual files, or hardware components). These are linked. If one is present on a particular Platform Build, then the others will necessarily be present. The Capsule has a defined structure (directory structure in the case of software, physical positioning in the case of hardware). In the case of software, the target structure is defined relative to a defined target location. The handover documentation defines whether the target location is fixed or can be varied (e.g. for performance purposes). A Capsule will have other items associated with it including, but not exclusively, handover notes, dependencies, supporting documentation.

In many cases, a product consists of a single Capsule.

Capsules have both *versions* and *variants*. A version is one of a sequence of instances of the product along a single track.

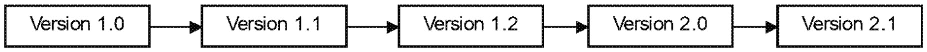

Figure 11.4 - Version Management

Variants is the term used to describe the situation where two or more different forms of the product exist in parallel, depending for example on the Platform they run on.

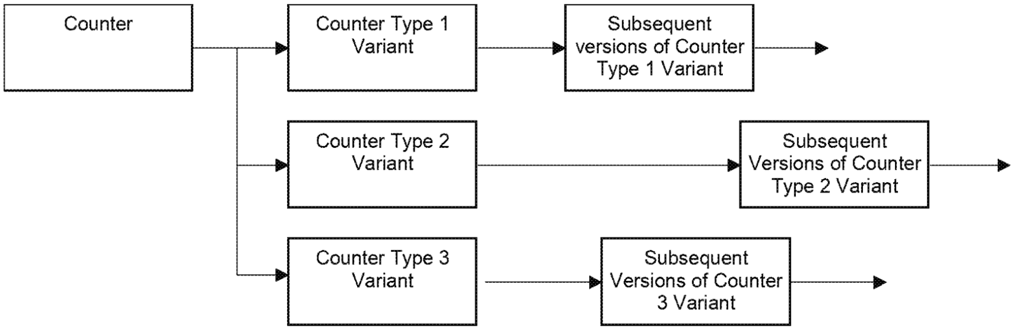
Counter
Counter Type 1 Variant
Subsequent versions of Counter Type 1 Variant
Counter Type 2 Variant
Subsequent Versions of Counter Type 2 Variant
Counter Type 3 Variant
Subsequent Versions of Counter 3 Variant

Figure 11 5 - Variant Management

Capsules are defined by agreement between Design and Development, and are documented in Chapter 10 “Platforms”.

Any operations or activities carried out on a Capsule must reference all its dependencies on software tools, and reference any supporting configuration information required. For example, NT services have to be registered.

11.9.4.2 Capsule Usage Management

Each Build is in effect a derived Product Breakdown Structure. Configuration management processes support recording and retrieving of both forecast and actual Capsule usage by Platform, Build and Release.

Upgrades and fixes to Capsules can be delivered as full handovers or as increments. Auto-installing increments must check that the requisite previous version is already present.

11.9.4.3 Dependency Management

Release management and migration between Releases depend on managing dependencies and dependency conflicts. Facilities are provided to record and retrieve both forecast and actual:

- dependencies between products
- dependencies between Capsules
- dependencies on operations and activities associated with a Capsule, including sequencing
- dependencies between Builds in terms of their Capsules
- PinICL dependencies on specific Capsule versions.

Each dependency is associated with a version (or a range of versions) of a dependent product Capsule and a range of versions of the product depended on.

11.9.4.4 Build Management

Four types of *Build* are required.

- Single Platform Build
- Mmultiple Platform (system) Build
- Service Build
- Release

Single and Multiple Platform Builds are combinations of specific versions of Capsules as required for integration and test, but are not necessarily "complete", and may include diagnostic tools and test stubs.

A Platform Build consists of Capsules and other subordinate Platform Builds that combine on a specific Platform. Multiple Platform Builds extend these to cover more than one Platform, and include inter-Platform interfacing constraints and information.

So for example a single Platform test cell typically contains several Platform Builds - a stable base Build (for example the Celestica cold Build), an application Build, an upgrade and fix Build, and baseline operational data.

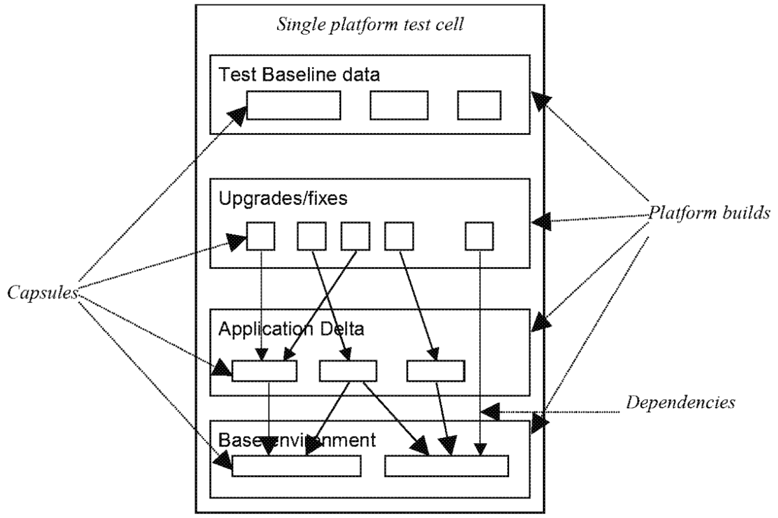

Figure 11.6 - Platform Build

A multi-Platform test cell typically contains a combination of Platform and system Builds.

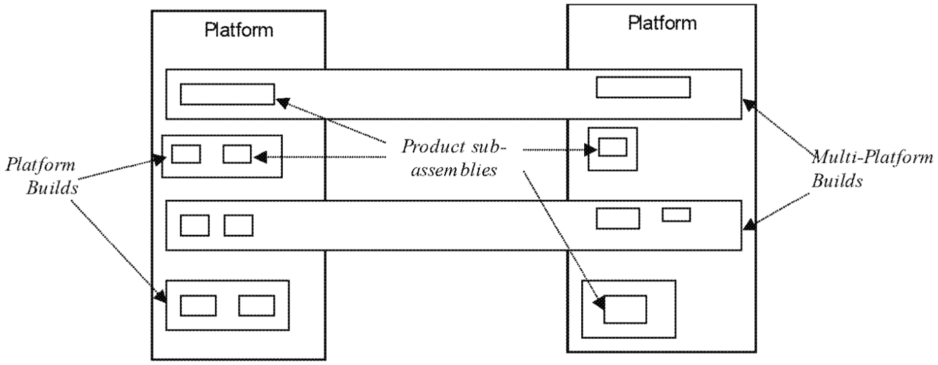

Figure 11.7 - Multiple Platform Build

Service Builds are clean (i.e. contain no diagnostic facilities or test stubs) and defined combinations of Capsules that mimic the live environment as closely as possible. Examples include the model office, CS Reference Builds and Integration Test Builds.

11.9.4.5 Build and Integration Components

The Build & Integration phase contributes to the component breakdown of each Platform, as follows.

Component	Platforms
Platform Installation Routines	*Platform*
Generic NT Platform Install Routines	*All NT Platforms*
NT Common File Set	*All NT Platforms*
NT Platform Fast Track Fixes	*All NT Platforms*
NT Secure Build	*All NT Platforms*
Secure Sequent Build	Data Warehouse Server Host Central Server
Secure Solaris	Firewall Management Server Firewall Module - 1 Network Management Server SecurID ACE Server

11.9.4.6 Acceptance Testing

Acceptance Testing takes place on a Service Build, and proves to the sponsoring Client that the development meets his functional requirements, and to PO Ltd that it may be brought into use without impacting on the existing solution or other applications.

11.10 RELEASE MANAGEMENT

11.10.1 Nature of a Release

A Release forms the culmination of the Build and integration process, and is the vehicle for many deliverables that will have consumed considerable Pathway management time.

A Release is a special case of a service Build. It is authorised for delivery on to the live operational system, and thus warrants special integration testing and will usually require Customer approval.

A Release is a derived complete (major Release) or incremental set (fix) of specific versions of interdependent sub-assemblies, together with the migration operations and dependencies that need to be considered when it is introduced to the live systems. These include issues such as sequencing the update of client and server pairs.

11.10.2 Contents of a Release

A Release can contain any combination of the following:

- New applications in response to requirements processed through the New Service Introduction process
- Changes to existing system functionality identified and authorised via the Change Control process
- Pathway business requirements, including system re-engineering activities where SLA limits are threatened or penalties are being paid
- Reference Data changes where the change requires corresponding code changes and/or materially affects the operation of the live systems.
- Changes to the Horizon infrastructure

11.10.2.1 Release Contents Definition

A Release is defined by a *Release Contents Description* (RCD) which lists what is to be delivered and any relevant exclusions. The origin of this is the [TED], as it is crucial that a Release contains an architecturally consistent set of products or product upgrades. The RCD identifies a set of documents that define the scope of the Release, and that set is then placed under Change Control.

The content of each Release must reflect business realities. Constraints may include the following.

- Time to deliver the Release is finite, and may not be improved by the use of additional resources because of the additional management complexity that this introduces
- Functionality may be needed by PO Ltd at pre-defined times for business reasons
- There must be a viable migration path to the Release
- Pathway may want to re-engineer aspects of the system that are showing high cost of ownership.

11.11 LOGICAL PRODUCT BREAKDOWN STRUCTURE

The following diagram brings together all the components of the Application Development process, and shows the major attributes of each. It summarises the descriptions in the previous sub-sections. Each component identified in this diagram is a different object type recorded in PVCS. The information associated with each object type is defined in [PBS].

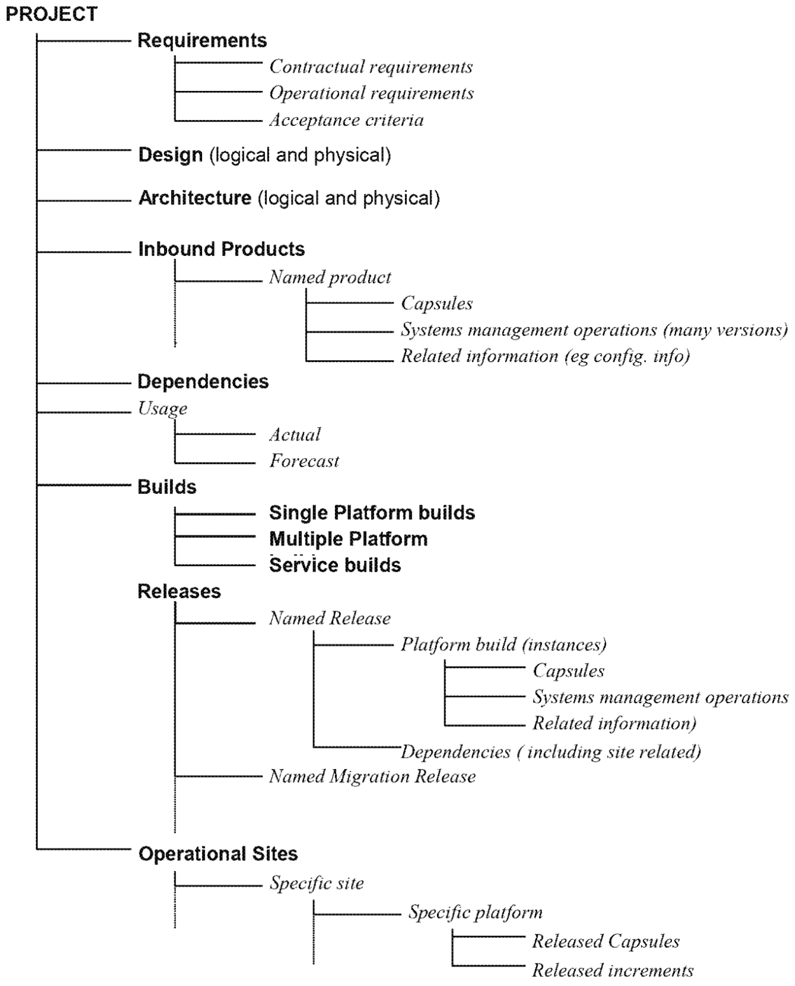

Figure 11.8 - Product Breakdown Structure

This structure is somewhat out of date, and does not fully reflect the full set of entities that are handled in Pathway. In particular, it does not fully model the ”front end” of the develoment process, and the architectural entites described in this Document. A more appropriate Product Breakdown Structure would include the entities shown here.

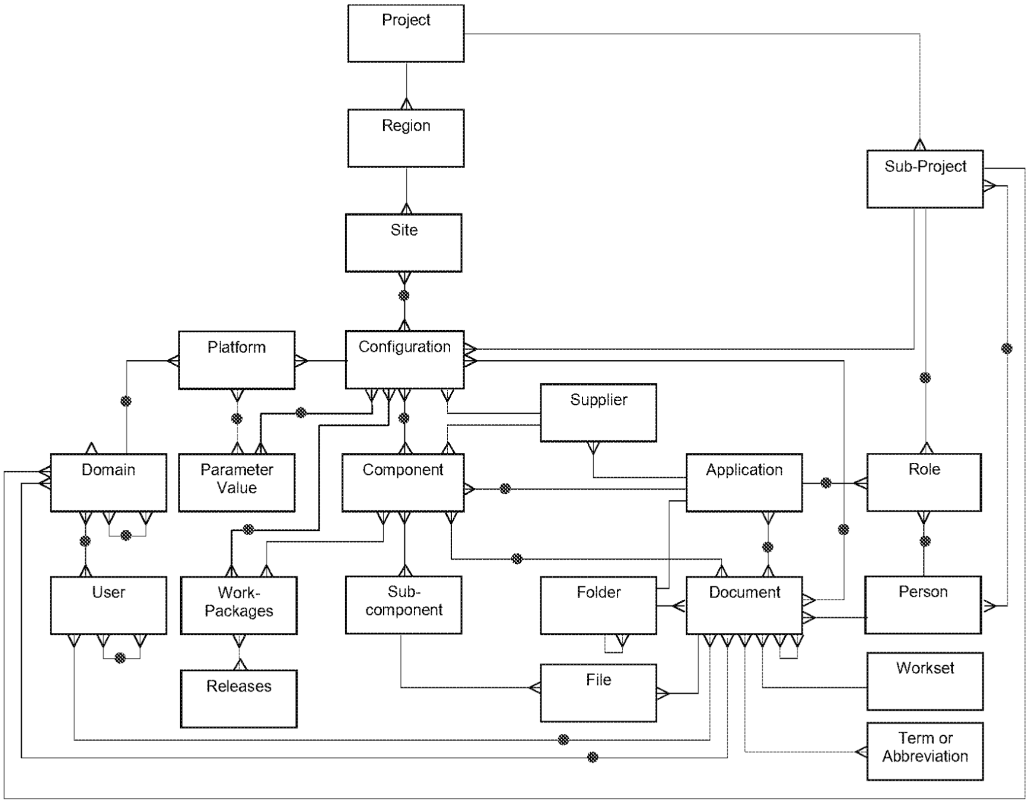

Figure 11.9 – Proposed PBS Entity Model

11.12 Further Reading

Ref	Document	Title	Comments
Previous	Chapter 10	Platforms	Describes the various Platform types used to support the Horizon services
Next	Chapter 12	Systems Management	Describes the Systems Management facilities
HADDIS	TD/STD/001	Host Application Database Design and Interface Standards	Defines the standards for the development of Host applications. (There are no similar documents as yet for other levels of the application architecture.)
OLS		Pathway On-Line Standards	Many of the processes documented in this Chapter are described (in more detail) in the *Pathway On-Line Standards*, a set of Windows Help Files available to all members of the Project.
PBS	SD/DES/001	Product Breakdown Structure Meta-Model	Defines the Product Breakdown Structure and elaborates on Figure 11.8

Chapter 12 - Systems Management

12.1 SCOPE

This Chapter describes the Systems Management facilities used in Pathway. It covers the following topics.

- The services that are required
- The Platforms that constitute the managed Pathway estate
- The product architecture(s) that deliver the management services
- The ways in which these services are used by the Service Providers
- The use of the Platforms that provide systems management services
- The impact of these facilities on Application designers

12.2 SYSTEMS MANAGEMENT REFERENCE MODEL

Systems management facilities and services enable service providers to manage complex multi-vendor business systems. Systems management tools and infrastructure help service providers to deliver the required IT services to users in accordance with service level agreements. Systems management applications manage the resources within the system. These range from the basic system infrastructure (network components, computers, operating systems, Filestores and others) to the applications that provide the services required by end users.

Systems Management applications provide the means of monitoring and managing a set of *Managed Objects* that ideally comprise all the system platforms. The managed objects include a set of *resources*. Usually, the management architecture requires the use of specific *sponsors* and *agents*, running on the Platform, to enable it to be managed.

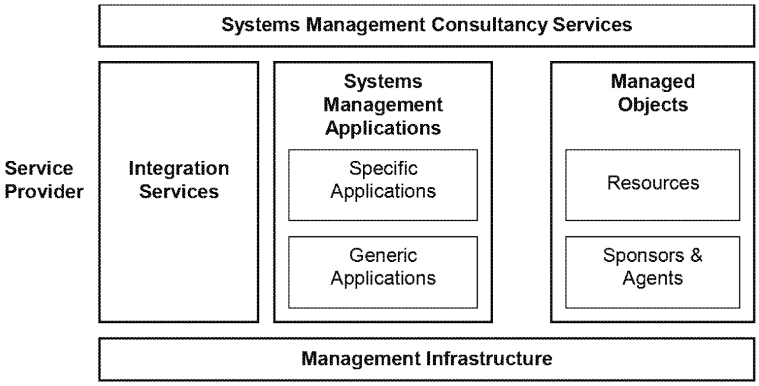

Figure 12.1 - Systems Management Reference Model

The systems management architecture requires a *Management Infrastructure* that provides a set of key enabling processes.

12.3 Business Issues

Pathway uses Systems Management facilities to maximise the availability of the contracted service to PO Ltd, and to monitor and ensure that it meets the contractual *Service Level Agreements* (SLAs). Investment in Systems Management facilities reduces service delivery costs in the following ways.

- Reducing the need for human intervention, e.g. visits to Outlets to install software
- Increased commonality between services provided on different systems
- Automating routine management activities, thus reducing the need for human operators
- Enabling problems to be anticipated and avoided, or their impact reduced
- Identifying the most cost-effective strategy for hardware upgrades or replacement
- Meeting contractual requirements for audit of security events

Management and operation of Horizon is contracted to Fujitsu Core Services (FCS), who are responsible for the choice of management tools. Pathway's involvement has been to ensure that they are fit for purpose and provide the necessary scalability. Pathway is also involved in the design of the use of the management tools.

12.4 Platforms Requiring Management

Chapter 10 "Platforms" discusses the Platform technology used, and Chapter 9 "Networking Services" the network structure that links these Platforms together. Platforms can be grouped together into a *Platform taxonomy*, where the hardware or software nature of the components effectively mandates a certain set of management tools and functions. These groupings are shown below.

Chapter 10 includes a number of *Client Platforms*, such as the DSS VME system running the ESNS application, that are not managed by Pathway, though some functions carried out there are reported back through the event system.

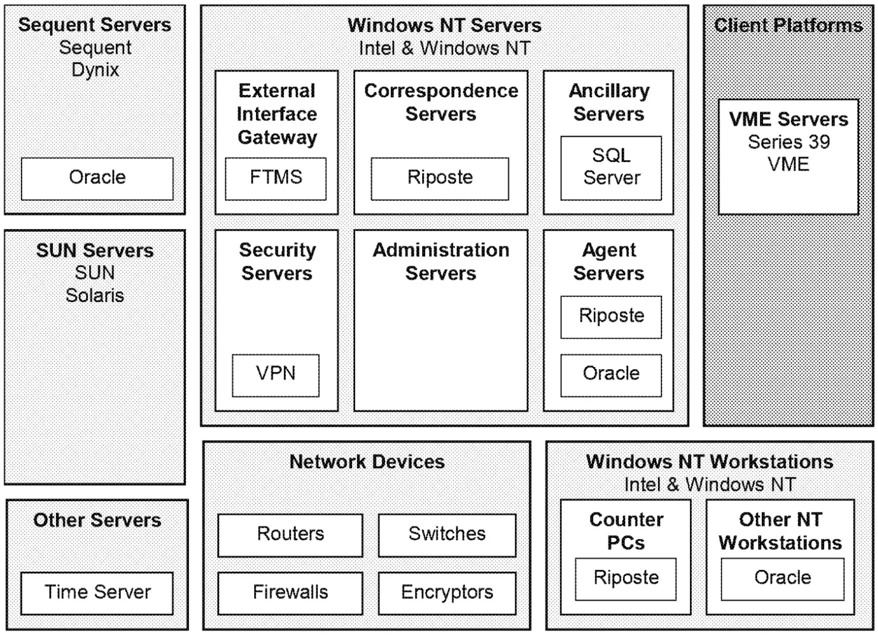

Figure 12.2 - Systems Management Platform Groupings

12.5 Systems Management Infrastructure

12.5.1 General

The systems management architecture provides a management infrastructure across all relevant Platforms. Simplistically, it is best to use a single product set to carry out the entire range of management processes. This is not always possible. Where a single product cannot support all Platforms (or there is a superior product for a particular Platform activities) then a proxy product is used to bridge the Domains.

- Architecturally, we need to look for integration and re-use of the management services and infrastructure. For example, the *Human-Computer Interface* (HCI) should be consistent across the services, and the event management service should be available for use by a number of different services.
- The chosen products should be scaleable to support the number of managed nodes. This is mostly driven by the number of Counters. Consideration should also be given to the number of Campus based systems, and the impact on the systems management architecture of "sideways expansion" of these to provide additional system capacity.
- They must provide notification of the outcome of management processes so that the overall operation and status of the estate can be monitored by support staff
- They must not overload the network. For example, it should be possible to schedule bulk systems management transfers out of normal working hours
- They must not overload the managed resources with management processes

The management products used by Pathway are as follows.

- *The Tivoli Management Environment* (TME). This is supplied by IBM and includes a range of products that cover most of the management processes required. Tivoli is used for all services on NT platforms. It provides a central event management service, and includes event proxies that intercept and translate event information generated by other management regimes. It also provides software distribution and resource monitoring facilities. The TME facilities have been extended to handle the scale of the Pathway network and to provide sophisticated inventory facilities
- *HP OpenView* together with Cisco Works are used to manage network products such as Routers. An OpenView Tivoli event Adapter maps SNMP traps generated by OpenView into Tivoli events
- *BMC Patrol* is used to handle the Host Central Servers and the Oracle applications running on them. Patrol is specifically tailored to the management of UNIX systems and applications, especially database applications. A Patrol Tivoli Event Adapter is provided to map Patrol events onto Tivoli events. BMC can generate *pager alerts* if problems arise on the Platforms it manages
- *Maestro* from Unison Software (now IBM) is used to provide scheduling facilities
- *PowerHelp* provides Help Desk facilities to the HSHD (part of FCS) for problems encountered with the Horizon hardware and software
- *Despatch-1* provides a hardware inventory used by UKSS (part of FCS) for spares management. It is not connected to any other management products
- The *Firewall Enterprise Centre* provides centralised management of all Firewalls

- The Pathway developed MIS applications, which analyse information stored in the Data Warehouse, are used to provide Service Level Management (SLAM) facilities
- A *Time Server* is used to distribute GPS-derived time signals to all servers, and local server-specific functions are used to interact with this
- An *Audit Service* using the Legato bulk storage management product is used to write historical audit information to bulk storage media, and retrieve it if required
- Pathway developed *Estate Management* applications are used to manage the introduction and configuration of new Outlets
- Pathway developed *Software Signing Mechanisms* are used to verify the integrity and origin of software installed on Pathway platforms

The interworking of these products is summarised here.

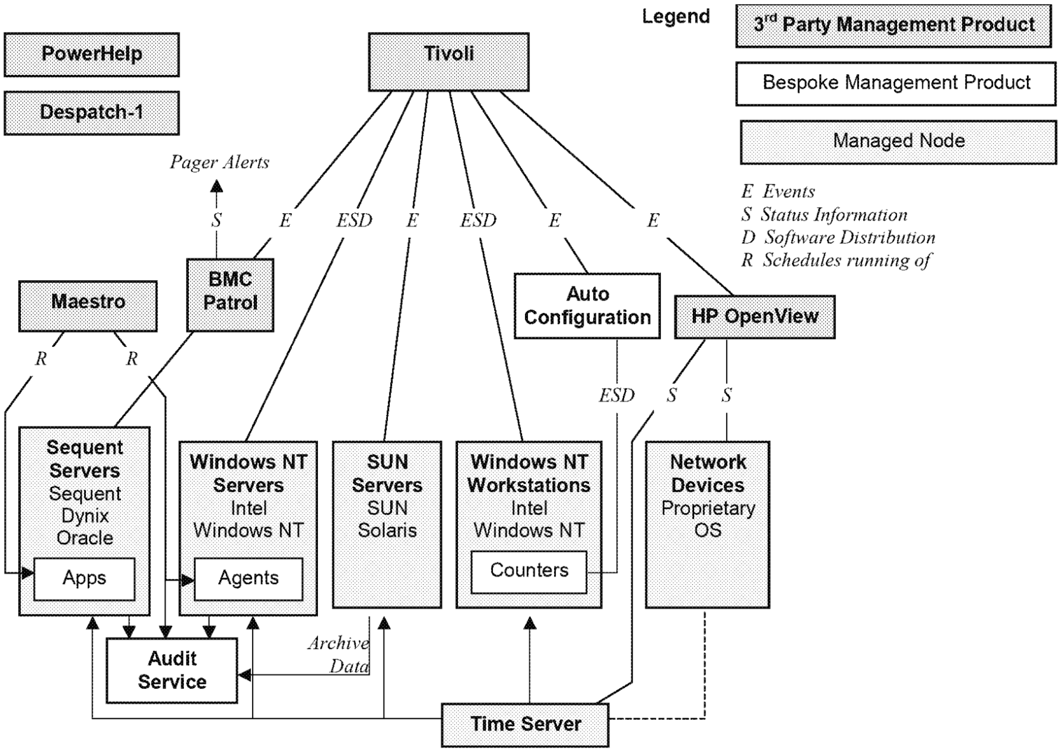

Figure 12.3 - Managed Object Domains

Client Systems are managed by the Client's own Systems Management products, if anything.

The remainder of this Section describes the capabilities and limitations of each of these products.

12.5.2 Tivoli Management Environment (TME)

12.5.2.1 General

TME provides a common set of management actions, and information stored on each managed node enables a local management agent to perform the local variant of these actions according to its own architecture and capabilities. These applications operate within a hierarchical management structure which permits a central management station to manage a set of subservient management centres, each of which manages an underlying set and so on. This structure avoids performance bottlenecks at the central management system.

12.5.2.2 Packaged TME Products

The core TME Management Framework components are packaged together into a number of components for each Platform type. The packages are named as follows.

Platform Type	Package Name	Function
Windows NT	MANNTEP	Core management facilties for NT platforms
Windows NT	MANSENTRY	Support code for Distributed Monitoring agents (previously known as Sentries). There are variants for different platform types
Windows NT	MANTOOLS	Bespoke software to support Tivoli tasks
Windows NT	MANEVENT	Event monitoring facilities; used with a platform-specific Filter definition
SUN Solaris	MANSOEP	Core management facilities for Solaris platforms
Sequent Dynix	MANSEQ	Core management facilities for Dynix platforms

Table 12.6 – TME Capsules

The Management Framework on each managed node attempts to make a connection to the management system each time it is booted. If this attempt fails, the management framework closes. Pathway supplied code restarts the Management Framework periodically to retry the connection.

12.5.2.3 Tivoli Management Regions (TMRs)

TME uses an object database on each managed node and end point. A central management system includes the details of each end point. However, support of up to 40,000 Counter PCs is beyond the scope of a single layered management architecture. Thus, a multi-level structure is used. The basic building block of TME is a *Tivoli Management Region*, or TMR, which consists of a database and software responsible for a number of enbd points (or other TMRs). A TMR can handle up to 1,000 end points, so we require a total of 40 Client Only TMRs. These are grouped four to a server. Ten servers are used, with five at each Campus.

A separate two-tier TMR is used to manage the Campus UNIX servers.

The resulting configuration is as shown here.

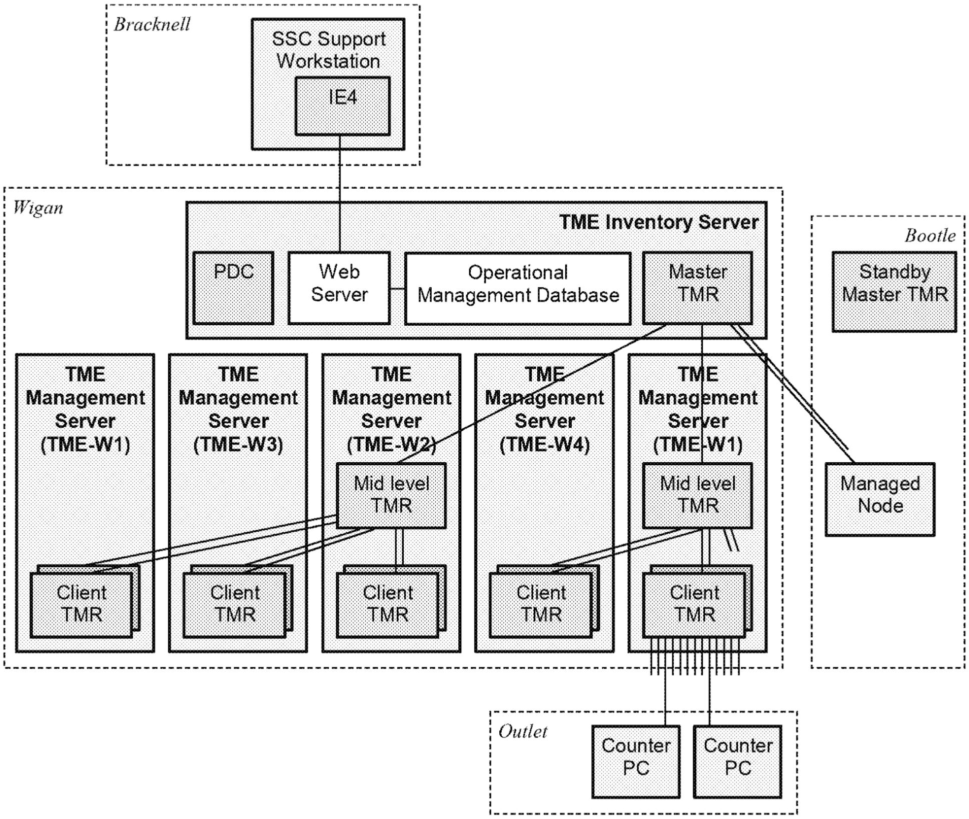

Figure 12.4 - TMR Hierarchy

A "Virtual LAN" (VLAN) is used to link the TME Servers on the two Campuses. Each Management Server has a standby at the Campus, and data is regularly transmitted between the two so that the standby systems are ready to take over should the need arise.

12.5.2.3.1 Master TMR

There is a single TMR (with warm standby). It contains persistent management information for each Counter. In addition, there are 20 TME Gateway Servers. These support most management operations between the endpoint (a Counter) and the central management system. At any one time, an Outlet is known to a single TME Gateway Server (and in fact has a preferred gateway). It may roam to other gateways under failure conditions. The process of returning to the home gateway is straightforward.

Thus, each gateway services:

- 900 Outlets
- 2,100 Counters
- 72 concurrent ISDN lines

12.5.2.3.2 Tivoli Desktop

This is a PC based client application that accesses the Master TMR. It runs on a number of Windows NT Workstations at Stevenage and Lytham St Annes, all connected via the WAN to the Master TMR. Stevenage handles the administration of management actions, Lytham St Annes the design and planning of them.

12.5.2.3.3 Operational Management Database (OMDB)

The TME Inventory Server contains an Oracle database known as the *Operational Management Databse,* or OMDB. This was originally supplied as part of TME. It has been substantially enhanced by FSCS to provide operational information to a number of support teams. Data from the OMDB is made available to the following operational and support teams via a Web server.

- FSCS Operations staff in Belfast
- FSCS SMC at Stevenage
- FSCS SMG at Lytham St Annes
- Pathway SSC at Bracknell
- Pathway security staff at Feltham
- Pathway Implementation team at Kidsgrove

12.5.2.3.4 Service Management Database (SMDB)

The TME Inventory Server provides highly valuable services within the Horizon system. It contains information that is extremely useful to the SSC and other support organisations. However, to protect the integrity of this data, it is not made accessible to all the organisations that could wish to use it. Instead, a separate SMDB Server is provided. It supports a *Service Management Database* (SMDB) that is regularly updated with significant information from the OMDB. This is a one-way feed via the Firewalls that protect the Campus systems. The SMDB is located outside the firewalls. Oracle web services are provided on the SMDB server to make support information from the SMDB available to all the staff who require it.

12.5.3 SYSMAN

Pathway has enhanced the core Tivoli product with a number of bespoke add-ons that provide additional scalability and monitoring facilities. The resulting product, SYSMAN, thus contains both Tivoli and bespoke code. It is structured as follows.

12.5.3.1 Structure

Notes

Supplier FS ISD

Component	**Platforms**
ACDB Feeder	TME Inventory Server
ACDB Watcher	Auto Configuration Delivery Server
AdminCfg	Counter PC
Auto-Targeting Aiming Device (ATAD)	TME Inventory Server
Auto-Targeting Engine (ATE)	TME Inventory Server
Brain Builder	Auto Configuration Delivery Server
	Tivoli Brain Builder
	TME Gateway Server
Brain Builder	TME Inventory Server
Counter Application Scheduler	Counter PC
EACRR-Client	Agent Server
	Correspondence Server
	DCS Agent Server
	NBS Agent Server
	VPN Server
ISDN Call Monitor	Counter PC
MANEVENT	(all NT platforms)
MANEVENT Filter Counter	Counter PC
MANEVENT Filter Server	(all NT servers)
MANEVENT Filter Workstation	(all NT workstations exceptCounters)
MANNTEP	(all NT platforms)
MANSENTRY Counter	Counter PC

MANSENTRY FTMS	(all FTMS Gatetway servers)
MANSENTRY KMA	KMA Server
MANSENTRY VPN Server	VPN Server
MANSENTRY VPNEX	VPN Exception Server
MANSENTRY VPNLW	VPN Loopback Workstation
MANSENTRY VPNPM	VPN Policy File Management Server
MANSENTRYCFG Counter	Counter PC
MANSENTRYCFG FTMS	AP Client Gateway - Local
	AP Client Gateway - Remote
	General Purpose FTMS Gateway - Local
	General Purpose FTMS Gateway - Remote
	Horizon Help Desk Gateway - Local
	Horizon Help Desk Gateway - Remote
	Network Banking FTMS Local Gateway
	Network Banking FTMS Remote Gateway
	POCL Standby Gateway - Remote
	POCL TIP Gateway Server - Local
	POCL TIP Gateway Server - Remote
MANSENTRYCFG KMA	KMA Server
MANSENTRYCFG VPN Server	VPN Server
MANSENTRYCFG VPNEX	VPN Exception Server
MANSENTRYCFG VPNLW	VPN Loopback Workstation
MANSENTRYCFG VPNPM	VPN Policy File Management Server
MANSEQ	Data Warehouse Server
	Host Central Server
MANSOEP	Firewall Management Server
	SecurID ACE Server
MANSOEP	TME Event Server - 1
	TME Event Server - 2
	TME Gateway Server
MANTOOLS	(all NT platforms)
MANTRC - Tivoli Remote Console Management	(all NT platforms except Counters)
NT Backup System	Counter PC
NT Fail Safe Code Generator Utility	One Time Password Workstation
NT Fail Safe Startup System	Counter PC
Operational Management Database (OMDB)	TME Inventory Server
Riposte Archiving Agent	Audit Server
SMDB Host Application	SMDB Server
Software Distribution - Counter	Counter PC
Tivoli Agent/Host Recovery	Agent Server
	DCS Agent Server
	DCS Management Server
	NBS Agent Server
Tivoli Web Browser	SecurID Admin Workstation

12.5.4 Software Distribution

12.5.4.1 Scope

Where a change cannot be handled by Reference Data, it may be necessary to distribute new or changed code. This is automated using Software Distribution facilities. Facilities include:

- The ability to define a software product or product upgrade in terms of the following.
  - Its constituent files
  - Scripts to perform the installation (and removal) of the product
  - Criteria by which it can be asserted that a software product is correctly installed (a software signature)
  - A naming scheme for identifying the product
- The identification of the managed systems and the network routes to those systems

The operations that can be executed by the Software Distribution system include:

- Distribute a software product or product upgrade to one or more end systems
- Activate a software product on one or more end systems, including executing any necessary data translation functions
- Revert to a previous version of a software product
- Delete a software product on one or more end systems

A scheduling infrastructure enables operations to be executed at a defined time. This allows a set of operations to be grouped into a single entity (a job or task) which can be individually scheduled.

A reporting infrastructure transmits the results of operations to the central systems and displays them to support staff.

The scope of the Software Distribution process is as follows. It is described in more detail in [SWDIST].

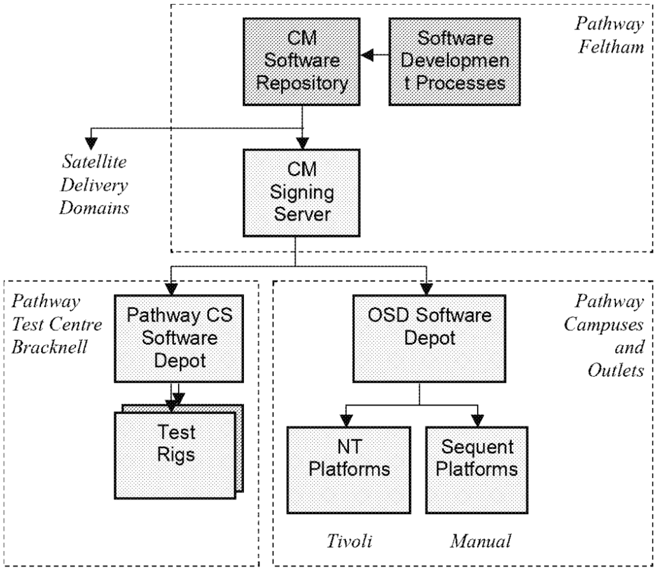
Pathway Feltham
CM Software Repository
Software Developmen t Processes
Satellite Delivery Domains
CM Signing Server
Pathway Test Centre Bracknell
Pathway CS Software Depot
Test Rigs
OSD Software Depot
Pathway Campuses and Outlets
NT Platforms
Sequent Platforms
Tivoli
Manual

Figure 12.5 - Software Distribution Routes

Software is generated in the first instance by Pathway and its suppliers, and lodged in the CM Software Repository (PVCS). It has an identifiable Name and Version Number. These are carried with it throughout the distribution process.

When it is ready for release, it is transmitted from PVCS via the CM Signing Server to either the Pathway Software Depot for testing at Bracknell, or the Outsourcing Software Depot for distribution to the live estate. In either case, it is first verified as being ready for release. The purpose of the distribution to Bracknell is to verify that the Tivoli distribution packages can be applied successfully.

The technology used to deliver software to its target Platforms depends on the Platform type and the tools selected. Tivoli is used for Windows NT platforms, both within the Campuses and in the Outlets.

(Some software is delivered to platforms, such as the Cisco Routers, that are outside the scope of this process.)

12.5.4.2 Tivoli Software Distribution

Tivoli Software Distribution provides the main part of the mechanisms used to deliver software to Counter PCs and other NT platforms. It is augmented by some software specifically developed for Pathway by FSCS.

12.5.4.3 Preparing for Software Distribution

Software is distributed in units called *file packages*. Packages are constructed by Pathway following detailed analysis, script development and rigorous testing. These must include the development of a regression capability. A package can represent a single file, a set of related files, an entire application, or any combination of these. File packages can be modified, for example depending on the destination. They can cause a system reboot.

12.5.4.4 Practicalities of Software Distribution to Counter PCs

The most common use of Software Distribution is to upgrade the software environment of the Counter PCs. Some specific issues need to be addressed here. Microsoft delivers bug fixes and enhancements to specific Windows NT versions in what are known as "Service Packs". These can be of some considerable size, as Microsoft's policy is that each Service Pack subsumes each of its predecessors. In addition, each Service Pack finishes by causing a system reboot.

Although Microsoft Service Packs now include a regression capability, their sheer size means that Pathway needs to take special care with the installation of a Service Pack. It must be assumed that the application of a Service Pack change could disable both the primary applications and the capability for systems management. Comprehensive validation of a patched system is carried out prior to any Release. This includes testing on every hardware combination.

It is possible to bypass the standard Service Pack installation process, and use Tivoli to apply the changes to the operating system in the same way that a standard application would be upgraded. This includes generating a regression capability. Counter PCs include a second cut-down Windows NT system, which can only be entered via a one-time password. Its sole function is to reverse the last upgrade. This is described in [FAILSAFE].

12.5.4.5 Distribution Management

Software Distribution operates in a hierarchical manner. Packages are passed first to a local Tivoli Management Server. This distributes it to the target environment (for example Outlets). Two bespoke tools are used to determine the distribution targets and network routes.

- The *Auto Targeting Aiming Device* (ATAD). This is responsible for setting up the distributions, using its knowledge of the ISDN network and the allocation of Outlets to Routers.
- The *Auto Targeting Engine* (ATE), which drives the actual distribution.

The interrelationships between these are shown here.

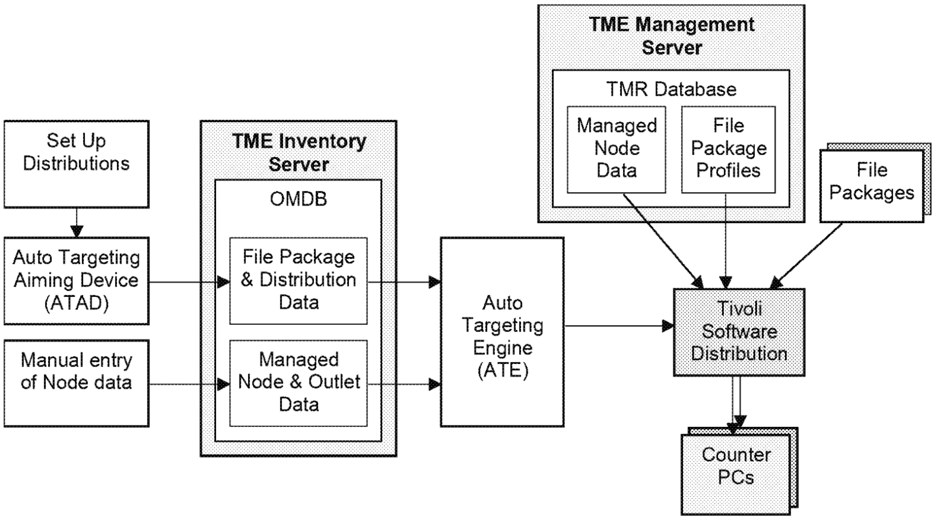
TME Management Server
TMR Database
Managed Node Data
File Package Profiles
File Packages
Set Up Distributions
TME Inventory Server
OMDB
Auto Targeting Aiming Device (ATAD)
File Package & Distribution Data
Manual entry of Node data
Managed Node & Outlet Data
Auto Targeting Engine (ATE)
Tivoli Software Distribution
Counter PCs

Figure 12.6 - Software Distribution Processes

12.5.4.5.1 Auto Targeting Aiming Device (ATAD)

This computes the distribution required to apply a given change to the live estate. It accesses the OMDB Inventory to identify which Outlets need the change.

12.5.4.5.2 Automatic Targeting Engine (ATE)

This handles the distribution of software packages to Outlets. There is one ATE per TMR. It operates during the *Software Distribution Window*, a period overnight when software distribution or activation is permitted to occur. This is controlled by the Maestro schedule. It ensures that Riposte is not running at the same time.

There are three types of underlying ISDN service:

- *Symmetric ISDN service*. There are no restrictions at Campus or Counter on call set up except the number of PRI lines available and the QOS of the backbone network service. This was the only type prior to BI1. It is retained in small numbers
- *FRIACO service – Dial in*. This is an asymmetric ISDN service where the Outlet can call into the Campus but the Campus cannot call out to an Outlet. The concurrency of calls is dictated by the number of ports purchased from the TELCO
- *FRIACO service – Permanently Connected*. Again the Outlet can dial in but the Campus cannot dial out to an Outlet. However, this service allows the Outlet to keep the line permanently open at a reasonable cost. Each connected Outlet consumes a single dedicated port

There are different QoS for each service, but these are not apparent to a (primarily) TCP based application like Tivoli. Hence, once established the ISDN call can sustain a data rate of 0.3 Mb/minute (the end to end data rate currently seen in software distribution).

The type of network available at a particular Outlet is held within the system management data for an Outlet. The components involved are as shown below.

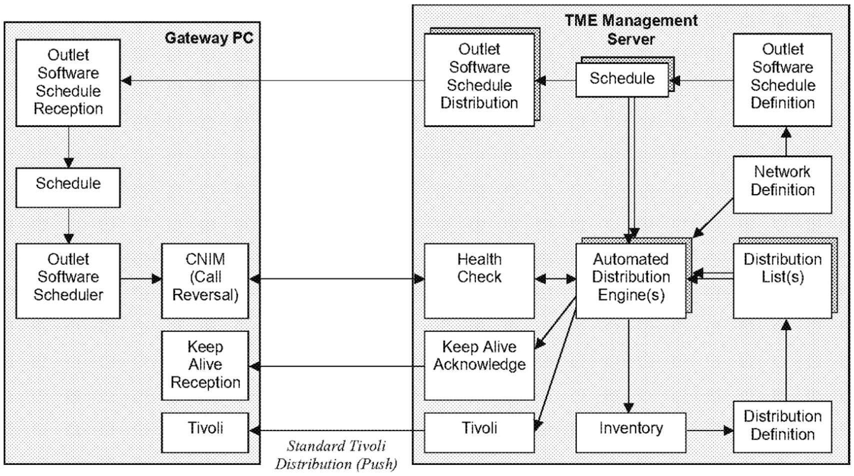

Figure 12.7 – Software Distribution with Call Reversal

The logical components are as follows.

- *Outlet Software Schedule.* This indicates, from the Counter viewpoint, when it should accept software distribution by call reversal. There is one Schedule per Outlet. Normally, it will indicate merely the standard software distribution window(s), but there will be cases (pilot, emergencies etc) where the schedule may be modified by a number of other considerations
- *Outlet Software Schedule Definition.* This component defines the Schedule.
- *Outlet Software Schedule Distribution.* This is the transport mechanism to update the schedule at the Outlet, and represents the existing infrastructure for software distribution using Outward calls from the Campus
- *Distribution Definition.* This uses the Inventory (part of OMDB) to enumerate the Counters to be updated for a single change, and generates a *Distribution List.* The current Pathway product is the ATAD
- At well-defined periods, the ATEs are activated and start processing the outstanding Distribution Lists. Each ATE services a portion of the estate. It looks in the Distribution Lists for Counters it services, and batches up a set of software distributions to give to Tivoli. The size and content of each batch is such that it does not overload the network or the platform on which the Tivoli distribution engine resides. Software distributions may run with quiet data transfer periods longer than the ISDN inactivity timer, and so to avoid the ISDN call being dropped a "Keep Alive" acknowledgement service is started that generates a continual stream of small packets (*Keep Alive Acknowledgements)* that is directed to a IP port where they are discarded. This port is the *Keep Alive Reception*
- When the ISDN calls reach the Outlet, it must be rejected but then the Outlet must immediately call back at the ISDN layer such that the call reversal is transparent to the ATE. This mechanism is implemented by the *Counter Network Information Monitor* (CNIM).
- Distribution then proceeds

12.5.4.6 Distribution Monitoring

Tivoli *Distribution Monitoring* runs on each client platform and monitors the operation of the installation process. It returns status information to the OMDB to record the system status and the presence of the installed files.

The OMDB includes a Web browsing capability. This enables support staff in a variety of locations to examine the status of distributions, the software state of any managed node, and any problems that have occurred with a distribution.

12.5.4.7 Activating New Counter PC Software

Within an Outlet, the Gateway PC forwards the package to the other Counter PCs.

The Tivoli *Commit* operation is used in a Software Distribution Window, perhaps some time later, to run the installation routine in unattended mode. The package is re-verified before installation takes place. Conventionally this operation creates a regression capability, for example taking before-looks of the NT registry, copies of replaced DLLs and so on. Installation is unattended, to avoid relying on (non-existent) technical support at the target site.

A utility called *PathwayLoad* is used to start (and stop) the Riposte Desktop. Thus when Tivoli needs to update any Counter PC software it executes the following sequence.

- Call *PathwayLoad* to close down the desktop (it uses APIs provided by Riposte)
- Shut down the Riposte related services
- Shut down the Riposte Message Server(s)
- Update the necessary software
- Restart the Riposte Message Service(s)
- Restart the Riposte related services
- Call *PathwayLoad* to start the desktop

(The same sequence is used to unload and reload the desktop each night. It is deferred if there is a user logged into the system at the time.)

Where the distribution involves changes to a Driver, it will be necessary to reboot the Counter PC. This is feasible, using standard Microsoft APIs to specify new files to be included at the next reboot.

The Counter PC system is configured with the following Windows NT Services:

- Riposte Message Servers (operational, mirror, training)
- Agents (e.g. PORedirector)
- Tivoli event adapter
- PCConfig (part of Auto-Configuration)

Most of these services will fail if they run on a locked filestore, and hence they cannot be started automatically by Windows NT. Instead, they are defined as "started manually", and the POLO process kicks them off during a normal reboot after it has unlocked the filestore.

It is unrealistic to expect the Post Office Manager to be present during the overnight software distribution window when a reboot is required, or for that window to be delayed until 09:00. Thus, where a Counter reboot is required, the Gateway PC communicates with the KMA Server to verify that it is reasonable for it to be rebooting at that time.

12.5.4.8 Software Distribution to Sequent Platforms

There is no automated software distribution to Sequent platforms.

Tivoli now has the ability to handle UNIX based packages that include calls on the standard pkgadd *and similar commands. This enables FSCS to distribute upgrades to these Platforms, and more importantly to ensure than any such upgrades are integrity sealed by Pathway (though this requires the availability of the Layer7 code on UNIX. It is likely that this form of software distribution will be introduced at an infrastructure Release beyond BI3.*

12.5.5 Problem Management

Lights out operation at the Campuses needs automated problem detection and management. Platforms should generate events in response to problems. Tivoli provides facilities to take events from one or more sources and use defined rules to establish whether local actions shall be taken and/or whether they should be forwarded to central event servers. Event servers include functions such as the ability to correlate events, to evaluate the actions to be taken, and to schedule these actions.

When the automated systems are unable to handle a problem, they should bring it promptly to the attention of a human. This person, who may be on a remote site, can manage the impact of the problem, assign it to an appropriate support team, and track the processing of the problem using automated Help Desk facilities.

Sources of problems include applications and the operating systems as well as hardware failures. Some platform types provide event handling facilities. *Event Proxies* take these Platform-dependent events and map them onto the normalised form for a central event manager. For example, NT appends events to several event logs. These can be retrieved by an application that reads the end of these logs as they are written. Some network components emit events as *Simple Network Management Protocol* (SNMP) traps.

12.5.5.1 Event Management

Tivoli Event Management is used to gather information about the past and present behaviour of the managed system, and pass this information back to the systems management centre. It has two principal components: *Tivoli Event Server* that collects and assesses events, and *Tivoli Event Console* (TEC), which displays the status of monitored nodes to an operator.

Each TMR is associated with a TEC that co-ordinates all system events created within TME or by other management systems that feed into it (OpenView and BMC Patrol). These processes are developed by FSCS.

12.5.5.1.1 Event Generation

The event generation process is non-invasive. Applications and Platforms use their standard event generation facilities, and these are then picked up by Tivoli. Event adapters include:

- UNIX Log File Adapter, which reads information from the UNIX *syslog* file, or from an application log file, and generates Tivoli events to send to the Event Server
- NT Log File Adapter, which monitors the Windows NT Event Logs and generates Tivoli events from designated record types
- HP OpenView Event Adapter which can forward SNMP traps to Event Server

Events are forwarded immediately they are generated. The NT Event Adapter will cache them in memory if the TEC is unable to accept them or if the network is busy.

Events generated on Counter PCs are treated in the same way as Riposte Priority messages. They cause the ISDN line to be raised immediately. Thus, Counter PCs do not use Tivoli events except in extreme conditions, to avoid raising the ISDN link. A filter on the Counter limits candidate events to those generated by Applications that are not of type "information".

12.5.5.1.2 Resource Monitoring

Tivoli *Sentry Monitors* provide the facility to monitor key system attributes. Some are provided by Tivoli, others by third parties. Monitors include those for:

- Disk
- Security
- Network
- Printers
- System resources
- Administration

Use of these functions at the Counters is governed by the limited capacity of the ISDN links.

12.5.5.1.3 Failure Monitoring

Tivoli "pings" the Tivoli agent on a remote Platform before beginning a complex operation. Lack of a response indicates that the Platform or service has failed or is unreachable (perhaps because of a network failure). These agents are located on each Windows NT Server.

Tivoli also provides a Heartbeat facility for failure monitoring. This is not used for routine monitoring of Counter PCs because of the network overheads that would be involved if the ISDN line were raised for each heartbeat. Tivoli agents on Counter PCs can generate status indications, but these are reserved for pathological conditions.

12.5.5.1.4 Event Collection

Event Server includes facilities to gather, collect, correlate and route information about the status of all aspects of the distributed environment. It provides rule-based event correlation facilities for integrating network, systems, database and application management. Grouping and filtering facilities are provided, so that it is possible to minimise the number of events displayed to operations staff.

In order to handle the volume of events generated by nearly 40,000 end points, a hierarchy of TEC servers is used. This comprises a master TEC server and six reception TEC servers. Incoming events go to one of the reception servers, chosen for load balancing and resilience. The reception servers perform event filtering against a rules base which, for example, copies all events to an archive schema and forwards a subset of events to the Master TEC Server for operator attention.

Automated Responses can be triggered when a monitored resource meets a predefined threshold. They can take the form of a notification or an action. Notifications can be delivered by electronic mail, a notice to the Tivoli desktop, a pop-up window alarm, or an alert to the Enterprise Console. Actions can take the form of a shell script, PERL script or C program.

12.5.5.1.5 Event Display

Events are fed both to the TEC and to an Oracle-based Web Server that can be used by support staff to interrogate the status of aspects of the system, particularly Outlets.

12.5.5.1.6 Event Retention

Events are retained within TME Event Server while they are current. However, a record of the events that have occurred within the system in the recent past is of great use for problem management and audit reasons. Thus each day the Tivoli events are off-loaded into an Oracle database (the *Tivoli Expired Events Database)* where they are retained for some considerable time. The off-load process removes duplicates and transient events. Web Browser access is provided to this database as well.

12.5.5.1.7 Event Auditing

An extraction from the event database is written to the Archive Service on a regular basis. This contains user Login and Logout details, as well as other significant events, and so acts as a *Security Event Monitoring* audit track.

12.5.5.2 Tivoli Remote Control (Control)

This tool provides the means for support staff to obtain *Remote Console* access to Windows NT systems. It is subject to the standard Windows NT security constraints, and hence conforms to the [ACP]. It is described in [TRC].

It includes three separate components:

- Remote Control Service - installed on all Platforms which can be remotely managed, and all those which may be involved in managing them
- Remote Control Controller - needed on the management systems
- Remote Control Target - needed on the systems that may be remotely managed.

12.5.5.3 Data Collection from Counters

Facilities are provided for support staff to extract some or all of the Riposte Message Store from a Counter PC and return it to the SSC. If more than a very few records are retrieved, the data is passed back encrypted.

In addition, a number of Tivoli tasks are provided on the Counter PCs and may be invoked either by script or by command from the central Tivoli systems. These can be used to gather status or diagnostic information such as ISDN traces, to re-boot a Counter, and for other support purposes.

12.5.6 Software Issue Verification

12.5.6.1 General

The *Digital Signature* added by the CM Signing Server is intended to ensure that the Software Depot and any domain to which the package is distributed is able to verify its integrity and origin. It uses the standard File Sign/Verify functions. The signature is used to ensure that it is a valid distributable and that its integrity is intact.

12.5.6.2 Structure

Component	Platforms
Counter Tivoli Inventory Signatures PVCS Server SI Verifying Functions (SVF)	Counter PC Configuration Management Server Counter PC Outsourcing Software Depot Pathway Software Depot
Signing Service	Auto Configuration Signing Server CM Signing Server

12.5.6.3 Counter Tivoli Inventory Signatures

12.5.6.4 PVCS Server

This holds software builds ready to go to live platforms.

12.5.6.5 Signing Service

Signing Services are provided on two Platforms.

- The CM Signing Server is used to sign software when it is first delivered into the live estate.
- The Auto Configuration Signing Server is used to sign software that is to be distributed via the Auto Configuration process. This software may not be installed on a particular platform for some considerable time after it is released, so Auto Configuration signs it when it is installed (i.e. when the Counter PC is installed.

12.5.6.6 SI Verifying Service

This exists on the Counter PCs and on other platforms involved in the delivery of signed software. It verifies the signature each time the software in question is loaded.

12.5.7 BMC Patrol

12.5.7.1 General

BMC Patrol is a management suite tailored to manage a range of databases including Oracle. It includes a set of *Knowledge Modules* (KMs) which are script-driven and sit alongside the normal management agent. These provide rules of what actions to take when particular events occur. The intention is that the KM enables automation of many of the tasks routinely carried out by a Database Administrator.

12.5.7.2 Structure

Component	Platforms
BMC Patrol Agent	Data Warehouse Server Host Central Server
BMC Patrol Console	Data Warehouse Server Host Central Server
BMC Patrol Knowledge Module	Data Warehouse Server Host Central Server
BMC Patrol Knowledge Module for APS BMC Patrol Knowledge Module for Dynix Base	Host Central Server Data Warehouse Server Host Central Server
BMC Patrol Knowledge Module for Hytec FTF	Host Central Server

BMC Patrol Knowledge Module for Hytec Sonnet	Host Central Server
BMC Patrol Knowledge Module for Hytec VME FTF Proxy	ESNS VME System
BMC Patrol Knowledge Module for LFS	Host Central Server
BMC Patrol Knowledge Module for Maestro	Data Warehouse Server Host Central Server
BMC Patrol Knowledge Module for OBCS	Host Central Server
BMC Patrol Knowledge Module for Oracle	Data Warehouse Server Host Central Server
BMC Patrol Knowledge Module for TPS	Host Central Server
BMC Patrol to Tivoli Event Filter	Data Warehouse Server Host Central Server

12.5.7.3 Patrol Agents

BMC Patrol is used to manage the Sequent servers. Patrol Agents are located on each Sequent server, and Patrol Tivoli Event Adapters are used to intercept events of interest and pass them back to the Tivoli Event Console. Patrol can also generate Pager calls for serious operational problems.

12.5.7.4 Standard Knowledge Modules

Standard Knowledge Modules are used for the following managed resources:

- Sequent Servers
- Maestro Scheduler
- Oracle Databases

12.5.7.5 Bespoke Knowledge Modules

Horizon-specific Knowledge Modules have been developed for some of the major applications and other software including:

- Hytec Sonnet FTF Software
- OBCS
- APS
- TPS
- DRS

12.5.7.6 Patrol to Tivoli Event Adapter

This is used to feed events generated by the Patrol software into Tivoli, the strategic systems management tool set for Pathway.

12.5.7.7 Patrol Development Console

12.5.8 Network Management

12.5.8.1 Structure

Component	Platforms
CISCO Works 3.2/Solaris - HP OpenView	Network Management Server
CISCOView	Network Management Server
CISCOView for Tivoli	Network Management Server
HP OpenView Network Node Manager	Network Management Server
HP OpenView to Tivoli Event Adapter	Network Management Server

12.5.8.2 HP OpenView

HP OpenView is used by network management staff within the Campuses to configure and manage the network active devices (hubs, Routers and Switches) used.

It is the standard tool used for Network management. It operates in conjunction with Cisco Works (see below) which provides graphical facilities that enable easy management and configuration of Routers and Firewalls.

12.5.8.2.1 HP Open View to Tivoli Event Adapter

Events generated by HP OpenView may be passed back to Tivoli via an appropriate Adapter.

12.5.8.3 Cisco Works

This is a glossy graphical management tool for Cisco Routers. It operates in the form of additional menus within the HP OpenView system.

[ACP] states that all access to the Routers is via the Network Management Station. However, Cisco Works is unable to handle the complexity of the Routers used. In addition, SNMP has a low interrupt priority on the Cisco Routers used, and hence under heavy workloads these may not be manageable by SNMP. Hence, on-line Telnet access to the Routers is provided for network management staff to use where needed. Telnet access is also provided to Cisco for support purposes. This mode of access is restricted by Firewalls to the NMS and designated suppliers. Users must specify a Username and password that are validated by the TACACS system in the Network Management Server.

12.5.8.4 Router Configuration

ISDN Routers used for connection to Outlets are each configured to handle a subset of the total Outlet population. This has the benefit of spreading the comms load across them, and hence avoid problems when (for example) distributing software to all Outlets. Data is fed from the Auto-Configuration Database via Tivoli to the Network Management Server and hence to the Routers.

12.5.8.5 Firewall Management

The Firewall-1 *Enterprise Centre* provides graphical facilities for configuring and monitoring Firewalls. It runs on the Authentication Server.

It provides a centralised graphical security management system, enabling them to be configured from a secure central point.

12.5.9 Maestro Scheduler

Facilities are required to start jobs automatically, to monitor their running, start jobs that depend on them when they finish successfully, restart jobs that fail, and invoke support calls for jobs that cannot be restarted. This is provided by Maestro.

12.5.9.1 Operation

The Maestro scheduler from Unison Software (now part of IBM) is used to carry out scheduling functions within Horizon.

The *Maestro Master Console* runs within the Host Central Server at the live Campus, and controls the scheduling of applications. Maestro Agents run on each managed server.

Maestro controls the starting and stopping of all major jobs within these servers, in particular the Bulk Agents. These Agents run to completion, and report any failure messages back to Maestro. Tivoli monitors Agents and can restart them if they fail.

Maestro agents also run on a number of other platforms, including the Auto Configuration Database Server.

Interactive Agents run at all times waiting for messages from their Hosts or Riposte, and are not scheduled by Maestro.

12.5.9.2 Structure

Supplier Unison

Component	**Platforms**
Maestro Master Console International	Data Warehouse Server Host Central Server
Maestro Remote Console Tivoli Maestro Agent for NT Platforms	RDMC Administrator Workstation ACDB Server Agent Server AP Client Gateway - Local Audit Server Correspondence Server
Tivoli Maestro Agent for NT Platforms	DCS Agent Server DCS Management Server Domain Controller - Local General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local KMA Server NBS Agent Server Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway OCMS Server OCMS Server POCL TIP Gateway Server - Local Short-term Performance Database Server SSC Support Server
Tivoli Maestro Host (Unix)	Data Warehouse Server Host Central Server

12.5.9.3 Maestro Master Console

This is installed on the Host Central Server and maintains overall control of the operation of Maestro within the Horizon system.

12.5.9.4 Maestro Remote Console

12.5.9.5 Tivoli Maestro Agent

Maestro Agents are installed on each platform that needs to be managed by maestro. NT and Unix agents are used in Horizon. They communicate with the Master Console and are provided, via the Maestro Schedule, with a list of tasks to execute and actions to take when they complete.

12.5.9.6 Maestro Schedule

The Schedule is a complicated structure that determines the interoperations of processes on a number of Campus platforms. It is used by the Tivoli Maestro Agent.

12.5.10 Help Desks

There are four Help Desks within Horizon.

12.5.10.1 Horizon Systems Help Desk

12.5.10.1.1 General

This is manned by staff from the UK Support Centre (UKSS). It is used by Outlet staff who suspect they have a problem with the operation of the systems in the Outlet

FSCS's PowerHelp is used to record and maintain information about calls to the Help Desk, and their progress. The PowerHelp platforms are not connected into the Horizon network.

The Help Desk terminals supporting PowerHelp are not connected to a LAN that has access to the Horizon network. Some users of the PowerHelp system may have parallel access to a workstation that *does* provide access to the live systems. This is provided by Pathway and enforces the authentication mechanisms described in Chapter 16 "Security".

12.5.10.1.2 Structure

Component	Platforms
Counter Diagnostics	Counter PC
FTMS BT to MIS Local Connection Configuration	Horizon Help Desk Gateway - Local
FTMS BT to MIS Remote Connection Configuration	Horizon Help Desk Gateway - Remote
FTMS MITEL to MIS Local Connection Configuration	Horizon Help Desk Gateway - Local
FTMS MITEL to MIS Remote Connection Configuration	Horizon Help Desk Gateway - Remote
FTMS SORBUS to MIS Local Connection Configuration	Horizon Help Desk Gateway - Local
FTMS SORBUS to MIS Remote Connection Configuration	Horizon Help Desk Gateway - Remote
PowerHelp Client	Horizon Help Desk Terminal

12.5.10.1.3 FTMS Configurations

FTMS links are set up to enable the Help Desk to sent data from BT, Mitel and Sorbus to the MIS.

12.5.10.1.4 PowerHelp

The PowerHelp Client runs on each Horizon Help Desk terminal. It provides call management facilities for Help Desk staff.

12.5.10.2 Service Management Centre (SMC)

This is based in Stevenage, with a clone in Manchester. Staff in this centre provide a second line support service to the HSHD. They handle calls raised on PowerHelp by HSHD staff. They have access to a range of support tools including the ability to "ping" an Outlet, and are provided with access to the Web service driven by the OMDB.

12.5.10.3 System Support Centre

The Pathway SSC is located in Bracknell. It supports the applications on several operational systems in the Campuses.

A major function of the SSC is to support the TPS and other Oracle databases. Normally, information archived from these is deleted once it is secured to tape. For support purposes, data from these databases is also copied to the SSC Support Server. The Riposte Message Store from the Correspondence Servers is also regularly copied there for support purposes. There is one of these in each Campus. The SSC has access to this server and can use it, for example, to analyse problems for which the Riposte messages have been archived from the Correspondence Servers, or to extract information such as lists of non-polled Outlets.

12.5.10.3.1 Structure

Component	Platforms
Archive Viewer	SSC Support Workstation
BSU Help Desk	MIS Client Workstation MIS Support Workstation
EndOfDay Reporter	SSC Support Workstation
Expiry Reporter	SSC Support Workstation
Formatted File Utility	SSC Support Workstation
Help Desk Common Files	MIS Client Workstation MIS Support Workstation
Message Store Utility	SSC Support Workstation
MessageStore Sort Utility	SSC Support Workstation
Pathway Event Viewer	SSC Support Workstation
Riposte Query UK	Audit Workstation SSC Support Workstation
SSC Support Applications	SSC Support Server
Stops Reporter	SSC Support Workstation
WinGrep Search Utility	SSC Support Server
WinOnCD Recording Software	MIS Client Workstation MIS Support Workstation SSC Support Workstation

12.5.11 OCMS Processes

Delivering Counter PCs and the associated network components to Outlets is a human-intensive task. Much has been done to automate the processes that make those PCs fully-fledged members of the Horizon network. These are extended to handle Counter PCs that are replaced subsequently should they fail or need to be upgraded. These processes must be designed to ensure that there is no scope for hackers or others to gain unauthorised access to the Horizon network.

Information about the soon-to-be-installed Outlets is handled by a number of different processes, as shown here.

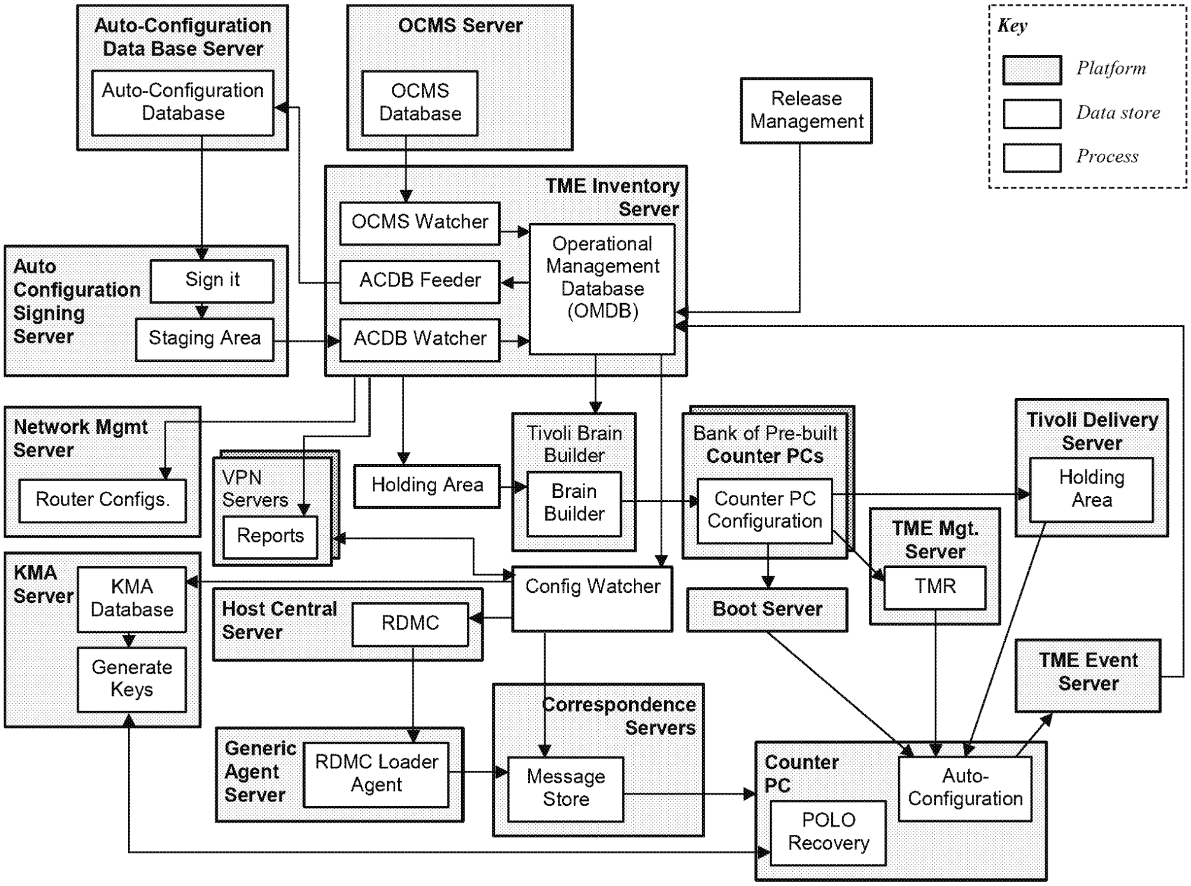

Figure 12.8 – OCMS Data Feeds

12.5.11.1 The Auto-Configuration Database (ACDB)

Information about new Outlets is fed from the OCMS to the ACDB well before installation.

12.5.11.2 Operational Management Database

12.5.11.3 Auto-Configuration Signing

Software to be installed in the new Counter PCs is fed from the ACDB to the Auto-configuration Signing Server, where it is digitally signed and passed to a Staging Area owned by FSCS.

12.5.11.4 ACDB Watcher

An ACDB Watcher (an Oracle Client) extracts information from the Auto Configuration Database and uses it to update the OMDB on the TME Inventory Server.

12.5.11.5 TME Configuration

Each new managed node needs to be made known to the appropriate TMR. During this configuration process, configuration data is written to the node.

In the case of new Counter PCs, this process can take around 20 minutes. It is not feasible to do this during the initial Auto-Configuration process when the Counter PC is installed. Instead, a set of "dummy" configurations is set up by a process known as the Tivoli *Brain Builder*. This uses a bank of six pre-configured PCs. Each in turn is built as if it is a new Counter PC, and Tivoli is invoked to set up its configuration files. The appropriate data (the Counter PC's "brain") is then copied to the Auto-Configuration Delivery Server, and the dummy PC can be re-used.

At a later date, when the actual Counter PC is installed, its "brain" is copied from the Delivery Server and the TME Management Server's address for the Counter PC is updated.

12.5.11.6 Other Pre-Installation Actions

12.5.11.6.1 Config Watcher

An Oracle Client process known as the *Config Watcher* runs three days before the designated Outlet installation date.

12.5.11.6.2 RDMC Update

Config Watcher feeds information about the Outlet to the RDMC, so that the Reference Data Loader Agent can generate its persistent objects.

12.5.11.6.3 Correspondence Server Update

Config Watcher also updates the Correspondence Servers. It generates a new Riposte Group and set of Nodes, and assigns them to an appropriate Cluster. At intervals, LUC is invoked by Maestro and picks up any new Groups.

12.5.11.7 Outlet Load Balancing

The load imposed by Outlets needs to be balanced across a number of system resources, including the Campus ISDN Routers, the Correspondence Server Clusters, and ISDN Hunting Groups. All of these can be handled automatically by the ACDB, based on the number of Counter PCs in the Outlet. Outlets with an expected unusually high transaction rate can be weighted to allow for this.

12.5.12 Auto-Configuration

The Auto Configuration mechanisms have two objectives:

- to reduce to a minimum the time taken to install the terminal
- to reduce the risk of configuration errors

This is achieved by the use of a “vanilla” terminal contains:

- Windows NT
- Riposte
- Applications
- Tivoli client software
- Sufficient communications data to enable it to connect to a designated server in Wigan.

This software set is built for a generic Counter PC. It has no *personalisation* for the Outlet in which it is installed, and may be out of date compared with the build state used in the rest of the live Estate. The *Auto Configuration* process is responsible for these two tasks:

- Personalise the Counter PC
- Bring its software build state up to date

The overall life cycle is shown here.

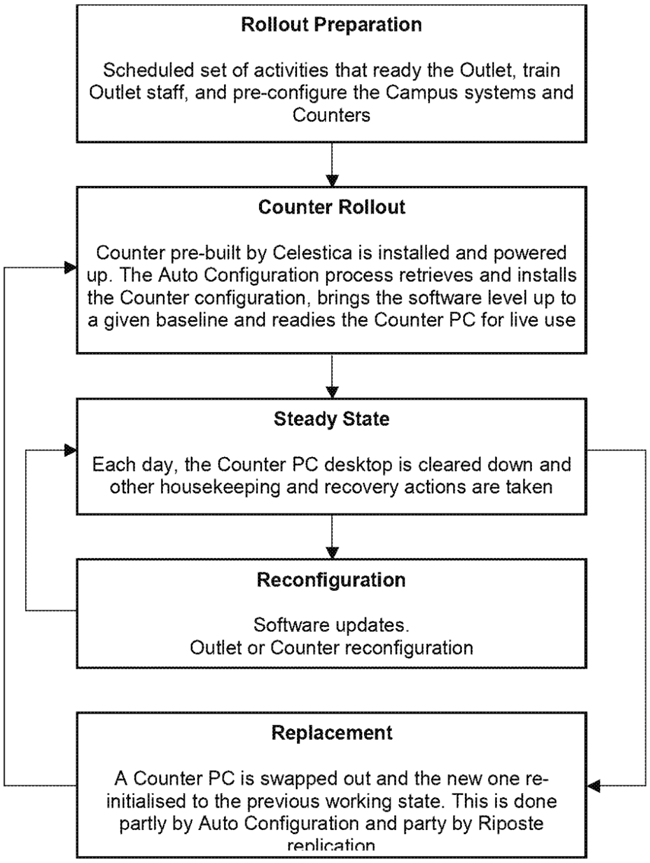
Rollout Preparation
Scheduled set of activities that ready the Outlet, train Outlet staff, and pre-configure the Campus systems and Counters
Counter Rollout
Counter pre-built by Celestica is installed and powered up. The Auto Configuration process retrieves and installs the Counter configuration, brings the software level up to a given baseline and readies the Counter PC for live use
Steady State
Each day, the Counter PC desktop is cleared down and other housekeeping and recovery actions are taken
Reconfiguration
Software updates.
Outlet or Counter reconfiguration
Replacement
A Counter PC is swapped out and the new one re-initialised to the previous working state. This is done partly by Auto Configuration and party by Riposte replication

Figure 12.9 – Counter PC Life Cycle

12.5.12.1 Structure

Component	Platforms
ACDB Client	ACDB Client Workstation
ACDB Server Application	ACDB Server
ACDB Server Executables	ACDB Server
ACF	Auto Configuration Signing Server
ACF with In-line SIPU	ACDB Server Counter PC
Auto Configuration - Counter	Counter PC
Auto Configuration Database	ACDB Server
AutoConfig ISDN Router Configuration Script Generator	Network Management Server
Boot Server Application	Boot Server
Boot Server Service for NDIS Driver	Boot Server
Counter Downloader	Counter PC
DayD Boot Server Application	Boot Server
DayD PC Config	Engineer's Day D Laptop
Eicon Diehl Boot Service for NDIS Driver	Boot Server
FAD Boot Search Application	Boot Server
Listener	Counter PC
PcConfig	Counter PC
Rollout Synchronisation (Counter)	Counter PC

SQL Mirroring	ACDB Server OCMS Server

12.5.12.2 Auto Configuration Database

This is at SQL Server database that retains information about all Outlets and their software state. It is used when the Outlet is first installed, and subsequently should any Counter PC in the Outlet need to be replaced.

12.5.12.2.1 ACDB Mirroring

There is one Auto Configuration Database at each Campus. One is "live", and the other a standby. The database on the live server is mirrored onto the standby database at the other Campus, so that this is relatively up to date should it be necessary to failover to the other Campus.

12.5.12.3 Auto Configuration Client

This runs on support workstations and is used to update information held in the Auto Configuration Database.

12.5.12.4 Boot Server Application

Newly installed Counter PCs only know the address of the Boot Server in one of the Campuses. This server contains an application that accepts and verifies the initial call from a new Counter PC, and starts the personalisation process by downloading the *Boot Server File* (BSF) to the Counter PC.

12.5.12.5 Auto Configuration on the Counter

A number of Auto Configuration components run on the Counter PC and are invoked when the Counter is installed.

12.5.12.5.1 PC Config

When the Counter PC is installed, a component known as *PC Config* is started. It ascertains the Counter PC type and connects to the Boot Server. This personalises it (e.g. by setting its IP address) and enables it to connect to its designated TMR. It then sets the Autologin flag to *Downloader* and causes a reboot.

12.5.12.5.2 Counter Downloader

Following a reboot, the *Downloader* component is entered. It copies the *Auto Configuration Files* (ACF) and the "brain" data set up as described above. This can include new software versions, later than those included in the PC's base build, that are needed to complete the installation. (Other software upgrades can be delivered overnight later). Once configuration is complete, it generates a Tivoli Event to signify that it exists. It then sets the Autologin flag to POLO and causes a second reboot.

12.5.12.5.3 Listener

The *Listener* runs in parallel with the POLO login function, following another reboot. It handles boot requests from other Counter PCs within the Outlet.

12.5.12.5.4 Software Catch-Up

Counter PCs are pre-build by Celestica using a "cold Build" supplied by Pathway. This may be out of date by the time the Counter PC is actually installed in an Outlet, because of fixes or upgrades applied to the live estate via software distribution. Thus following installation, the Counter PC goes through a "catch up" process (*Rollout Synchronisation*) in which all fixes and upgrades introduced later than the date of the cold Build are installed on it. A standard method is adopted for closing all Counter applications, including the Riposte Desktop and related services, prior to the upgrade.

Riposte causes particular problems when a Counter PC is replaced by one from spares. The new PC is likely to be several fixes behind the other Counter PCs in the Outlet. The catch-up process can be used to update the new Counter, but this must be done *before* Riposte is started. This is because, as soon as it starts, it will replicate its message store from the other Counters in the Outlet. The message store indicates the software level that the Riposte software should be at. While the catch-up process will get the Counter to the latest software level, should replication begin before the catch-up is complete, Riposte Desktop will fail to start.

The outstanding updates need to be applied following installation. However, there are significant limitations, including the following.

- The size of each update. ISDN bandwidth is likely to be a factor
- The number of updates to each package. It is best to apply a single cumulative upgrade, rather than a series of patches
- Scheduling and distributing the upgrade via Tivoli during the roll out
- Whether patches can be applied *after* the Counter PC is handed over to the Post Office

The approach used is as follows.

- Each Release has a Release signature which identifies the current Counter PC baseline.

- Following Auto-configuration, the Tivoli script reads the current Release Signature on the Counter PC, which identifies when the Build was created. It determines from this Signature whether any upgrades should be applied immediately, and if so copies them from the TMR and activates them. Individual Product signatures may change as a result of this.

- After configuration the Counter PC reboots and enters POLO. After POLO executes it starts Riposte and invokes the "Pathway journal synchronisation process". At this time, the RMS journal is empty and thus Riposte fails its operational integrity check (there are no security Persistent Objects yet). It thus synchronises its journal with the Correspondence Server.

These mechanisms are also used to force Windows NT to reload the Riposte Desktop each night. This is necessary to ensure that new versions of Persistent Objects are picked up. Persistent Objects are used to configure some applications, and to specify the Menu Buttons and their meanings.

There is one further complication. Upgrades cannot be applied after installation to the software that manages the catch-up process. If this software changes for any reason, it is necessary to prepare a new Celestica build.

12.5.12.5.5 Counter Operational Control

In normal operation, Counter PCs run under the control of a *Counter Scheduler* that executes a number of tasks at specific times of the day. This facility is used to invoke tasks such as the following.

- Run Counter initialisation processes in a defined order once POLO is complete
- Run End of Day activities
- Close down the desktop each night, to enable new Riposte menu items to be picked up

The sequence of operations is shown here.

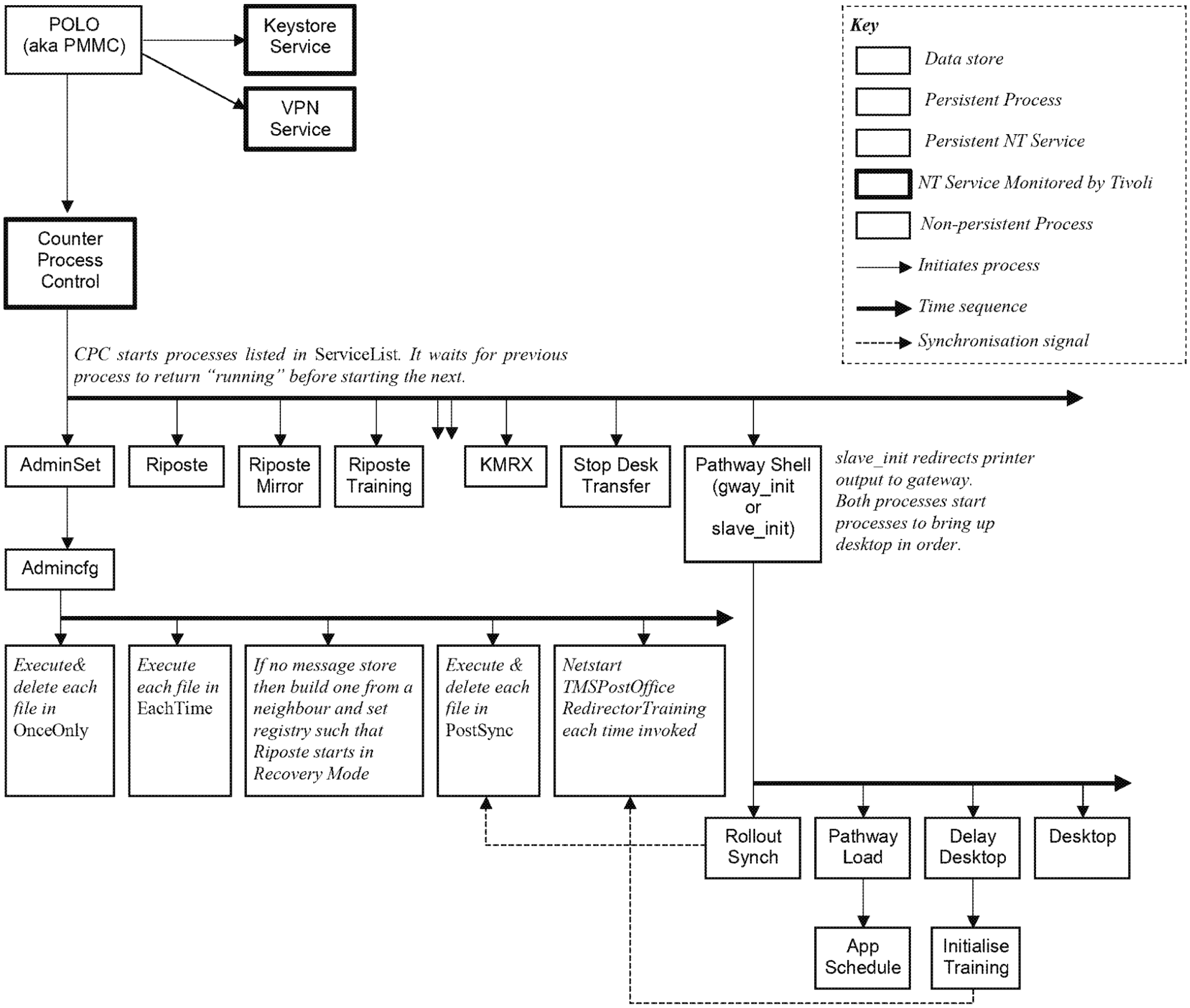
POLO (aka PMMC)
Keystore Service
VPN Service
Counter Process Control
CPC starts processes listed in ServiceList. It waits for previous process to return "running" before starting the next.
AdminSet
Riposte
Riposte Mirror
Riposte Training
KMRX
Stop Desk Transfer
Pathway Shell (gway_init or slave_init)
slave_init redirects printer output to gateway. Both processes start processes to bring up desktop in order.
Admincfg
Execute& delete each file in OnceOnly
Execute each file in EachTime
If no message store then build one from a neighbour and set registry such that Riposte starts in Recovery Mode
Execute & delete each file in PostSync
Netstart TMSPostOffice RedirectorTraining each time invoked
Rollout Synch
Pathway Load
Delay Desktop
Desktop
App Schedule
Initialise Training
Key
Data store
Persistent Process
Persistent NT Service
NT Service Monitored by Tivoli
Non-persistent Process
Initiates process
Time sequence
Synchronisation signal

Figure 12.10 – Counter Process Control

12.5.12.5.5.1 AdminSet

This handles the service logon details, and invokes AdminCFG when logon is complete.

12.5.12.5.5.2 AdminCFG

This handles a number of actions needed to place the Counter in a "runnable" state. These include:

- Generate a new password for the AdminCfg Account. This has administrative privileges, so needs to be safely obfuscated.
- Execute any files, delivered by Tivoli, that need to run each time the Desktop is loaded
- Execute any files, delivered by Tivoli, that need to run once, and then delete these files.
- If necessary, obtain a copy of the Riposte Message Store from a neighbour (the squirreled copy discussed in Chapter 13) or from an exchangeable disk in the case or a Single-Counter Outlet.

12.5.12.5.5.3 Riposte

12.5.12.5.5.4 Riposte Mirror

12.5.12.5.5.5 Riposte Training

12.5.12.5.5.6 KMRX

12.5.12.5.5.7 Stop Desk Transfer

12.5.12.5.5.8 Pathway Shell

12.5.12.5.5.9 Rollout Synch

12.5.12.5.5.10 Pathway Load

12.5.12.5.5.11 Delay Desktop

12.5.12.5.5.12 Desktop

12.5.13 Outlet Change Management

The mechanisms above handle the initial installation of an Outlet. An estimated 2.5% of Outlets are changed each year: they are closed; new Outlets open; and the number of Counters in each Outlet may change. The *Outlet Change Management System* (OCMS) handles changes to Outlets once they are installed. Changes may include the following:

- Permanent or temporary closure of an Outlet
- Opening of an Outlet
- Changes to the number of Counters in an Outlet
- Changes to the address or telephone number of an Outlet

See [OCMSHLD].

OCMS provides data feeds to other applications including Tivoli and ACDB.

12.5.13.1 Structure

Component	Platforms
FTMS OCMS to UKSS Local Connection Configuration	General Purpose FTMS Gateway - Local

FTMS OCMS to UKSS Remote Connection Configuration	General Purpose FTMS Gateway - Remote
OCMS Client Application	OCMS Client
OCMS Database	OCMS Server
OCMS Server Application	OCMS Server

12.5.13.2 Functions

OCMS responds to requests from PO Ltd to vary the number or properties of Outlets. It provides facilities to close Outlets or vary the number of Counters.

12.5.13.3 Data Input

Data to drive OCMS is sent by email from PO Ltd and is entered manually via a Client interface on a dedicated Workstation.

12.5.13.4 OCMS Database

OCMS uses a Microsoft SQL Server database running on an NT Server platform. The Host Application is an SQL Server application running on this database.

12.5.13.5 Data Feeds

OCMS feeds are generated by OCMS for the following, and passed via FTMS.

- ACDB, for the generation of configuration data for new Outlets or to modify the number of Counters in existing Outlets.
- FSCS UKSS, for engineering, ISDN installation and site preparation services.
- Tivoli, for systems management, “brain building” and forwarding of configuration details to other systems.

Other data feeds are manual, using Reports generated from the database.

The sequence of data flows is as shown here.

12.5.13.6 Outlet Configuration

The number of Counters in an Outlet is known to the Riposte service within that Outlet, and hence if the number changes, Riposte must be informed. This is carried out by a task executed on the Gateway PC via Tivoli.

12.5.14 Service Level Management

Pathway has contracted to stringent service levels for many of the functions provided by Horizon. Sophisticated facilities are used to monitor these and ensure that the contractual requirements are met. Many system components log timestamps and other service level related information, and this is eventually fed to the Data Warehouse where it is analysed by the SLAM application. This has been especially developed for Pathway.

12.5.14.1 Outlet Installation

Various constraints on the timeliness of the processes involved in Outlet preparation and installation.

12.5.14.2 Data Arrival at Outlets

Reference Data, OBCS Stop Lists and AP Smart data all have associated thresholds for the times at which they should be available to Counter PCs.

12.5.14.3 Data Arrival at Clients

Data that representsthe outcomes of transactions is expected to be delivered to PO Ltd (in the case of TIP) or it's Clients by defined times each day.

12.5.14.4 Response Times

Times taken for transaction execution, especially where it involves more than one service provided, are measured and apportioned between the various service providers. SLAs define the maximum permitted average response time in each domain.

12.5.15 Time Co-ordination

12.5.15.1 Concepts

To enable consistent job scheduling, consistency in timestamps, and to avoid clock drift on the Counters, a mechanism is required to keep system clocks close to real time. See also [TIMESV].

The strategy adopted is to use two GPS *Time Servers*, one in each Campus. GPS is a satellite navigation system that is used to determine accurate locations. It does this by transmitting a highly accurate time signal, and GPS receivers calculate their position by comparing the time delays in receiving the signals from three or more satellites.

GPS receivers are now available which can receive a very accurate time from a roof-mounted antenna and broadcast it over a network using NTP.

All changes to system clocks made by these mechanisms, or for changes to and from BST, should be recorded for audit purposes. All timestamps used in Horizon should be in GMT. Where appropriate, applications should record both the GMT time and the Local time at which events occurred.

12.5.15.2 Time Co-ordination on Sequent Platforms

The clocks on the Sequent servers are co-ordinated by NTP. These UNIX-based Platforms make sophisticated use of NTP and can use several time sources concurrently, though only one is provided by Horizon. They use holistic algorithms to calculate the time at any particular server, assuming that there are network delays between it and the time sources. Times are synchronised at system boot-up. If the time is subsequently found to be out, it is "drifted back" to the correct time.

12.5.15.3 Time Co-ordination on Windows NT Servers

Windows NT servers at the Campus co-ordinate with a time service using a product from the Windows NT Resource Kit called *TimeSERV*. TimeSERV depends on a single accurate time source, which could come from a variety of sources including an SNTP server. If the time is found to be out, it is changed instantly to the correct value.

Microsoft have apparently committed to include TimeSERV in the standard W2K product, as they need it for their own Directory services

12.5.15.4 Counter PCs

The intermittent nature of the ISDN links to the Counter PCs mean that it is not possible to use the NTP protocol to co-ordinate the clocks at most Outlets with those at the Campuses.

Thus, instead, the Counter PCs have their clocks co-ordinated by a built in Riposte feature which co-ordinates them with the Correspondence Servers each time the link is opened. The Correspondence Servers themselves co-ordinate their times with the Time Server using the Windows NT TimeSERV facilities.

12.5.15.5 Time Co-ordination on Solaris Platforms

Solaris supports the same NTP protocols as Sequent.

12.5.15.6 Routers

Cisco Routers support time synchronisation using NTP.

12.5.15.7 Network Management Server

HP OpenView runs on a SUN Solaris platform which, uses the NTP protocol as described above.

12.6 OTHER SYSTEMS MANAGEMENT FUNCTIONS

Some management functions are not supported by specific management tools or infrastructure.

12.6.1 Audit Management

12.6.1.1 Management of Audit Archiving

An Audit Servicehas responsibility for handling all the long-term bulk storage requirements of Pathway. These include:

- Database archives
- File transfer archives
- Riposte message archives

A dedicated Audit Server is used, connected to a large-capacity DLT drive (or, from BI3, a Tape silo). It is managed by Legato, which keeps track of what files are held on which tapes, and can retrieve files when needed. Legato clients can run on other Platforms that have access to DLT tape drives. Thus, it is not necessary for all archived data to be transferred first to the Audit Server, so long as there is a single source of tapes.

To be useful, audit tracks must be protected from unauthorised access, especially from tampering (see [SFS] and [ACP]), and in particular from tampering by people whose actions the audit track may record. Thus, there is a need for a mechanism to verify the integrity of stored audit records and detect whether the content has been changed. This is done by the Audit Service, which adds a seal to audit tracks before writing them to bulk storage media. The seal is stored separately and may be used to verify the integrity of the retrieved file.

Local system audit file management facilities are responsible for making audit information available to the Audit Service. To do so, they must include processes to do the following.

- Create audit files of the required size with access controls as in the ACP
- Set the policy for the use of these files. For example, determine whether one file is used, or a number are used cyclically. These policies will depend upon the application. If generalised methods are used, they should accept these types of parameters.
- When a file is full or contains all necessary records pertaining to the audit period, it should be closed and renamed with a name which indicates to the Audit Service that it is available for writing to bulk storage media. If the file is not immediately available to the Audit Server or another Platform with access to the bulk storage device(s), it should be copied to one via FTMS (to provide an audit trail of its movements!).
- Delete files when they are no longer required. Implicit in this requirement is another to synchronise file deletion so that it happens only when the information has been safely transferred to the Audit Service. (It may be best if files are only deleted by the Audit Service when it knows that it has secured them to bulk storage media.)

12.6.1.2 Auditing of Systems Management

The systems management facilities provide the ability to carry out a range of critical functions. All of these need to be audited. All systems management operations need to be registered by Tivoli events that are then fed back to the central event console. This event data should be loaded into the Audit Server at regular intervals for audit purposes.

12.6.1.3 Legato Archive Management Software

Software provided by Legato is used to control audit and retrieval functions.

12.6.2 Remote Administration

12.6.2.1 Backup and Restore Operations

The Sequent product ptx/Alexandria provides database backup and restore functions for the Oracle databases located on the Host Central Servers and Data Warehouse Server. Each of these systems is provided with a 48-tape DLT Autochanger, so that databases can be restored with the minimum of operator intervention.

12.6.3 Remote Support

Some third party organisations need direct access into the Horizon systems for support purposes. They are listed here. Chapter 16 “Security” discusses the security implications of this type of access. [ACP] describes in detail the security constraints that are necessary.

There are no facilities for interactive access to the Counter PCs. Pre-configured Tivoli tasks, held under Change Control, may be used to do preconfigured diagnostics, one-off tasks and so on.

Other diagnostic processes need to be handled by pre-configured tasks wherever possible. An example is a tool to dump the Windows NT event log to a file and fetch it, thus avoiding the need for direct access to the server.

Horizon contains data that is Nationally Classified as RESTRICTED, and thus HMG impose constraints on who can see diagnostics that may contain sensitive data.

12.6.3.1 EMC

EMC require access to the live Central Host systems for support of Symmetrix discs. The disk arrays are monitored by an internal system, which regularly checks the disks against predefined thresholds such as numbers of failed read or write attempts. When a threshold is exceeded, the disk monitoring system automatically telephones the EMC support unit in Cork, Eire.

12.6.3.2 General Signals

General Signals support the communications facilities used to link the Symmetrix disk systems. EMC staff contact them should a disk problem be tracked down to the communications infrastructure. They use the same facilities as EMC to fix the problem.

12.6.3.3 Cisco

Require Telnet access to the Network to support Router problems.

12.6.3.4 Security Audit Staff

These are expected to require access to most of the systems in the Campuses.

12.7 BUSINESS APPLICATIONS AND MANAGEMENT

The existence of the systems management framework imposes certain constraints on the behaviour of applications. They must conform to overall standards for:

- Software Distribution
- Event management
- Resource monitoring

12.7.1 Software Distribution

Applications must be designed so that they can be installed unattended by Tivoli. Builds must include a software signature file.

12.7.2 Event Management

Application designs must document all possible events that can be generated. These include system errors, application errors, time-outs and thresholds exceeded. There are limits on the types of event information that Tivoli can forward. Applications must comply with this when generating events. Events must include a unique indication of the application's name and version.

12.7.3 Resource Monitoring

Applications should not assume that there is any external resource monitoring in place. If they require monitoring, they must provide a self-administering routine which takes appropriate action should the resource exceed its parameters.

12.7.4 Software Monitoring

A number of the processes discussed above are intended to ensure that only authorised software is installed on Horizon platforms. Some of these processes have been introduced only recently, and there are examples where platforms installed beforehand have been found to contain non-standard or unauthorised software.

Thus, all Platforms now include Triage monitoring sortware, which can be invoked periodically to report on the exact software state of that platform.

12.7.4.1 Structure

Component	Platforms
Triage Monitoring Client	*All NT Platforms*

12.8 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 11	Application Development	Describes the application development and Release management processes used
Next	Chapter 13	Availability	Describes the mechanisms used to ensure high levels of availability of the Horizon services.
AUTOCF	TD/DES/019	Auto-Configuration Design	Describes the design of the systems which support the Auto-configuration process
CACHECF G	TD/DES/087	CacheCfg High Level Design Specification	Describes the processes necessary to recreate the Message Store from a cached copy
CTRSHD	TD/DES/109	Counter Application Scheduler HLD	Describes the operation of the Counter Scheduler
FAILSAFE	Startup.doc	NT Fail-safe Start-up	Describes the use of a second partition on the Counter PCs, to handle fail-safe start-up should the primary partition become unusable
NFR		Non-Functional Requirements Register	Collects together all the SLAs relevant to Systems Management
RECONFIG	Reconfig.doc	Autoconfiguration Design Proposal	Describes the Reconfiguration process used as part of Auto-configuration
SWDIST	SD/DES/059	Software Distribution Framework for Operational Systems	Describes the software distribution mechanisms
TIMESV	TD/DES/030	Time Services Specification	Describes the use of the Time Server
TIVOLI	Approach.do c	High Level Tivoli Design Approach for Sorbus - Pathway Project	There is little detail of the systems management processes in the Project Library. This remains the best description of the use of the TME known to the author, though it is somewhat out of date.

Chapter 13 - Availability

13.1 SCOPE

Availability is a measure of whether an IT system is there when the users need it. Availability is achieved through a combination of factors.

- *Reliable components*, both hardware and software
- *Detectable failures*, so that a failed component is immediately detected and notified to the support organisation
- *Resilience*, so that major components are replicated or include retries and error processing to minimise the impact of failure.
- *Recovery and repair processes* that can restore a failed component or system to normal operation speedily
- *Distribution, installation and activation processes* that can be used to install and configure components remotely to fix an identified problem, or to minimise the disruption when a key component is out of service
- *Measurement techniques* that may be used to determine the overall availability of the services provided by the information system and whether these conform to agreed service levels.

13.2 STRUCTURE

The Chapter discusses the following subjects.

- The overall strategy for resilience.
- The resilience of each major system component.
- The approach taken to disaster recovery.
- Resilience in the external links to outside suppliers
- Resilience in the external systems upon which Horizon depends.

13.3 BUSINESS ISSUES

PO Ltd is totally dependent on the Horizon system to support their Outlet business. A set of SLAs is included in the CodifiedAgreement. The principal areas where these SLAs apply are as follows:

- Horizon Systems Help Desk is expected to achieve 100% availability during normal business hours, and longer given adequate notice.
- Response time requirements for on-line and batch workloads imply the need for 100% availability of links from Outlets to Campuses to PO Ltd, for those applications that require on-line access. The same availability is required of the Correspondence Servers, Agent Servers, Host Central Servers and External Interface Gateways, taken as a whole.

These factors drive Pathway into providing a highly resilient system to ensure that no single failure can have a significant impact on system availability. The rest of this section describes the particular features of the solution that provide the required level of availability.

13.4 SYSTEM RESILIENCE

The strategy for resilience is one of replication. Every major component is duplicated.

- There are two Campuses, each with a similar network configuration and set of servers. Each Campus, and all the equipment in it, is sized to be capable of running the entire workload
- Each Campus has two internal LANs, and every Campus server is connected to both LANs
- Each Campus has two discrete connections to the Energis network, with cables leaving by different routes at least 20 meters apart to avoid the "JCB effect"
- Each Campus has two or more Correspondence Servers, Agent Servers, TME Servers, VPN Servers, Campus ISDN Routers and Campus WAN Routers
- Archive data is written to Centera disk arrays at both Campuses, and stored independently
- Where there is more than one Counter PC in an Outlet, the Riposte Message Store is replicated across all of them. Where there is only one Counter PC, the PC contains two, disks, one fixed and one exchangeable, so that the message store can be recreated on a replacement Counter PC if necessary.
- All platforms are replicated across both Campuses. Thus, where there is only one instance of a Platorm at a Campus, the strategy in the event of failure is to failover the service to the similar platform at the other Campus.
- VLANs are used, crossing the inter-Campus boundary, to facilitate this. It enables a Client application to use a single IP address for its server, and this IP address can follow the server from one Campus to the other.

Here is a simplified view of this redundancy.

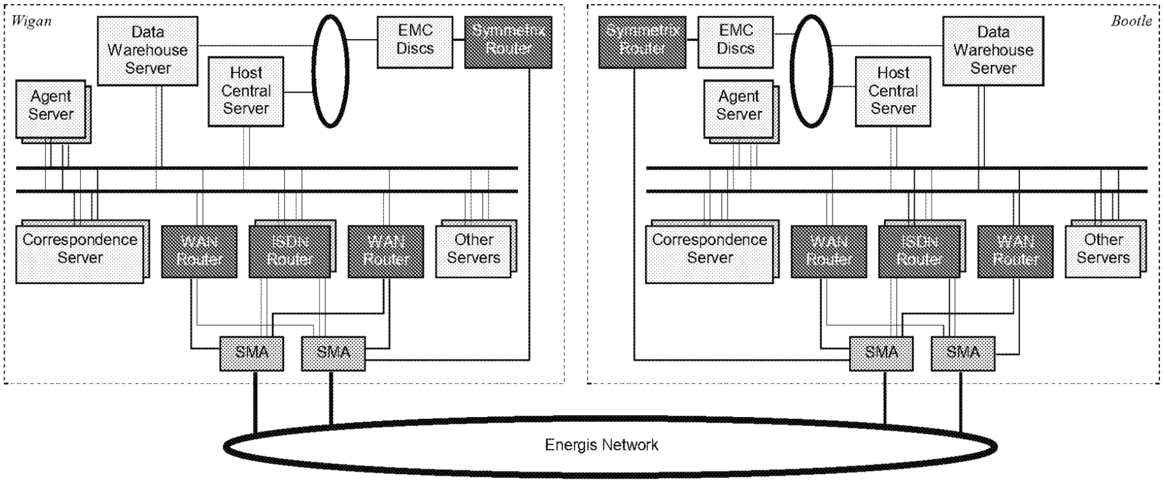

Figure 13.1 - Campus Redundancy

13.5 RESILIENCE IN SYSTEM COMPONENTS

This sub-section examines the methods used to ensure high levels of availability within each of the major Platform types used. These include the following.

- Counter Systems
- VPN Servers
- Correspondence Servers
- Agent Servers (including NBS and DCS Agent Servers)
- Host Central Servers
- Data Warehouse
- External Interface Gateways
- KMA Servers
- Auto-Configuration Database Servers
- TME Servers
- Audit Servers
- Campus LAN
- External Connections
- Firewalls
- Horizon Systems Help Desks

13.5.1 Counter Systems

13.5.1.1 Counter Resilience

A powerful, industry standard PC is used to support the Counter functionality.

Many Outlets contain multiple Counter Systems, and thus the loss of one (for example through power supply failure) does not prevent the use of other Counters.

13.5.1.1.1 Message Replication

Riposte ensures that transactions completed at a Counter are replicated both on the other Counter PCs within the Outlet, and on a number of Correspondence Servers in the Campuses. It provides for automatic recovery of transaction data. Thus if a Counter PC fails, its transaction can be completed at another Counter PC within the Outlet.

13.5.1.1.2 Resilience in Single Counter Outlets

Counter PCs in single-Counter Outlets are fitted with exchangeable hard disk units, as well as fixed disks, so that the information held on the disk can be moved to a replacement Counter PC. The new Counter PC then reconstitutes its message store from the removable disk, and continues where the old Counter PC left off. To avoid this process taking too long, a compressed copy of the message store is taken and stored on both drives each night when the desktop is reloaded. It is this squirreled-away copy that is used at first; any messages that have been added to the message store during the day are obtained by replication from the Campus.

13.5.1.1.3 Fast Spares Installation

When a spare Counter is installed in an Outlet, the default action is for it to replicate its entire message store from a neighbour. This can be a slow process. It speed is significantly increased by using a similar mechanism to that used in a single-Counter Outlet. Each Counter takes a compressed copy of its message store each night when the desktop is reloaded. When a spare is installed, it obtains a reasonably up-to-date message store from one of its local neighbours. The only replication necessary is to obtain the messages generated or received during that day.

This "squirreled" copy of the message store is also available for use if to rebuild the message store if it is corrupt or cannot be read.

13.5.1.1.4 Loss of a Complete Outlet

This could be caused by fire, flood, or theft of all Counter systems. It has two implications.

- Contingency arrangements (Foreign Encashments) exist within the applications for benefits to be paid at any other Outlet.
- Any transactions that took place within the Outlet, but have not been replicated to the Campus, will be lost. Where the equipment, rather than the Outlet as a whole, is destroyed then any outstanding transactions can be reconstituted from the tally roll records. Each of these includes the Transaction Number. When the Outlet is reconstituted, Riposte enables it to identify the last transaction number secured at each Counter. The remainder can be manually rekeyed.

13.5.1.2 Provision of Spares

Spare PCs are kept by Sorbus and can be used to replace failed Counter PCs. These spares are taken from the Celestica "production line" and hence will reflect the Build State current at that time. This Build state is likely to be out of date when the Counter PC is finally installed in an Outlet. The Auto-configuration Process described in Chapter 12 "Systems Management" brings a newly installed Counter PC up to the latest software Build state.

13.5.1.2.1 Installation of Message Store

The message store is then copied from another nearby Counter PC, using Windows NT File Copy. To enable this to happen, each Counter PC copies its message store to a second partition overnight, and this backup copy is made available as a read-only Windows NT share to the Counter PC's neighbours. The message store is copied in its encrypted state, as the same Filestore Encryption Key is used on all Counters within an Outlet. (Should this not be the case, for example because the Post Office Manager has lost his Key) then the rather slower Riposte synchronisation mechanisms are used.) These mechanisms are described in [CCFG].

13.5.1.2.2 Synchronisation of Message Store

The Riposte service is then started. It will synchronise the message store with messages generated since the overnight copy was made.

Loss of both a single Counter PC, and its exchangeable disk, is likely to be rare and is most likely to arise from theft.

13.5.1.3 Failure of Communication Link

Losing its communication link means that the Counters in an Outlet will not be able to communicate with their Correspondence Servers, and vice versa. Riposte message replication will not operate. This was not a significant issue prior to BI3. Messages are stored and only transmitted between the Outlet and the Campus when the link is established, either on a timer basis or because of the need to send a Priority Message. When the link is re-established the Campus will be brought up to date. Until it is, the Outlet will become progressively more out-of-date, and the Campuses will have no record of transactions that have taken place at Counters in that Outlet.

If the Gateway PC fails or the link itself fails, work can continue. However, certain operations that would normally make a real time connection to the Campus will time-out and the Counter Clerk will be required to make a telephone call to the Help Desk. When the PC or the link is repaired, Riposte message replication brings the Outlet and the Correspondence Servers back into line.

The Communications link must exist to enable the Post Office Manager to complete a normal POLO process.

Starting in BI3, there is an increasing number of applications that rely on the ability to contact the Campus. NBS and DCS are the first two such applications, and more will follow. In response to these, two developments have been made to the Outlet-to-Campus network.

- A *Counter Network Information Monitor* (CNIM) is introduced. This monitors the status of the link, and if it is not available displays an appropriate Icon to the Counter Clerk. It then periodically monitors the line, and removes the icon as soon as a link can be re-established.
- A new FRIACO-based data network is introduced, based upon facilities provided by Energis. This enables certain more heavily used Outlets to be permanently connected to the Campus, at least for the busy parts of the day. While this is no protection against breaks in the local loop, it will avoid the situation where the Gateway PC cannot make a connection to the Campus because of congestion within the BT network

13.5.1.4 Failure of Peripherals

13.5.1.4.1 Keyboard

Many transactions are entirely peripheral- or Touch Screen-driven, and require no use of the keyboard. However, Post Office Log On (POLO) cannot operate without a functioning smart card reader.

The Riposte Desktop can display a cut-down "keyboard", and the Counter Clerk can touch the relevant point on the screen to simulate pressing the associated key. This provides a certain degree of fallback should the keyboard be broken.

13.5.1.4.2 Screen

There is no provision to use a Counter PC without a working display. Should the display fail, it must be replaced from spares.

13.5.1.4.3 Magnetic Card Reader

Any transaction initiated by a Magnetic Card Reader Impulse has a backup action whereby the Counter Clerk can type in the card details at the keyboard or via the Touch Screen.

13.5.1.4.4 Bar Code Reader

Similarly, all transactions that take data from a Bar Code Reader also provide a fallback whereby the Counter Clerk can type in the data directly. This presupposes that the document or item containing the bar code also displays it in Arabic numerals.

13.5.1.4.5 Weigh Scales

Electronic scales generate an Impulse, containing the weight of the object on them, whenever they are used. If the scales are broken, or the link from them to the Counter Systems is out of order, the Counter Clerk can type in the weight from these or a backup (manual) set of scales via the keyboard.

13.5.1.4.6 Tally Roll Printer

Riposte includes a "print preview" facility for all reports including receipts. The Counter Clerk can use this and then copy the screen contents manually to a piece of paper. This is slow, but it works.

13.5.1.4.7 Post Master's Memory Card

The Post Office Manager needs to present a valid card during Counter PC boot-up. However, if the card cannot be read, there is a fallback procedure that enables a second (spare) PMMC to be written for future use.

13.5.1.4.8 PIN Pad

This is added at BI3, in support of NBS. There is no fallback, other than use of a different Counter.

13.5.2 Correspondence Servers

In summary:

- Correspondence Servers are replicated at each Campus
- Internal recovery features are used on the Correspondence Servers
- Riposte message replication is used to keep the Correspondence Servers in a Cluster in step with each other and with the Outlets serviced, and to bring a Server up to date following its replacement
- Mirrored Disks are used on EMC disk arrays to hold the Message Stores in case of disk fail
- Message Store Archiving is used to restrain the disk space needed
- Multiple LAN connections are used to cater for LAN or LAN card failure
- Tape Backups are taken of the Message Stores each week, and are used for recovery of all or part of a message store.

See [CSMSR] for more details.

13.5.2.1 Correspondence Server Redundancy

There are a number of Correspondence Servers at each site. Each is part of a Cluster of four Correspondence Servers, two at each Campus, which service the same Outlets. Each Cluster supports up to 5,000 Outlets.

13.5.2.2 Hardware Resilience

Compaq DL360 servers are used. These have internal recovery features including two processors that provide back up for each other. Windows NT system disks are hardware mirrored within the servers.

The Riposte Message Store data is held within the Campus's EMC Disk Array. This provides hardware-enabled disk mirroring. The EMC disks are configured in groups of 8 x 18 GB disks per Correspondence Server. EMC firmware presents these to Windows NT as 16 x 9 GB disks They are further configured as eight Windows NT stripe sets per server. Disk 1 is striped with Disk 9, Disk 2 with Disk 10 and so on. In addition to the stripe sets, there are eight disks allocated as Business Continuity Volumes and two disks configured as hot spares.

Should a disk fail, data from its mirror is automatically copied to a warm standby disk that then becomes the second plex. The failed disk is then replaced, and the replacement becomes the new warm standby disk.

13.5.2.3 Message Replication

The facilities described in Chapter 6 "Distributed Application Services" are used to replicate the RMS message store across all the Correspondence Servers in a Cluster. Four copies of the data held centrally, with two mirrors on each active Correspondence Server.

13.5.2.4 Message Store Recovery on Disk Fail

Where a complete Correspondence Server disk is lost, replication via Riposte would take too long. Thus, these disks are hardware mirrored. Hardware recovery facilities within the EMC Disk Array are used to repopulate a replaced disk from the mirror.

13.5.2.5 Message Store Recovery on Loss or Corruption

Should both plexes be lost or corrupt, recovery by replication from the other Campus would take an impossibly long time. Thus, regular backups of the Riposte Message Store are taken to tape. This is performed using the *Business Continuity Volumes* (BCVs) in the EMC Disk Array. The RMS itself is mirrored. One BCV is attached as a "third plex" to each mirror pair, and the disk array makes a copy of the mirrored data onto the BCV volume. That volume is then detached from the "parent" volumes, and copied to tape via the backup server.

If it becomes necessary to restore the disk volumes, they are copied from tape and then Riposte message synchronisation is used to bring them up to date.

This process is described in [CSMSR].

Corrupt message stores are detected by the Riposte Integrity Checker. This runs periodically on the SSC Support Server.

13.5.2.6 Message Store Recovery on Correspondence Server Fail

Where the Correspondence Server itself fails, the mirrored disks are automatically reattached to a hot standby in the same Campus. The server in the other Campus will continue servicing the work for the Cluster's Outlets while the failed Server is replaced by its hot standby. During the time that it is being configured and brought into play, the standby Correspondence Server will become out of step with the active Server.

Correspondence Servers regularly exchange Message Markers to synchronise their message stores. This process is used to bring the new server up to speed. The system being recovered does not generate any further messages until this recovery is complete.

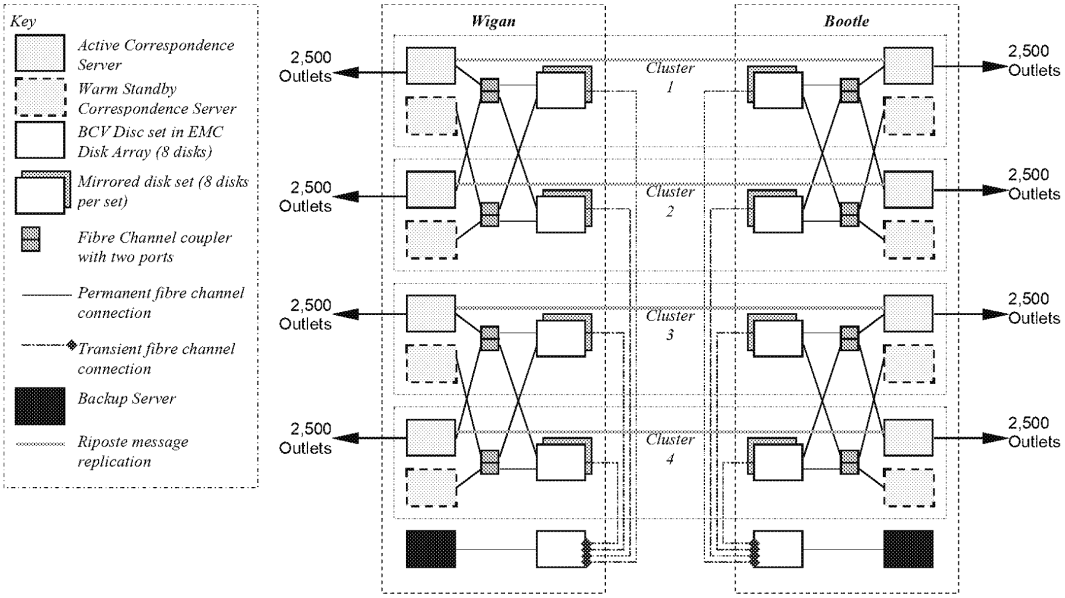
Key
Active Correspondence Server
Warm Standby Correspondence Server
BCV Disc set in EMC Disk Array (8 disks)
Mirrored disk set (8 disks per set)
Fibre Channel coupler with two ports
Permanent fibre channel connection
Transient fibre channel connection
Backup Server
Riposte message replication
Wigan
Bootle
Cluster 1
Cluster 2
Cluster 3
Cluster 4
2,500 Outlets
2,500 Outlets
2,500 Outlets
2,500 Outlets
2,500 Outlets
2,500 Outlets
2,500 Outlets
2,500 Outlets

Figure 13.2 - Correspondence Server Clusters

13.5.2.7 Message Store Archiving

Every message within the message store has an expiry period as part of its attributes. This is the number of days that the message will stay on-line in the message store. It may be set explicitly by the application that creates the message, or it may default to the system default that is set as a Riposte configuration parameter.

A Riposte background task appends expired messages to a nominated serial file and then deletes them from the message store. The file name is set as a configuration parameter and can be changed. The expired messages are written as attribute grammar text with one record per message. If the file name is null, the messages are merely deleted.

If archiving is enabled, then an expired message cannot be retrieved from Riposte even if it has not yet been archived.

Correspondence Servers have archiving enabled, to ensure that the system's disk does not fill up, but with a null archive file. Instead, a daily archive process writes all new Riposte messages to a serial file that is then written to the Centera Audit Data Repository by the Audit Service. This ensures that messages generated on the same day are stored together, and can thus readily be retrieved together, which is substantially easier for an auditor than if messages are stored with others that *expired* on the same day.

Access to the archived messages is achieved by copying them from an entire archive file back into the Audit Server and loading them into a Riposte Message Store with archiving disabled. Normal Riposte utilities can then be used to search for and retrieve specific messages.

13.5.2.8 Failure of LAN Connection

Each Correspondence Server is connected to both discrete LAN segments and can use either. Riposte is configured such that, should it fail to access a neighbouring Correspondence Server for replication it will try an alternate route which is configured to go via the other LAN card (on both systems).

13.5.2.9 Platform Resilience

Each Correspondence Server is configured with two Windows NT services, each in a separate disk partition. The first is the primary service. The second has a networking capability installed. Its functionality is limited to that required to diagnose faults on the server, and the minimum set of security software.

If the primary service is unable to start, the second may be started. The only action it may carry out is to copy various diagnostic files to an SSC server.

13.5.3 Agent Servers

13.5.3.1 Generic Agent Server Redundancy

There are a number of Agent Servers at each Campus. Each runs a number of Agent services, some interactive (running all the time) and some bulk services that are scheduled by Maestro. There is no inherent relationship between service and server, and each Agent Server contains the full range of Agent service software.

The bulk Agent software is designed to distribute the workload across the servers that are available at "start-up". If a Bulk Agent service fails then a sweep-up process at the end detects that some work has not been completed. It schedules it to one of the surviving servers. Any Oracle locks set by the failed Agent expire after an average of five minutes.

13.5.3.2 Failure of Agent Services

Interactive Agent services are monitored by Tivoli. Should a service fail, Tivoli will detect the fact and start another instance of the Agent on another Agent Server. The failure is detected by the inability to access the failed server, and so a LAN or LAN card failure as well as a server failure are all treated as server failures.

At BI3, this facility is enhanced to provide speedy failover for real-time Agents.

Each instance of a real-time Agent supports a proportion of the Outlet estate. With one Agent instance per Cluster, any failure will result in loss of service to 25% of the estate. Thus, each active Agent has a hot standby at the other Campus, and a form of "heartbeat" is used between these instances so that the standby server can take over if the active server fails. These heartbeat messages are transmitted via the Correspondence Server Riposte Message Store. Each Agent instance connects to a different Correspondence Server, so that loss of the connection between Correspondence Servers in the same Cluster will also trigger a failover.

A number of factors and resources influence the availability of real time Agents. These include:

- The availability of the Agent Server hardware, including internal cards – for example any crypto cards that may be included

- Resources external to the Agent Server platform, such as:
  - The Riposte service running on a Correspondence Server
  - Any external service such as the NBE or MA
  - The network connection to any external resource

13.5.3.3 Platform Resilience

Each Agent Server is configured with two Windows NT services, each in a separate disk partition. The first is the primary service. The second has a networking capability installed. Its functionality is limited to that required to diagnose faults on the server, and the minimum set of security software.

If the primary service is unable to start, the second may be started. The only action it may carry out is to copy various diagnostic files to an SSC server.

13.5.3.4 Agent Configurations

The diagram below shows the Campus configuration, and represents the viewpoint of a single Cluster. Each Campus on its own is capable of supporting the NBS load in a resilient way.

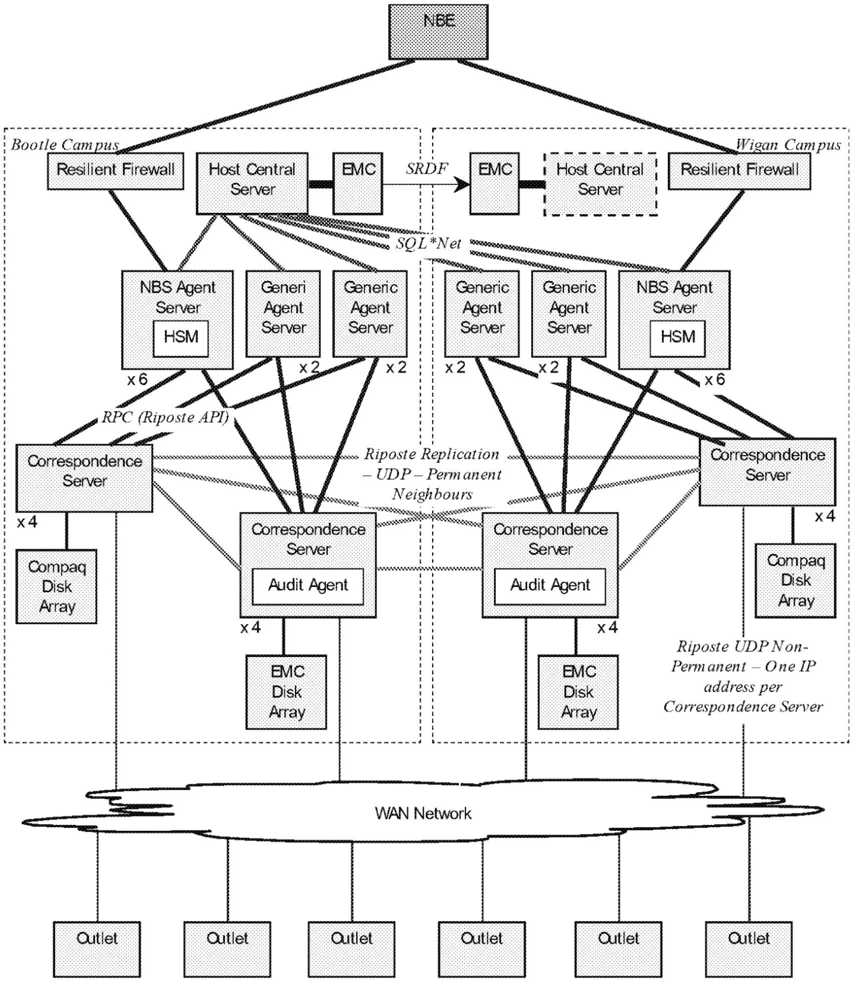

Figure 13.3 – Symmetric Campuses with Resilience on Disaster

The main characteristics of this configuration are as follows.

- There are four Correspondence Servers in a Riposte Cluster, each sharing the Outlet load equally. They are defined as neighbours in a "fully meshed" configuration
- Every Outlet has a neighbour configuration to four Correspondence Servers (a single network path to each rather than to two as at present)
- In each Cluster, all Correspondence Servers are of the same processor specification. Clusters 1 and 2 have 550 MHz systems, while Clusters 3 and 4 have 450 MHz systems. The allocation of Outlets to Clusters at the end of the Rollout is unbalanced, and this aligns the most powerful processors to the Clusters with the busiest Outlets
- In each Cluster, one server at each Campus uses EMC disks, the other uses Compaq Disks
- The audit workload is run on the Correspondence Server at each Campus that is connected to the EMC disks
- There are four Generic Agent Server per site, with two connected to each get of Correspondence Servers

13.5.4 Host Central Servers

In general:

- The Host Central Server and Data Warehouse Servers act as routine standby systems for each other
- All applications run at one Campus
- Data owned by these applications is replicated at the other Campus
- The other Campus provides a Disaster Recovery site

13.5.4.1 General

The recovery strategy for the Host Central Servers embraces recovery from two different types of failure:

There is one Host Central Server and one Data Warehouse Server at each Campus. Each comprises a Sequent NUMA-Q node. In normal use, the entire workload runs within these systems at a designated (Primary) Campus. Should either Node fail, its workload is transferred to the other Node.

In the event of a disaster situation that renders the principal Campus unusable, its entire workload is transferred to the other Campus.

13.5.4.2 Hardware Resilience

The Sequent NUMA-Q servers used to support the central systems have built in resilience features.

- There are two Nodes
- Each Node has its own power supply
- Each Node has two Quads
- Each Quad has two processors
- There are multiple connections to the Fibre channel.

The Hosts are operated from FSCS in Belfast. BMC Patrol monitors the state of the Hosts, and reports any failures to Tivoli.

13.5.4.3 Database Replication

Identical Sequent NUMA-Q Nodes at each Campus support the Host databases and applications. As well as having their own private disks, each Node is connected to the EMC Symmetrix disk array. This contains the Oracle databases used by the Host applications, the Correspondence Server message stores, and data required by a number of other Campus applications. The arrays contain two mirrored copies of each database, plus additional disks that are used for Business Continuity.

In addition, the arrays at each Campus are connected via SRDF technology over an E3 communications link. This enables each database to be mirrored at the other Campus.

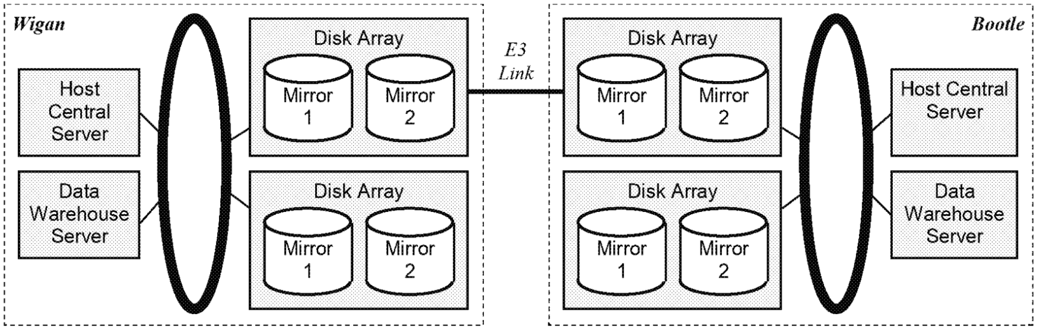

Figure 13.4 - Symmetrix Disk Replication

The SRDF technology designates one site as the master or "source", and the other as its shadow or "target". An application runs solely at its master site. SRDF ensures at the hardware level that the data is consistently updated at both the master and shadow sites. Different applications can have their masters at different sites.

This four-way mirroring is transparent to the Host Central Server. It protects the data from a catastrophic failure of a whole site. If the master site is lost for any reason, the database at the shadow site can immediately be started up. After rolling back any uncommitted transactions, it continues processing as if it were the master site, without the loss of any data.

13.5.4.4 Recovery from Local Failures

Maintaining four mirrors of the databases almost entirely eliminates the possibility of losing data through media or environmental failures. There are, however, still opportunities for operator errors or application failures to cause corruption on all four mirrors simultaneously. To ensure that recovery times are as short as possible, each database is backed up daily.

13.5.4.5 Node Failover

Should a node (or one of the Quads within it) fail, the workload is transferred to the other Node within the Campus.

13.5.4.6 Disaster Recovery

If the active Campus is lost for any reason, the live applications are transferred to the servers at the other Campus. All the live data is already available at that Campus via the SRDF connected disks.

A manual process is used, including the following steps.

- The Symmetrix disks that are designated as the “slaves” at the failover site, and hence are normally invisible at that site, must be made available to the failover system with read/write properties.
- The failover system must be taken down and rebooted. This is necessary to pick up the changed status and visibility of the slave disks.
- A different set of Maestro scheduling parameters is used, to reflect the fact that the operational workload is now running on the failover system.
- The Oracle databases are started. They will go through an Oracle recovery process that involves rolling forward the redo log, and then rolling back the database. This should not take an excessive amount of time, as all checkpoint units are small.
- All communications links used by the Host must be reconfigured to go to the other Campus. This includes the OBCS links, as well as links from the Agent Servers.

13.5.4.7 Recovery of Maestro Schedule

The current position in the Maestro schedule is replicated over the SRDF link and hence is available to the other site following failover. To avoid any risk of corruption of the schedule, it is further copied to an otherwise little-used Windows NT platform (a Domain Controller) at frequent intervals.

13.5.5 Data Warehouse

13.5.5.1 Availability Requirements

A large amount of data is gathered by the Data Warehouse each day and it would be difficult to catch up after a prolonged outage. However, the contractual requirements are not so great as those for the Host Central Servers, and thus a different strategy is adopted.

13.5.5.2 Hardware Resilience

The Data Warehouse Server is a Sequent NUMA-Q Node that is broadly similar to the Host Central Server node at the same Campus. Either Node can take over the workload of the other in the event of a Node failure. All the data needed by either Node is held in EMC disk arrays that are connected (via the Fibre Channel) to both Nodes.

In normal working, one Quad is configured to run the Data Warehouse applications (e.g. the data loaders), and the other the MIS applications.

13.5.6 External Interface Gateways

This covers the Windows NT systems used to transfer files to and from PO Ltd and its Clients and Pathway’s suppliers. They include:

- POCL TIP Gateway - Local
- POCL TIP Gateway – Remote
- Horizon Systems Help Desk Gateway - Local
- Horizon Systems Help Desk Gateway - Remote
- General Purpose FTMS Gateway – Local
- General Purpose FTMS Gateway - Remote
- Automated Payments Client Gateway – Local
- Automated Payments Client Gateway - Remote
- Network Banking FTMS Local Gateway
- Network Banking FTMS Remote Gateway

Tivoli monitors the FTMS services at regular intervals, and raises an alert if any fails. It monitors the disk space on the gateway servers once per day, and ensures that there is sufficient free space for three days worth of files.

The servers are usually configured in pairs, with one at a Campus and one at the Client. For resilience, there is one of each type at each Campus. If the live server (that in the "live" Campus) fails, the remote end can be reconfigured to use the gateway at the other Campus, with the traffic routed via the inter-Campus links.

In most cases, two servers are supplied to the remote site. The second acts as a standby in case of failure of the primary gateway. In most cases this is a cold standby, and is brought into use should the primary fail. Scripts are provided to automate the failover process.

Where needed (i.e. for TIP) it is a warm standby that constantly monitors heartbeats from the primary gateway, and automatically cuts in if the primary fails. All data is mirrored on both servers in this case.

Virus protection is provided on the External Interface Gateways.

For more information, see [FTMSRR].

13.5.7 KMA Servers

The KMA Server is replicated at each Campus. The Key Management Application data is held on the EMC Disk Array. It is thus replicated between Campuses and permits fast failover if required.

The KMA Workstations and KMS Admin Workstations that access this server will in the first instance try to access the live server. If this connection times out, they will re-connect to the standby server. The two servers are linked by a cross-Campus VLAN, and a single “roving” IP address is used by these workstations and any other clients that need to access the KMA Server. If the main server fails, the failover procedures switch this IP address to the standby site, so that reconnecting clients automatically pick up the standby server.

The KMA Database is regularly backed up by the Audit Server.

13.5.8 VPN Servers

There are multiple instances of these at each Campus. There is one VPN Exception Server and one VPN Policy Management Server at each Campus.

VPN Servers are grouped into Clusters in a way that provides both scalability and resilience to network failures. VPN Servers do not contain any persistent data, and so do not need to be backed up. Policy File data is held by the VPN Policy Management Server and fed to each VPN Server when it boots.

13.5.9 Auto-Configuration Database

One of these is installed at each Campus. Each acts as standby for the system at the other Campus. These servers run under Microsoft SQL Server, and standard SQL Server facilities are used to update each other's transaction logs on a regular basis.

The ACDB is held on the Campus EMC Disk Array, and hence is available at the backup Campus should failover be required.

The database is archived nightly. It is checked for consistency first.

13.5.10 TME Management Servers

Each TME Management Server has a backup server at the other Campus, and data is regularly interchanged between the two. In the event of a Campus failure, each backup TMR is backed off to a known point before processing re-commences.

The primary TME servers are configured to share a virtual LAN (VLAN), and the backup servers a second VLAN. These VLANs are bridged across the Inter-Campus LINK to provide high-speed data transfers between the primary and backup servers.

13.5.11 Audit Servers

Each Campus contains an Audit Server, which is responsible for auditing all the transaction information generated on that Campus. The Audit Server gathers audit information from a variety of sources, and writes it to an EMC Centera Disk Array. Loss of one Audit Server (or of its Campus) thus leaves the other Server at the other Campus. Although the data written by the two Servers is not identical, any auditable information within the system is eventually processed by both Audit Servers.

Audit data gathered but not yet secured is held in a redundant disk configuration so that a single disk failure will not result in loss of the data. Data is not deleted from the Audit Server until it has been written to tape and the tape copied to the other Server.

13.5.12 One Time Password Workstation

This is not connected to the Horizon Network. A cold standby is kept in case of failure.

13.5.13 Operations Centres

There are two operations centres located in Belfast, and each is capable of operating the Horizon network. Each includes a number of X-terminals which are used to manage the Host Central Servers, the Maestro scheduling system, the BMC Patrol system and the ptx/Alexandria tape management system.

13.5.14 Campus LAN

Each Campus contains a number of duplexed 100baseT LANs, with each plex serviced by a separate Cisco Catalyst 6500 Hub. Each major Platform within the Campus is connected to both plexes. Each will have a "preferred" plex Should this fail, connections can be re-routed via the other LAN.

13.5.15 External Connections

13.5.15.1 Campus Connections

As shown in Chapter 9 "Networking Services", each Campus is connected to the Energis Network via two discrete Fibre cables. Thus the worst effect that any single component or line failure can have is to lose half the communications links into that Campus.

With the exception of the Symmetrix link used to mirror updates to the EMC disk arrays, each connection into the Campuses is replicated with different PVCs routed via different network components.

13.5.15.2 WAN Routers

The WAN Routers are used for inter-Campus communication and communication to DSS sites and to the PO Ltd TIP sites. Two are provided at each Campus. Each is connected to the Energis SDH Network by its own E3 connection. The campus is resilient to the failure of one Router or one connection. See also [NWDES].

The Energis Network itself is "path protected" in that there are at least two paths from each node to the next, so providing automatic resilience against loss of a path.

13.5.15.3 Outlet Facing Routers

13.5.15.3.1 Campus ISDN Routers

Prior to BI2, Campus ISDN Routers provide the principal means to handle links to the Outlets. For capacity reasons, each Campus contains six of these. The ISDN primary lines from the Routers connect into the Energis SDH Network within the Campus. The connections leave each Campus through two separate ducts out of each building.

Each Campus ISDN Router has two fast Ethernet cards, each with two connections. If one of these cards fails the other will continue to work and the Router itself will continue functioning.

Each ISDN connected Outlet has a list of three phone numbers. Each number is associated with one hunting group at one Campus. Each hunting group is permanently associated with one ISDN Router. The Outlet always attempts to call the Primary number first. If this fails, then depending on the failure condition it will either reattempt the call or move onto the secondary telephone number, which is that of its "buddy" Router within the same Campus. If both calls fail (for example if the entire Campus is out of action) the fallback is to a Router in the other Campus, as shown here.

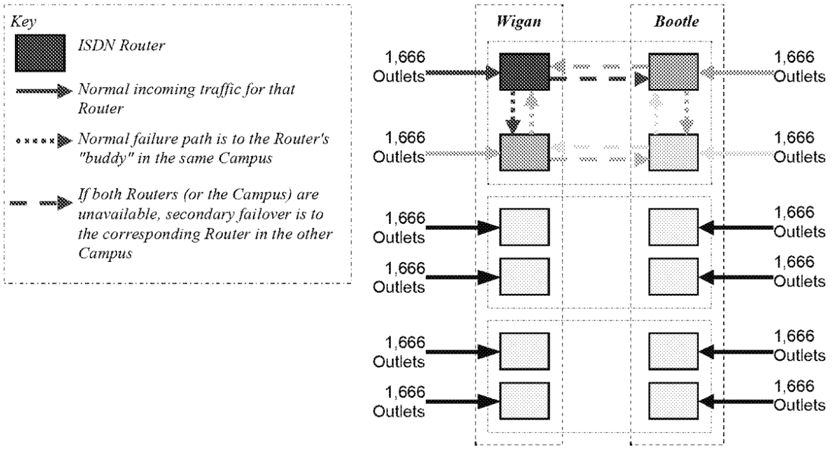
Key
ISDN Router
Normal incoming traffic for that Router
Normal failure path is to the Router's "buddy" in the same Campus
If both Routers (or the Campus) are unavailable, secondary failover is to the corresponding Router in the other Campus
Wigan
Bootle
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets
1,666 Outlets

Figure 13.5 - ISDN Router Fallback

Correspondence Servers and TME Management Servers are also configured with a prioritised set of Campus ISDN Routers to use for communication with their Outlets.

13.5.15.3.2 Frame Relay Routers

Two of these are provided in each Campus, each connected to both Campus LANs via Firewalls. Outlets connected via Frame Relay know the IP address of all four, and messages sent to the Campuses use "multicast" facilities to ensure that they arrive at both Campuses.

13.5.15.4 Gateway Routers

The ISDN and WAN Routers used to communicate with PO Ltd TIP and APS sites, and Pathway supplier sites, are not duplicated within a Campus. One is provided at each Campus, and the policy should one fail is to reroute connections via the other Campus.

13.5.16 Firewalls

Firewalls are always used in pairs. Each pair has a primary and a back up. When the Firewalls are configured, the configuration information is written to both. "State" information about the connections managed by the Firewall is also replicated in the other. When the primary Firewall fails, the back up can take over its task immediately because it has access to this state information.

13.6 Disaster Recovery

Given the overall strategy for recovery, a "disaster" is the complete loss of one of the following:

- A Campus
- All connections into a Campus
- Another major site

13.6.1 Loss of a Campus

The strategy for a disaster situation at a Campus is to move all the work to the other Campus. As described in Chapter 15 "Performance", each system component is sized on the basis that each Campus is able to carry the full peak workload.

Moving the entire workload to one Campus will require the following steps.

- If the lost Campus was running the Host applications, close down the Sequent Host at the surviving Campus, and reconfigure the EMC disks so that they are all writeable to by the Host at the surviving Campus.
- Reconfigure the Maestro schedule at the surviving Campus to run all Agents and Host applications at that Campus
- Reconfigure all network connections from remote External Interface Gateways to use the surviving Campus

Connections from Outlets automatically try the other Campus should one not respond. While this adds some seconds to the ISDN call set up time, this is allowable in a disaster situation. Energis can reroute all IP addresses and ISDN telephone numbers to the other Campus within around eight hours.

13.6.2 Loss of Connections to a Campus

In practical terms, the effect of this is the same as the loss of a Campus. The recovery strategy is the same.

13.6.3 Loss of Riposte Message Store

The RMS is the fundamental heart of the Horizon system. Any data-dependent fault that prevents access to a Correspondence Server's message store will very soon be replicated to all other Correspondence Servers in the same Cluster. Introduction of message compression could conceivably introduce such a problem. The Horizon response, should such a situation arise, is to first of all work with Escher to understand and fix the problem, and then recreate the message store from information held in the Riposte Audit Archive.

13.6.4 Loss of Bracknell Site

Two major Pathway functions are located at Bracknell:

- The CS Management Support Unit (MSU)
- Validation & Testing Rigs

The former is critical to the proper functioning of the Horizon services, as it reports to PO Ltd on the adherence to SLAs. No major servers are located in the MSU, but the workstations that are used to access the Campus servers, and generate MSU reports, are replicated at Feltham for resilience.

13.7 RESILIENCE IN EXTERNAL LINKS

The operation of Horizon is dependent on a number of communications links between Outlets, Campuses and external bodies. The resilience provided at the Campuses is discussed above. This sub-section discusses the measures taken at the external sites to provide resilience in these links.

13.7.1 OBCS$_H$

Pathway provides two Gateway WAN Routers at the OBCS ACC. Each provides a separate 2 Mbps tail into each Campus via the Energis SDH Network, with a CIR of 1 Mbps and peak of 1 Mbps. Under normal operation, both links feed into the Campus where the Host applications run. Under fail-over, these links are re-routed to the other Campus. The Routers form a “spanning tree” bridge and will automatically switch to an alternate in the event of failure of the primary Route Bridge. The Routers themselves are managed by HP OpenView using SNMP over IP, and any problems detected are raised as Alerts that are passed to Tivoli.

13.7.2 TIP

There are two WAN Routers at the PO Ltd TIP site. These feed separate 1 Mbps tail into the Energis SDH Network. Under normal operation, both links feed into the Campus where the TPS application runs.

13.7.3 Automated Payment (AP) Data

An ISDN card is provided in each remote APS Gateway. It can communicate with either Campus.

13.7.4 Support Centres

Each Campus is connected to two or more FSCS Support Centres. Operations Centres are in Belfast and Stevenage. Management Centres are in Stevenage and Lytham St Annes.

There are two Routers at the major support and operational sites, one at the others (such as Feltham) where the resilience requirement is lower.

13.8 Resilience in External Systems

13.8.1 DSS VME Systems

The OBCS system runs on a multi-node Fujitsu VME server owned by DWP and managed by EDS. Most traffic between the DSS and Horizon systems is via File Transfer. A BMC Patrol proxy knowledge module running as an ADI service on the OBCS systems monitors the status of the file transfers and reports to the central Patrol console if problems are encountered.

13.9 Further Reading

Ref	Document	Title	Comments
Previous	Chapter 12	Systems Management	Describes the Systems Management facilities used
Next	Chapter 14	Usability	Describes the methods used to ensure high levels of Usability
ACSRR	TD/DES/094	Agent and Correspondence Server Resilience and Recovery	Describes the methods used to ensure resilience at the Agent and Correspondence Server layers

		at Release 2+	
CAOR&R	TD/DES/050	CAPS and OBCS Access Service Interfaces - Resilience and Recovery for Release 2	Describes the methods used to ensure resilience in the OBCS services
CCFG	TD/DES/087	CacheCfg High Level Design Specification	Describes the mechanisms used to install a new Counter PC's message store from other Counters in the Outlet.
CSMSR	TD/DES/086	Correspondence Server Message Store Backup and Recovery for Release 2	Describes the mechanisms used to take backup copies of the Correspondence Server message stores at regular intervals, and to recover from these backups should it become necessary.
FTMSRR	TD/STR/007	FTMS Resilience and Recovery Strategy for CSR+	Describes the mechanisms used to secure the transfer of files to and from PO Ltd, PO Ltd's Clients and Pathway's suppliers
NFR		Non-Functional Requirements Register	Intended to Include the detailed SLAs for resilience and recovery. Some are there, but there are significant gaps.
SCO	TD/DES/048	Riposte Mirroring for Single Counter Outlets at Release 2	Describes the use of exchangeable disks in a Single Counter Outlet

Chapter 14 - Usability

14.1 Scope

This Chapter covers the *usability* of the Horizon systems. Usability is a measure of the degree to which users can achieve specified goals in a particular environment with effectiveness, efficiency and satisfaction. In this definition:

- *Effectiveness* is a measure of the accuracy and completeness of the goals achieved
- *Efficiency* is a measure of the resources such as time, money and human effort used to achieve these goals
- *Satisfaction* is a measure of the physical comfort and subjective acceptability of the system to its users and to other people affected by its use.

These measures can be analysed further as shown here.

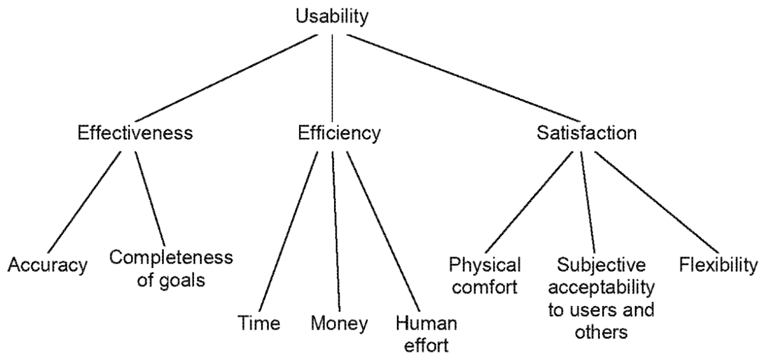

Figure 14.1 - Measures of Usability

There is a further measure of Usability. Horizon is a complex system and can be relied on to throw up complex problems on occasion. To achieve the high levels of SLAs contained in the Codified Agreement, Pathway's support organisations must be provided with safe but effective support tools and facilities to enable them to diagnose and fix problems as quickly and safely as possible.

14.2 Counter Systems

14.2.1 General

Usability is an important aspect of the Counter PCs.

- They support colour Touch Screens and provide an intuitively discoverable HCI for access to the Counter applications
- A special financial keyboard is provided to support data entry where this is more convenient than Touch Screen operation
- Tokens such as swipe cards or Smart Cards cause the associated applications to be entered automatically, without the Counter Clerk needing to press a Button
- Sessions may easily be transferred to another Counter PC
- Shared peripherals (such as weigh scales) reduce the space taken up on the Counter by the Horizon systems, and thus avoid a feeling of crowding in the Outlet
- The Riposte *MemoView* facility is used to broadcast messages to all Outlets or a Group of Outlets

Chapter 8 "User Interface" discusses these and other aspects of the Counter PC User Interface in more detail.

14.2.2 End User Help

There are two types of help available at the Counter.

14.2.2.1 Bubble Help

This is activated by pressing an "information" icon before touching the Button for which help is needed. This help appears next to the Button in question as a pop-up bubble containing the help text (in English only).

Bubble help is an attribute of the Button and is held within the Persistent Object that defines the Button.

14.2.2.2 Extended Help

This is activated by touching an "i" character within the Bubble Help. It uses HTML pages that can be displayed using Microsoft Internet Explorer. The pages can contain text or graphics and can link to other pages, in the conventional HTML manner. The Uniform Resource Locator *(URL) of an entry page is held as an attribute of a Button in a Riposte Persistent Object. Access to these pages is policed by Riposte, which passes the HTML request on to the Internet Explorer. The HTML pages are cached as local files on each Counter. Updates from changes made to the central Web server are managed by Riposte. No Browser access outside of the Counter filestore is possible, and no access is possible to pages not declared within Persistent Objects. There is no connection from Horizon to the Internet.*

A web server will be established at each Campus, with tools to administer these HTML pages. Completed pages are distributed to Outlets via Tivoli.

14.2.2.3 End user training

14.2.2.3.1 Training Mode

The Riposte Desktop contains a "Training" Button. This allows the user to enter Training Mode.

Training mode uses a separate Riposte message store on each PC. These message stores are pre-populated with a set of messages corresponding to training transactions. This is achieved by copying all Persistent Objects from the "real" message store on the PC.

Selection of Training Mode switches Riposte to use this separate message store. The fact that a Counter PC is in Training Mode is indicated by a different coloured screen background (Puce instead of Green).

Applications are expected to operate as normal, without knowing that they are using the training message store. However, there is a Riposte API that they can call, if required, to determine if they are running in Training Mode or not. This feature would be used to bypass on-line connections etc.

14.2.2.3.2 Populating the Training Mode Database

Riposte only allows the application to access one message store at a time. Hence, all Persistent Objects and other messages required to support the Counter applications when in Training Mode have to be included in each of these Training message stores. Mechanisms are provided to populate the Training message store when Training Mode is first entered after switch on. Riposte copies all the Persistent Objects from the live message store to the training message store. Some of these Persistent Objects contain "wrapped" training data that is then extracted by a specific Pathway developed "training" application.

This initialisation can be repeated whenever a user wants to restart a particular piece of training. Normally the message store will retain its previous content, which allows users to continue training with the data in the same state as where they last left off - their position within the application is not remembered.

14.2.2.3.3 Factors Concerning Training Mode

Some messages, in particular End of Day markers, must be written to the main message store rather than the training message store, even if the Counter PC is in Training Mode at the time the marker is generated.

14.3 SYSTEMS SUPPORTABILITY

There are three ways in which the Horizon system can be designed to be "supportable".

- Provide adequate support tools to the System Support Centre (SSC)
- Build diagnostic tools into the major system components.
- Build error management into all Pathway supplied software.

Note that the ability to fix problems "on the fly" must never be a substitute for fixing the *cause* of the problem.

14.3.1 SSC Support Requirements

14.3.1.1 General

Support Guides are needed for all major services and other significant aspects of the system. These are produced by the Development Units, and updated at each significant Release.

14.3.1.2 Host Systems

- Access to Oracle databases in read-only mode via Discoverer 2000
- Read access to support logs
- Ability to patch database problems via suitably audited scripts

14.3.1.3 Windows NT Systems

- Read-only access to NT Registry settings

14.3.2 Diagnostic Tools

Appropriate diagnostic tools will be installed on all appropriate platforms, especially Counter PCs where the cost of a site visit to fix a problem could be prohibitive.

14.3.2.1 Counter PCs

Counter PC diagnostics should include aspects such as the following. In general, where standard system facilities do not provide the required level of information, pre-prepared Tivoli scripts should be used.

- ISDN call failures and call durations
- Instances of and reasons for reboots
- Riposte message failures
- Integrity of executables
- Symbol files for dump analysis

In addition, facilities should be provided to enable simple system testing (such as CLIP dialback) during Counter PC installation.

14.3.2.2 Windows NT Servers

Symbol files should be included in the builds for these, so that dumps can be analysed.

14.3.2.3 ISDN Routers

There is a need to be able to monitor ISDN call rates and failure rates.

14.3.3 Error Management

All code developed by Pathway should be designed on the principle that things will go wrong. Error management must be an integral part of any procedure.

14.4 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 13	Availability	Discusses the architectural mechanisms that ensure a high level of Availability
Next	Chapter 15	Performance	Discusses the methods used to ensure a high level of throughput and response times
ACDBSUP	DE/SPG/002	AutoConfig Downloader/Listener Support Guide	
APSSUP	AP/DOC/003	APS Support Guide	
CNTSUP	SY/MAN/004	Steady State Counter	

		Management Support Guide	
EPOSSSUP	EP/MAN/001	EPOSS Operational Support Guide	
FTMSSUP	TD/MAN/015	FTMS Support Guide	
ISDNSUP	DE/SPG/001	ISDN Call Monitor Support Guide	
KMSSUP	RS/MAN/012	KMS Support Guide for SSC	
LFSSUP	LF/MAN/001	Logistics Feeder Service Systems Management Support Guide	
LIFT	D06A-9999-B057/01	Financial Keyboard Specification	Describes the specification of the Counter PC keyboard
MISSUP	DW/PRD/123	CSR+ DWh: Operational Support Guide	
NBSSUP	TD/MAN/020	Network Banking Support Guide	
OBCSSUP	OB/MAN/002	OBCS Operational Support Guide	
PCCSUP	DE/SPG/005	AutoConfig PCConfig Products Support Guide	
RDMSSUP	RD/MAN/006	RDDS Host System Support Guide	
SSHSUP	DE/SPG/003	OpenSSH Auditing and Logging Server Support Guide	
STYLE	SD/STR/001	Pathway Horizon Office Platform Service Style Guide	The Riposte style guide
TIMSUP	SY/MAN/001	Time Services Support Guide	
VPNSUP	RS/MAN/009	VPN Operational Support Guide	

Chapter 15 - Performance and Scalability

15.1 Scope

Performance is a measure of the rate at which a system is able to perform useful work, its *throughput* and the responsiveness with which the results are presented. It is thus a key measure of the ability of Horizon to meet the SLAs negotiated with PO Ltd.

In engineering terms, the combination of *measurement* of performance, with *scalability* of the system components gives us a measure of *predictability* that enables Pathway to manage risk.

This Chapter thus considers the performance of Horizon, in terms of its capacity, response times, scalability and ability to carry out the required workload expressed in terms of capacity, response times and scalability. It discusses the defined workload, and provides justifications for the numbers, sizes and configurations of the systems described in Chapter 10 “Platforms”.

15.2 Structure

The Chapter discusses the following subjects.

- The Business Issues surrounding the performance required
- The approach taken to performance analysis
- The Business Volumetrics supplied by PO Ltd
- The Derived Volumetrics calculated from these by Pathway
- The Key SLAs which must be met
- The performance modelling and measurement strategy
- The system capacity of the system, including the scaleability of the major components
- The performance in fall-back mode, i.e. following the loss of a Campus
- The major response time requirements

15.3 Business Issues

Pathway must provide Platforms and network components of sufficient size and capacity to meet the agreed functional requirements and business volumes, and exceed the SLAs. To obtain this balance, and provide only the necessary and sufficient Platform capacity, Pathway adopts a combination of empirical projections based on measured capacity, coupled with performance analysis and modelling in critical areas.

Empirical projections are used for the bulk of the expected workload. Performance Engineering is used in critical areas of performance or capacity. It depends on a precise understanding of the behaviour of the system and its users, as well as on agreed Volumetrics. In a new system such as Horizon, it takes some time for this understanding to arise, and it is only cost-effective to acquire it in the most critical areas. Even then, it may vary. Users often change their behaviour as they get used to the system and the degrees of freedom it affords them. A good understanding of the Volumetrics and user's behaviour patterns can give Pathway's technical management access to a detailed understanding of the behaviour of the system under stress. This will be invaluable as the business requirements develop, for example in making a risk assessment as to whether a particular new application will need new kit, or whether it will run adequately on what is already in place.

15.4 PERFORMANCE ANALYSIS IN HORIZON

15.4.1 General

Complex IT systems do not deliver the required levels of performance by accident. Performance is "designed in" from the outset. This Chapter outlines the performance engineering techniques used during the development of the system.

More information is provided in [PERFOV].

15.4.2 The Approach to Performance Engineering

The approach taken is to analyse the system requirements, which are described in a structured way in the other Chapters in this Document and in the volumetric statements given in [BUSVOLS]. A number of performance models are derived. Input to these models is taken from a number of sources:

- Business Volumetric information derived from the Codified Agreement
- System Volumetrics derived from the Business Volumetrics. An example is peak throughput loading on the services, and Riposte message sizes and amounts based on transaction volumes
- Measurement data taken from live Outlets
- Measurements made by PO Ltd on their existing systems
- The Key SLA figures which must be exceeded

Issues which arise from the analysis of this information, or from the output from the modelling tools, or from system measurements, are fed into the Architecture enhancement process or (if urgent) into specific design enhancements for future Releases. The design, modelling and measurement processes are iterative, the objective being to derive the most effective solution to deliver the requirements.

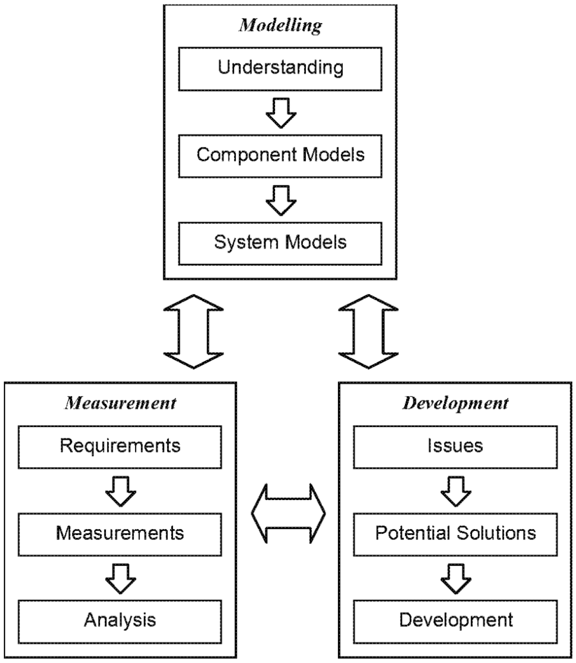

Figure 15.1 - Performance Modelling and Analysis

Three main areas of activity are identified.

15.4.2.1 The Modelling Process

This predicts whether the system can deliver against the requirements for throughput and responsiveness for a given workload. It includes consideration of the following.

- *The business model* - the business volumes specified by the Customer
- *The workload model* - the derived peak volumes
- *The service model* - the implementation model of the system
- *The throughput model* - the throughput of each component of a service
- *The resource model* - the resources used by each component of a service.

Sizing activity estimates the resources required to process each of the important workload components.

The models allow "what if" questions to be answered across the system. This enables Pathway to plan changes in configurations that are required to support workload growth or changes.

The process of developing understanding, building component models, and extending these to produce system models will continue throughout the life of the project as requirements change, new measurements are made available, and new business applications are added to the system.

Horizon is a complex system, and there is a complex set of relationships between some of the raw business data and the impact on the capacity of the major system components. Some (but by no means all) of these are shown here.

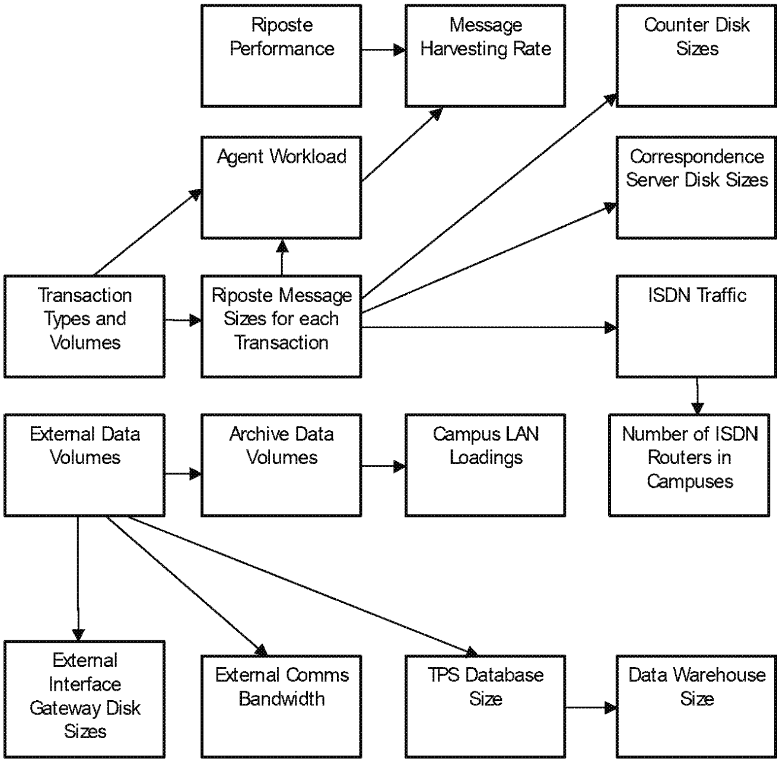

Figure 15.2 - Typical Capacity Dependency Matrix

15.4.2.2 The Measurement Process

This is used to test the assumptions used in building the models and to verify their scalability; to populate them; and to provide detailed calibration for them. Some of the values in the dependency matrix, for example, can only be derived by measurement. A *Performance Management Service* (PMS) is used to measure the performance of critical aspects of the system. Measurements are taken of important component and system performance variables, and fed back to a central Performance Management Server. The result of each measurement is analysed and evaluated and where necessary the models are updated in-line with the measurements. A major aspect of the measurement process is to identify any discontinuities in the performance of key system components. This process is repeated as the project progresses, as new Releases of code are received and the measurement requirements are clarified, for example as a result of modelling work.

15.4.2.3 Performance Development

This process takes performance metrics coming out of modelling and measurement work, and evaluates potential solutions. Those considered most effective for addressing the performance requirements identified are then developed, and can be fed into the measurement process for evaluation. This process is repeated as new versions are measured and more issues arise from the measurement and modelling work.

15.4.2.4 Performance Modelling Outputs

The modelling process produces a set of documents describing Horizon in a structured way that allows the system to be modelled. This approach to this modelling work is discussed below.

15.5 BUSINESS VOLUMETRICS

This sub-section summarises the volumetric requirements on Horizon at BI3 and beyond.

15.5.1 Source of Volumetric Information

[BUSVOLS] specifies the Business Volumetrics used for performance engineering prior to BI3, and [BUSVOLSN] the new volumes added by support of NBS and DCS. This Chapter summarises some of the key Volumetrics. These have been chosen to clarify the shape of the workload and identify some of the key capacity indicators.

15.5.2 Transaction Types

Transactions occur at a number of levels.

- Batch transactions between Horizon and PO Ltd and its Clients
- Batches of transactions between the Outlets and the central systems
- Real-time transactions from Counters to the central systems and beyond

15.5.3 Counter Transactions

Counter transactions are made up of the following.

- Benefit payments (OBCS)
- EPOSS and AP transactions

In each case, figures are provided for the total yearly volumes of transactions. Figures for the peak week, day and hour are extrapolated from these using additional data about workload patterns supplied by PO Ltd and estimates agreed with them.

It is particularly important to assess these peaks, as a major part of the on-line volumes arise from benefit payments. These are predominantly paid on Mondays and Thursdays.

15.5.3.1 OBCS Transactions

OBCS usage is expected to decline over the next two years as NBS replaces it as the way benefit payments are made. For this reason, the Design Volumes are set at the Historical Peak and no additional contingency is allowed. The Historical Volumes are taken from actual volumes for the Peak Month, Peak Week, Peak 2 Days and Peak Day. For Peak Hour and Peak 5 Minutes the Historical volumes are calculated from the Peak Day and a known profile.

Volume	Historical Peak	Design Volume
Peak Month	58,548,437	58,548,437
Peak Week	15,038,246	15,038,246
Peak 2 Days	8,144,758	8,144,758
Peak Day	4,718,625	4,718,625
Peak Hour	1,151,345	1,151,345
5 Minutes (Per Sec)	380	380

Table 15.1 - Benefit Payment Transaction Numbers

15.5.3.2 EPOSS Products

EPOSS Product volumes have been fairly consistent over the last two year and are not expected to grow significantly in the future. The Design Volumes are set at 20% above the Historical Peak.

The Historical Volumes are taken from actual volumes for the Peak Month, Peak Week, Peak 2 Days and Peak Day.

For Peak Hour and Peak 5 Minutes the Historical volumes are calculated from the Peak Day and a known profile.

Volume	Historical Peak	Design Volume
Peak Month	100,195,596	120,234,715
Peak Week	33,637,564	40,365,077
Peak 2 Days	14,876,498	17,851,798
Peak Day	8,192,874	9,831,449
Peak Hour	1,171,581	1,405,897
5 Minutes (Per Sec)	328	394

Table 15.2 - EPOSS Transaction Numbers

15.5.3.3 APS Transactions

APS is growing at around 10% per year (compound). The Design Volumes are set at the expected volumes in March 2005, with an additional 20% contingency. This gives a Design Volume 52% higher than the Historical Peak volumes. The Historical Volumes are taken from actual volumes for the Peak Month, Peak Week, Peak 2 Days and Peak Day. For Peak Hour and Peak 5 Minutes the Historical volumes are calculated from the Peak Day and a known profile.

Volume	Historical Peak	Design Volume
Peak Month	32,001,334	48,642,028
Peak Week	9,064,479	13,778,008
Peak 2 Days	4,430,096	6,733,746
Peak Day	2,387,065	3,628,339
Peak Hour	441,607	671,243
5 Minutes (Per Sec)	141	215

Table 15.3 – APS Transaction Numbers

15.5.3.4 Settlement Transactions

Settlement transactions are generated when the customer session is settled. They record the payment of cash to the customer or the receipt of cash or cheque by the outlet. All Settlement volumes are estimates, as historical volumes are not available. The formula used is that for each product sold (APS, OBCS or EPOSS) generates 0.6 settlements (i.e. for each Settlement there are 1.7 products sold).

Volume	Historical Peak	Design Volume
Peak Month	114,447,220	136,455,107
Peak Week	34,644,173	41,508,798
Peak 2 Days	16,470,811	19,638,180
Peak Day	9,179,138	10,907,047

Peak Hour	1,658,719	1,937,090
5 Minutes (Per Sec)	509	593

Table 15.4 – Settlement Transactions

15.5.3.5 LFS

LFS is a low volume service to support stock and cash ordering in the outlets. For this reason, only the Peak Day numbers are appropriate.

There are a number of different components for LFS. These are covered separately in the table.

Peak Day Volume	Historical Peak	Design Volume
Planned Orders	17,050	20,000
Advice Notices	Not Used	10,000
Pouch Collection	3,506	10,000
Pouch Delivery	6,407	20,000
Cash Declaration	17,313	20,000
Stock Declaration	17,050	20,000

Table 15.5 – LFS Transactions

15.5.3.6 NBS Transactions

NBS is a new service at BI3. The load generated on the Horizon infrastructure by NBS is significantly different to that of the Existing Service workload, in that every transaction generates a real-time message to the Campus.

The rate of growth of NBS is driven by:

- The take-up rate of the service by personal banking customers
- The rate at which CAPO™ cards are be issued and the number of such cards
- The replacement rate of benefit payment books by cards

PO Ltd. has predicted the future workload volumes but the process for the introduction of infrastructure capacity recognises that there are variables in the workload volumetrics and allows for planned change though the Capacity Management Service. The volumes are expected to increase in phases, and at full take-up to be as follows.

Volume	Contracted Volume	Design Limit	Scalability Threshold	Contracted Notice Period	Design Limit Notice Period
Peak Month	41,847,560	50,217,072	62,771,340	3 months	9 months
Peak Week	10,960,032	13,152,039	16,440,049	3 months	9 months
Peak 2 Days	5,656,759	6,788,111	8,485,138	3 months	9 months
Peak Day	3,264,181	3,917,017	4,896,271	3 months	9 months
Peak Hour	694,976	833,971	1,042,464	3 months	9 months
5 Minutes (Per Sec)	222	267	334	3 months	9 months

Table 15.6 – NBS Volumes

15.5.3.7 Debit Card System (DCS) Transactions

DCS is introduced at S30 and enables customers to pay by debit card as well as or instead of cash or cheques. It is predicted that the customer behaviour that determines the distribution of DCS payments over the day will be similar to that for EPOSS transactions.

The key difference between EFTPoS and other services is that Saturdays are expected to be significantly busier than weekdays. The predicted Saturday peak results from a series of variable events occurring on the same day e.g.:

- Month end resulting in a significant increase in MVL payments and
- Large utility companies issuing quarterly bills

The full volume workload is expected to be as follows.

Volume	Contracted Volume	Design Limit	Scalability Threshold	Contracted Notice Period	Design Limit Notice Period
Peak Month	4,210,000	5,052,000	6,315,000	3 months	9 months
Peak Week	1,264,768	1,517,721	1,897,152	3 months	9 months
Peak 2 Days	565,949	679,139	848,923	3 months	9 months
Peak Day	288,425	346,110	432,637	3 months	9 months
Peak Hour	79,368	95,242	119,052	3 months	9 months
5 Minutes (Per Sec)	22	26	33	3 months	9 months

Table 15.7 – DCS Transactions

15.6 DERIVED AND SYSTEM VOLUMETRICS

This Section lists the key system Volumetrics, in terms of expected peaks, which flow from the business Volumetrics listed above based on the system architecture.

15.6.1 Real Time Counter Traffic

This is defined as those messages travelling to and from Outlet Counters, where the Counter Clerk has to wait for a response. This usually arises from a requirement to authenticate the transaction before it can be completed. Full target volumes are derived from the sum of the NBS and DCS workloads listed above.

The impact of these transactions on the Counter to Campus network depends on the type of network connection. As described in Chapter 9, significant enhancements are made to this network at BI3 to support a major increase in real-time transactions. The network is designed to be easily scalable by moving more Outlets onto fixed connections as the workload increases. The driving factor is that there is a limit to the ISDN call attack rate that the network can support, and the number of dial-on-demand connections must not exceed this limit. Since fixed connections are more expensive than dial-on-demand ones, there is a straight trade off between the network capacity and the network cost.

15.6.1.1 Outlet Types and Constraints

The network design supports the following Service types.

- *Satellite Connected Outlet* - Supports around 250 Outlets
- *Bronze Outlet* - Uses a "connect on demand" technology to establish an ISDN connection when an online transaction occurs
- *Silver Part-time Outlets* - During limited defined hours, the ISDN line is kept open. Outside these times, a "connect on demand" service is used. There are two types:
    - Type A - ISDN Line kept open 08:30 to 10:30 Monday, 08:30 to 09:30 Tuesday and 08:30 to 09:30 Thursday.

- Type B - ISDN Line kept open 08:30 to 12:30 Saturday

- *FRIACO Silver Daytime Outlets* - During daytime hours (08:00 to 17:30 Monday to Friday and 08:00 to 13:00 Saturday), the ISDN line is kept open. Outside these times, a "connect on demand" service is used
- *Non FRIACO Silver Daytime Outlets* - the same as d) but in a geographic area not covered by FRIACO
- *FRIACO Silver 24 Hour Outlets* - The ISDN line is kept open 24 hours per day, 7 days per week
- *Non-FRIACO Silver 24 Hour Outlets* – as above but in a geographic area not covered by FRIACO

15.6.1.2 Volumes

The maximum On-line Transaction rate (i.e. for NBS and DCS) that can be supported by the dial on demand network is calculated by taking the maximum 5 minute Dialled Transaction rate that the network can support and subtracting an allowance for OBCS Foreigns. The allowance needed for OBCS foreigns is calculated as the product of:

- 2% (maximum OBCS foreign workload as a proportion of the whole)
- 5 minute volume for OBCS (this declines as NBS replaces OBCS)
- The % dialled workload (which declines as more outlets are made Silver).

The maximum Dialled Transaction rate varies by time of day (and day of week), as allowance needs to be made for other causes of ISDN calls including regular Riposte connections and systems management functions (e.g. software distribution).

The volumes that can be supported are defined below.

Volume	Contracted Volume	Design Limit	Scalability Threshold	Notice Period	Design Limit Notice Period
5 Minute Total Online Transaction Rate/sec	226	272	339	3 months	9 months
5 Minute Dialled Transaction Rate - Period 1/sec	13.5	13.5	13.5	N/A	N/A
5 Minute Dialled Transaction Rate - Period 2/sec	10	10	10	N/A	N/A
5 Minute Dialled Transaction Rate - Period 3/sec	5	5	5	N/A	N/A

Table 15.8 – Outlet Network Capacity

The three periods are defined as:

- Period 1 - Monday to Saturday 08:30 to 10:30. During this period, the number of calls made by causes other than Dialled Transactions is designed to be low.
- Period 2 - Monday to Saturday 08:00 to 08:30 and 10:30 to 17:30. During this period there may be regular Riposte connections but the calls caused by Systems management functions is designed to be low.
- Period 3 - All other times. During this period there may be regular Riposte connections and / or calls to support systems management.

Note as it is not possible to the Contracted Volumes or Design Limits for the 5-Minute Dialled Transaction Rates, no notice period is given.

15.6.2 Riposte Volumes

Based on figures in [BUSVOLS], and the design of the principal applications, and the retention periods for record types, the size and number of record types held within the Riposte message store are as shown in the following Table.

Message Type	Volumes		Riposte			TIP Interface		
	Average	Peak	Msg Size	Volumes (GB)		Msg Size	Volumes (GB)	
				Averag e	Peak		Averag e	Peak
EPOSS Product Line	5,080,700	8,689,420	570	2.90	4.95	134	0.68	1.16
AP Product	699,301	884,615	820	0.57	0.73	174	0.12	0.15
EPOSS Settlement	6,225,078	9,951,908	570	3.55	5.67	134	0.83	1.33
Cash Accounts	531,818	0	400	0.21	0.00	44	0.02	0.00
Stock Holding	709,091	0	400	0.28	0.00	75	0.05	0.00
TOTAL	**28,743,358**	**51,099,535**		**17.87**	**33.25**		**2.33**	**3.91**

Table 15.9 - Riposte Message Volumes

Based on these figures, it is calculated that at steady state the message store will hold 410 million messages. These are replicated across each Correspondence Server node. Based on the following assumptions, this equates to 160 GB of filestore per node.

- Full set of indexes
- 3:1 compression ratio
- 70% maximum fill factor
- Persistent objects

It excludes messages generated by Foreign Encashments, and a 10% Windows NT disc allowance.

15.6.3 Batch Derived Volumetrics

15.6.3.1 Batch interfaces to PO Ltd

There are three interfaces between Horizon and PO Ltd. The data volumes on these are shown below. Note that these are *derived* figures, based upon the design of Riposte and the Counter applications, and on a knowledge of the number of records generated for each transaction type.

Interface	Peak records/day	Notes
Horizon to TIP	50M	This includes the basic transactions, the payment record and is scaled by 3 to allow for the peak on the last Thursday of each month
Horizon to PO Ltd for AP Clients	2M	
PO Ltd Reference Data to Horizon	70K	

Table 15.10 - Peak Batch Volumes to PO Ltd

15.6.3.2 Audit Volumes

The main factor controlling the space taken up by audit data is for how long it must be stored. Audit data is generated for two purposes.

- To prove or disprove that an event has happened. That event may be benign or malevolent, but has to be investigated and cleared before the relevant data is deleted. From BI3, audit data relating to NBS must be retained for fifteen years
- To enable analysis of the normal behaviour of the system. [ATFS] states that this type of data must be retained for 19 months minus one day

The following are overestimates where no detailed data is available.

15.6.3.2.1 Data Volumes

15.6.3.2.1.1 File Transfers

File transfers in and out of Horizon are expected to average about 5 GB a day and peak at 10 GB per day. Control files are negligible in comparison with this and may be ignored.

15.6.3.2.1.2 Host and Agent Transaction Records

This is also expected to average around 5 GB and peak at 10 GB per day. This covers OBCS and TPS only.

15.6.3.2.1.3 Riposte Messages

Identified new Riposte messages average around 17.9 GB per day, and peak at 33.3 GB. These figures exclude a number of message types such as card events and Login/Logout. These are currently unquantified but can be expected to add around 10% to these figures, giving an average of 19.6 GB and a peak of 36.6 GB per day.

15.6.3.2.1.4 Tivoli Events

No information is currently available. It needs to be derived from the policy for Windows NT event log collection. As a raw guess, we have allowed an average of 1 GB and a peak of 2 GB or archived Tivoli messages.

15.6.3.2.2 Analysis of Data Volumes

These figures give an average of 30.7 GB per day, and a peak of 58.5 GB per day, of archive data. These volumes are substantial. If data needs to be kept for 18 months, it amounts to around 13.2 Tb of data in total at steady state (78 weeks x 5.5 days x 40 GB)

15.6.3.3 MIS Volumes

These are derived from [MISARCH].

Data feeds to the MIS peak at around 12 GB per day. This must be processed between the time that operational systems have finished their overnight processing, and 08:00.

15.7 KEY SLAS

This sub-section summarises the key SLAs contained in the Contract and the impact that these have on the sizing of the system. The complete set of SLAs is contained in a number of documents and is summarised in [NFR].

15.7.1 Business SLAs

The following are specified [CA].

15.7.1.1 On-Line Transactions

A complex set of maximum transaction times is defined APS, OBCS, NBS and DCS. The maxima range between 20 and 33 seconds, depending on the type of transaction.

15.7.1.2 TIP

Files must be delivered to TIP by 03:00 on the day following that to which they refer

15.7.1.3 Reference Data

B03, 5.2.1 states that Reference Data must delivered to Pathway by 20:00 on a particular day (Day A) must be available to the following percentages of Outlets by the start of core days 2, 3 and 4 as follows:

Type	Day B	Day C	Day D
IMMEDIATE	97%	99%	100%
ADVANCE	---	99%	100%

Table 15.11 - Availability of Reference Data

15.8 PERFORMANCE MODELLING AND MONITORING

15.8.1 Performance Modelling

Being able to predict the loading on all the key components of the system will minimise the risk that any part of the system becomes a bottleneck when new services are implemented.

This is achieved by the construction of a *resource model* that predicts future component source loadings based on volumetric information and system performance parameters. The output from this model feeds into the design and development processes and helps identify where performance shortfalls are likely to occur. Early warning of performance issues enables designers and implementers to put in place corrective actions to review and modify designs and implementations (where appropriate) or to recommend changes to the system configuration before (lack of) performance becomes an issue.

The initial values for these inputs were derived from estimates. As component test measurements and live information became available, the model was calibrated with "real" numbers. The model's algorithms are tested by comparing the predictions, once calibrated, with the system's real behaviour.

A number of performance models are used. They focus on components of the system which are heavily used or where there is a requirement to process on-line or batch workloads within the SLA constraints.

A sizing activity documented in [PERFSERV] estimates the resources required to process each of the main workload components. The resource loading is generated by applying the resource estimates to the throughput model. The model can be used to identify performance deficiencies within the system. It can also be used to evaluate alternative solutions.

A *system model* links together the component resource models and allows the impact of one component on another to be assessed. It enables "what if" questions (e.g. changes in transaction mix and volumes) to be answered across the system.

15.8.2 Performance Monitoring and Measurement

Monitoring mechanisms allow performance parameters and volumetric data to be extracted. They vary from Platform to Platform. Where it is possible to monitor behaviour against predetermined thresholds, any instances in which the thresholds of key measurements are exceeded will be notified to Tivoli as events.

15.8.2.1 Monitoring Capabilities

Different mechanisms are available on different Platforms, as follows.

15.8.2.1.1 Windows NT

Use is made of the Windows NT Performance Monitor. This is especially useful in measuring the performance of the Riposte system on Counter Systems and Correspondence Servers.

15.8.2.1.2 Riposte

Riposte has over 100 statistics that can be accessed via the Windows NT Performance Monitor.

15.8.2.1.3 Sequent Dynix

A BMC Patrol framework is used on the Sequent platforms. The performance of the Sequent system, the Oracle database services and of the applications themselves will be monitored by BMC Patrol Knowledge Modules, using primarily information collected by `sar`.

The Knowledge Modules inform the system manager about changes to the performance of the system, e.g. high disk transfer rates, heavy memory paging or overflow within the database that could affect user-perceived performance.

Performance monitoring tools are used to help diagnose performance hotspots and to track performance over time for use in capacity planning models.

15.8.2.1.4 Network Routers

Network Router statistics are extracted using Cisco Works and HP OpenView. Appropriate messages are passed to Tivoli.

15.8.2.2 Performance Measurements

Measurement activity is carried out by the Performance Management Service (PMS) and covers a number of system components, especially those assessed as being of high risk. Measurements cover Stress, Capacity and Peak Volumes. They ensure that the system components can cope with processing high volumes of data within time limits such as those imposed by Pathway's SLAs.

The output from these tests feeds into the Performance Modelling tools. The priority in performance measurement is to generate the information needed to calibrate and populate the performance models.

The following systems and components are monitored, as specified in [PMSSOD].

- Host systems – DYNIX, applications, Oracle, EMC and SRDF
- Data Warehouse – DYNIX, applications, Oracle and EMC
- Agents – NT and applications
- Correspondence Servers – Riposte and Disk Arrays
- Counter PCs – Riposte, LAN, disk performance
- External Interface Gateways – FTMS and inter-site network connections
- Tivoli Systems Management System
- The ISDN network and Routers
- The Campus networks
- The Inter-Campus WAN

15.9 SYSTEM CAPACITY OF THE HORIZON SOLUTION

15.9.1 General

This sub-section considers the overall sizing of each system component. Each system component is analysed to ascertain, where appropriate, its requirements in terms of:

- processor capacity
- memory
- disk space
- network connectivity
- number of instances of the Platform

The scaleability of the Platform is discussed.

Transaction rates for batch and real-time are dealt with in different ways. For batch, the main issue is the time window available for processing the peak daily load. For real-time traffic, it is the peak expected message rate per second and the response times that this gives rise to.

The architecture and hardware of Horizon has been explicitly chosen to provide a substantial growth potential. This is to mitigate three potential risks.

- The solution consumes more resources than originally sized and cannot be tuned enough to keep it within the hardware purchased
- The mix of transactions is significantly different from that expected, e.g. the proportion of OBCS Foreign Encashments
- The business transacted by PO Ltd with Horizon increases beyond that estimated

Scaling can be achieved at all levels of the design.

The major architectural principle is to allow scaleability by "sideways expansion" in most cases. That is, where a Platform is provided to carry out a certain function, an increasing demand for this service is normally catered for by providing additional similar Platform instances sharing the workload. As well as providing for scaleability, this provides a degree of resilience, especially where the additional Platforms are geographically separate, for example in different Campuses. Performance modelling will be used to verify that scaleability is feasible, and to identify any discontinuities that may arise.

Where this is not possible, scaleability is provided by the potential to increase the size of the particular Platform.

Both these approaches are used, as shown here.

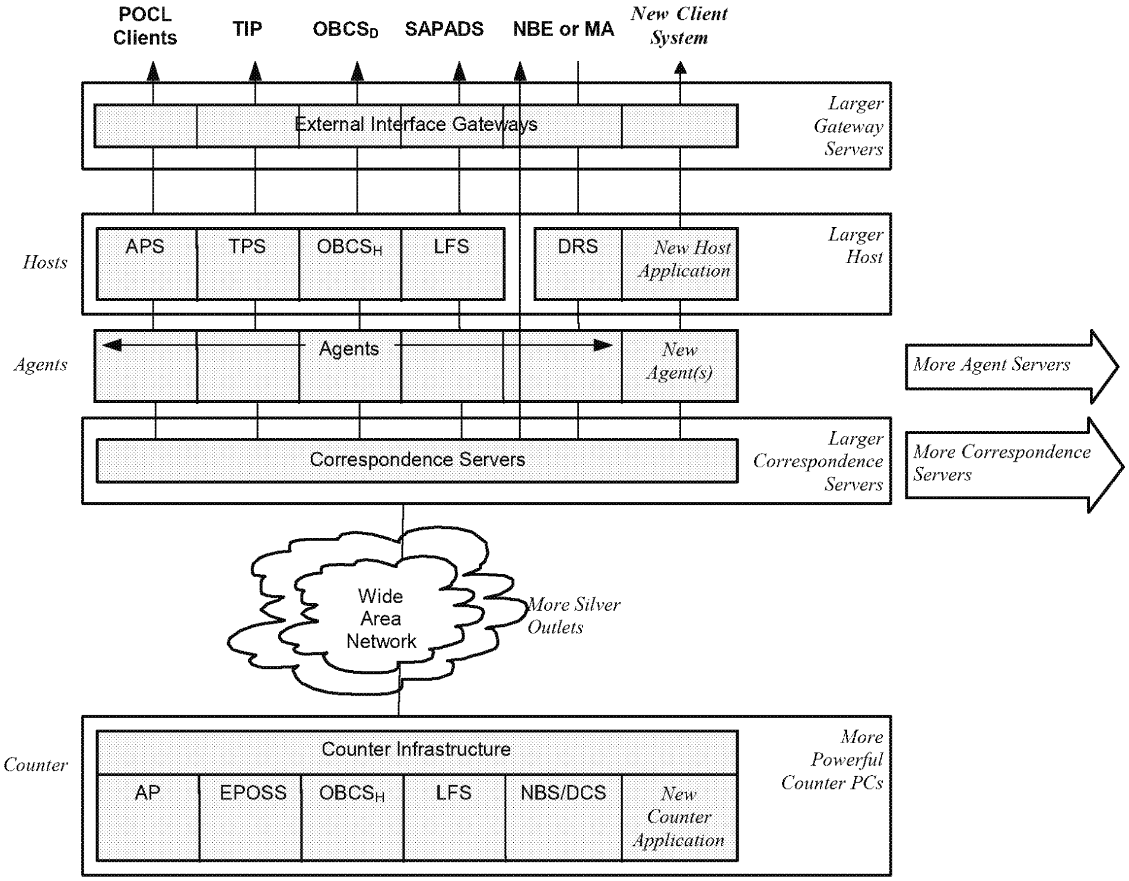

Figure 15.3 - Scaleability

A number of assumptions have been made to simplify the amount of detail provided in this Section. Many of the Platforms used are commodity Compaq servers or Fujitsu workstations running under Windows NT. These systems are supplied with standard amounts of memory, disk space and processor types, as outlined in Chapter 10 “Platforms”. Where these are considered acceptable, there is no further discussion here although in every case measurements are carried out periodically to ensure that the Platform has adequate capacity. Where some additional components are supplied, for example additional disks, this is discussed here.

The following system components are discussed.

- Counter Systems
- Correspondence Servers
- Agent Servers
- Host Central Servers
- Data Warehouse Server
- External Interface Gateways
- Audit Server
- TME Servers
- Communications Links

15.9.2 Counter Systems

15.9.2.1 General

The factors that can affect the performance of the Counter PCs during normal daily operation are:

- Riposte performance
- Counter Application performance
- Memory utilisation
- File encryption and decryption costs, especially as the swap file will be encrypted

Other factors that can affect the Counter, in particular the costs of using ISDN, include:

- Download of software
- Download of Reference Data
- Time to open the ISDN line to the Correspondence Server

The performance of any of the following should not impact the performance of the normal business transactions, even in the largest Outlet.

- Replication traffic
- The size of the message store
- Start-up, log-in and log-out of the Counter PC
- End of Day processing

15.9.2.2 Number of Counter PCs

Outlets vary between one and twenty Counters. The number of Outlets of each size varies and the trend is downwards. Historical figures are shown in the following Table.

Counters	Instances
1	8,950
2	6,404
3	2,396
4	740
5	285
6	187
7	155
8	123
9	73
10+	163
Total	**39,507**

Table 15.12 - Numbers of Counters

15.9.2.3 Processor Capacity

A design consideration for the Counter PCs is that they should be constructed from readily available PC hardware. Standard Counter PCs use a Pentium processor running at 300 MHz. Benchmark tests have shown that this provides an adequate response time to key SLAs.

The need to meet electromagnetic emission standards can limit the speed with which Pathway can intercept new processor technology.

15.9.2.4 Memory

The Counter PCs are configured with 128 MB of memory. This is expected to be adequate for BI3 and S30.

15.9.2.5 Disk Capacity

The major factor influencing the disk space required in Counter PCs is the size of the Riposte Message Store.

As all Counters replicate all data from the other Counters at the same Outlet, the size of the message store is a function of the number of Counters at an Outlet. The disk size required in large Outlets is greater than that for single Counter Outlets. The size of each Counter's contribution to the message store is based on the following.

- The number of messages generated a day
- Their average size
- The number of days for which the messages must be retained at the Outlet before they are archived.

Messages are retained for up to 35 days. This is necessary for some message types, but not for all. Each application will be investigated to determine the time for which its messages need to be retained.

Given these, the uncompressed disk sizes required in different sized Outlets are as shown in the following Table.

Counter PC Disk Requirement	MB
Counters	
1	500
2	620
3	747
4	849
…	…
10	1,276

Table 15.13 - Counter PC Disk Requirements

These figures show the maximum allowed. The standard Counter PC disk size of 13 GB is entirely adequate for this, but some early Counter PCs have smaller disk sizes.

The sizings assume that TeamWARE Crypto encryption temporarily creates a second message store when the encryption key is changed on a Counter. However, the current strategy is to stop Riposte, delete the message store, change the encryption key and restart Riposte. The message store is rebuilt (and re-encrypted on the fly) from the

Counter's neighbours. The original strategy is retained for single-Counter Outlets, but disk size is not a problem in these.

15.9.2.6 Network Connectivity

The Gateway PC in an Outlet must deal with replication of messages across the communications line between the Outlet and the Campus. This additional load must not significantly reduce its performance for Counter operations. For large Outlets, the Gateway PC may be dedicated to this task, with an additional PC for the first Counter position.

When a real-time transaction occurs, a Priority Message is generated and placed in the message store for that Counter. This causes the ISDN line to the Campus to be opened, if not already open, and the message run synchronised. Messages are synchronised in time order, so the time taken for the Campus to process the Priority Message is determined by the number of messages in front of it, and their sizes. Thus, the number of messages waiting needs to be limited to ensure that the SLAs for real-time transactions are met.

15.9.2.7 Scalability

15.9.2.7.1 Single Use

Each Counter PC is dedicated to use by a single Counter Clerk at any one time, and improved performance can only be achieved by a faster processor, faster disks, larger memory or improved communications bandwidth (for Riposte message store replication). This is most likely to be required in the largest Outlets, and if needed will be handled by system replacement. Riposte will replicate the message store onto a new Counter from its neighbours once it has gone through the Auto-configuration process.

15.9.2.7.2 Hardware

There is likely to be considerable growth in the business functions supported by the Counter PCs over time. Thus, these PCs are configured with powerful processors and sufficient disk capacity to cater for the anticipated growth rate in Counter transactions. The serial card in the terminal includes space for three additional peripherals.

15.9.2.7.3 Outlet LAN

Intra-Outlet communication is via an *Unshielded Twisted Pair* (UTP) LAN connections, and this form of cabling makes it easy to move or replace Counter PCs.

15.9.2.8 Counter PC Swap Out

Counter PC swap out is used in the event of a failure. The failed PC is replaced by a "vanilla" PC that then goes through the Auto-configuration process described in Chapter 12 "Systems Management. Once the PC is correctly configured, it goes through a process of restoring its Riposte message store from one of its neighbours. To ensure that this process does not take an inordinate amount of time, the new PC first copies a cached version of the Outlet's message store that was taken during the previous night. This cached version is almost up to date, and hence only the messages generated during the day need to be obtained via normal Riposte replication.

15.9.3 Correspondence Servers

15.9.3.1 General

Correspondence Servers are configured in loosely coupled Clusters of four servers. Each server has its own message store that is mirrored within the EMC Disk Array. Consistency is maintained across the Cluster as data is replicated across the Cluster. Each Cluster is split, with two servers in each Campus.

The Correspondence Server workload comes from a number of sources:

- Messages (transaction) being replicated from the Outlets
- Replication of messages across the Correspondence Servers within a Cluster
- Foreign transaction processing
- Messages flowing in from the host systems
- Messages being extracted by the host systems

Regular performance tests are conducted to determine the throughput and resource consumption of the Correspondence Servers. Data from these tests is used to calibrate the capacity model.

15.9.3.2 Processor Capacity

The basic philosophy is that the Correspondence Servers will be based on the most powerful commodity Windows NT Platforms available. Compaq DL360 servers are used.

15.9.3.3 Memory

Riposte performance is optimal when it has access to a large amount of memory. 512 MB is provided on each Correspondence Server.

15.9.3.4 Disk Capacity

An analysis of the Riposte requirements predicts that the amount of disk storage required by each Correspondence Server during steady state is around 200 GB. The disks are connected on two fast-wide SCSI Channels.

15.9.3.5 Number of Correspondence Servers

Riposte can support an unlimited number of Outlets per Correspondence Server Cluster. However, the machine performance limits the number of active Outlets that can be serviced, so the full population of Outlets cannot be supported by a single Cluster. For resilience, each Cluster contains four Correspondence Servers. The expected load from 20,000 Outlets requires four Clusters, thus leading to a figure of eight Correspondence Servers per Campus.

The Agent Servers contain functionality to provide a mapping between Clusters.

15.9.3.6 Scaleability

A number of measures are taken to reduce these sizes, including the following.

- Message Store compression
- Reducing EPOSS message retention dates to 35 days
- Using Flat Files to hold some data which is currently held as Reference Data (such as receipt layouts)

Adding more Clusters would provide greater throughput, but this is lengthy and complex process. As the number of Outlets is not expected to increase, there are no plans to increase the number of Clusters.

15.9.4 Agent Servers

15.9.4.1 General

The *Agent Servers* form the interface between the Host Systems and the Correspondence Servers. They serve two distinct roles:

- Moving information in both directions between the Host Systems and Riposte. This uses Oracle Client to access the Host Systems' databases and RPC calls to access Riposte
- Moving real-time messages to and from external systems such as the NBE or MA

Different types of Agent Server are used for these different functions.

15.9.4.2 Processor Capacity

All Agent Servers are sized such that any one Campus can run the entire batch workload while meeting the SLAs. This requires, for example, that it is possible to run 64 instances of the TPS Harvester Agents.

15.9.4.3 Memory

Agent Servers are configured with256 MB of memory.

15.9.4.4 Number of Agent Servers

Four general purpose Agent Servers, and four each of the NBS and DCS Agent Servers, are provided per Campus. That is one of each type per Cluster.

This number will be evaluated under load to ensure that it is sufficient to meet the peak workload requirements.

15.9.4.5 Scaleability

Each general purpose Agent Server runs Agent processes that do one of the following.

- Pull data (Flat Files or Oracle records) from the Host Servers and create Riposte messages via RPC calls to the Correspondence Servers
- Read messages from Riposte and write records into Flat Files or (via SQL*Net) into Oracle tables on the Host Servers.

This architecture is inherently scaleable, with Agents acting completely independently of each other. Thus, any increase in demand (for example following the introduction of a new application) can be met by installing new Agent Servers and modifying the Maestro schedules to bring them into play.

However, an increasing Agent workload will also increase the workload on the Host Central Servers and on the Correspondence Servers, both of which are accessed by RPC; and on the Campus LAN. These may prove a bottleneck in due course.

The NBS Agent Server and DCS Agent Servers are optimised to handle real-time traffic to external authorisation services.

15.9.5 Host Central Servers

15.9.5.1 Processor Capacity

The Host Central Server is a Sequent NUMA-Q Quad, containing two 400 MHz Intel Xeon processors.

15.9.5.2 Memory

Each Node supports up to 4 GB of memory.

15.9.5.3 Disk Capacity

The Host Central Server data is held on 18 GB disks in an EMC 3430 disk array. The array is connected via Fibre channel. The layout of the Host systems databases is covered in [HOSTSS].

15.9.5.4 Number of Host Central Servers

Cost and space considerations limit these to one Node per Campus. Each is sized to be able to carry the entire workload. This runs entirely within one Campus, with a site failover strategy to transfer the entire workload to the other Campus.

15.9.5.5 Scaleability

15.9.5.5.1 System Performance

The physical components that potentially limit the performance of this configuration include the following.

- Processor power
- Disk I/O bandwidth
- Disk controller throughput
- Memory (required to run many parallel tasks and provide cache and buffers for Oracle)
- Database design and implementation
- Application design and implementation
- Network connectivity

15.9.5.5.2 Memory

NUMA-Q systems support up to 4 GB of memory per Node.

15.9.5.5.3 Host Database Sizes

The Oracle disk layouts are designed to optimise the traffic per spindle. Oracle has the ability to extend existing tables onto new disk volumes, should any be available, though this expansion does not take into account the original disk layout strategy and can thus lead to performance problems.

Any requirement to unload and reload the Oracle databases, for example to make major changes to these disk layouts, is a lengthy process.

Most of the time-critical work on the Host Central Servers is batch based. The limiting factor for these is usually channel or disc bandwidth. The elapsed time of a job is roughly proportional to the amount of work to be processed. Discontinuities can occur, however, when indexes have to split to another level.

The sizing of the Host applications will involve a combination of modelling and component measurements. The resource model will be validated using measurements taken when the Host is under different conditions of stress.

15.9.6 Data Warehouse Server

15.9.6.1 Data Warehouse Database

The database size is calculated at 1.4 Tb, made up as follows.

Table	Size (GB)	Purpose
Data table spaces	615	
Index Table spaces	280	
Temp space	100	
Set Aside area	288	Holds retrieved copies of historical archives. Sized to hold six weeks data
SLAM	10	
Total	1,400	

Table 15.14 - Data Warehouse Database Size

The size of this is dependent on a number of factors including the following.

- Number of EPOSS transactions
- Number of transactions per customer session
- Number of EPOSS product types supported
- Number of weeks that weekly aggregates are held for - currently 20
- Number of days that daily aggregates are held for - currently 140

Sizings allow for 10% contingency on all table sizes.

15.9.7 External Interface Gateway Platforms

15.9.7.1 Transfer Rates

The file transfer protocol is the Windows NT file copy process. This supports a transfer speed of around 2 MB/sec over a 100 Mbps LAN.

15.9.8 Audit Server

15.9.8.1 Archive Volumes

Horizon generates around 20 Gb of audit data per day. Compression techniques are used to reduce the amount of space required to store this, and in practice a compression ratio of around 6:1 can be achieved. Thus, there is a need to store around 3.34 Gb per day. This is generated in files of around 65 Mb, or 10 Mb compressed.

Data is stored for up to 15 years.

15.9.8.2 Archive media

The choice of archive media is dictated by the total amount of data that must be held; the daily rate of additions to this; and the response time required for audit data retrievals.

Prior to BI3, DLT tapes were used to hold audit data. However, these give rise to tape storage and handling problems, and are not as reliable as first throught. From BI3, the audit tapes are supplemented by a Centera disk array that is especially designed to store audit data in a secure and retrievable manner.

15.9.9 TME Servers

The Tivoli systems have been sized to support the work generated by 40,000 Counter PCs. There is a limit of 1,000 managed nodes per TMR, which imposes a need for 40 Client TMRs. These are grouped together on the TME Management Servers, with four TMRs per server.

15.9.9.1 Scaleability

Pathway and FSCS have worked closely with Tivoli to prove the scaleability of the TME system up to 40,000 managed nodes.

The main factor is software distribution. Mechanisms have been developed to throttle the rate of both distribution and activation processes to a rate that can be handled by the ISDN Router network.

15.9.10 Communications

15.9.10.1 POCL and DWP WAN Connections

These are sized on the required transit time for the maximum expected size file. Increases in planned file sizes will require these links to be reviewed. Currently they are 2 Mbps links. Bandwidth can be increased by adding more links; Energis provide nothing between 2 Mbps and 34 Mbps, though a CIR as low as 4 Mbps can be leased over the latter.

15.9.10.2 Inter Site WAN Connections

These are sized on the traffic between Correspondence Servers. This peaks at around 3.5 Mbytes/sec (specifically 09:00 to 10:00 on the last Monday before Christmas).

Most other traffic is small in comparison.

The two Campuses are linked by two PVCs with reserved bandwidth of 4 Mbps. The number of PVCs has been established by modelling. The capacity of each PVC is less than that of the Campus LAN, so it is possible for traffic to be generated faster than it can be carried over the WAN. The target is for no more than 1% of Datagrams to be dropped over consecutive 5-minute periods.

There is, however, substantial growth capacity in these links without any hardware change, merely by buying more guaranteed bandwidth from Energis.

15.9.10.3 Inter Site Disc Mirroring of EMC Disks

EMC disks are connected by a dedicated 34 Mbps PVC running over the inter-Campus ATM link. This can deliver instantaneous throughput in excess of 3 MB/sec. Current sizing shows this is acceptable. The entire Host workload runs at one Campus, so this link is only used to ensure that the servers at the other Campus have up to date versions of the data used by the primary services. It has no immediate effect on batch run times.

15.9.10.4 Campus Connections to Outlets

This is out of date. Replace by FRIACO numbers.

15.9.10.4.1 ISDN Connections

ISDN Channel Demand is estimated to peak at 757,517 calls between 09:00 and 10:00 on Mondays, representing 14.61% of ISDN channel capacity with six Campus ISDN Routers per Campus in normal operation. Six Routers are used based on a maximum utilisation of 70% when a single Campus is taking the entire load (i.e. in disaster mode). The detailed analysis is given in [NWARCH]. It is based on the following peak Hour Assumptions:

- 30 Foreign Transactions/second
- 1,000 transactions/second giving rise to 1,500 Riposte messages/second
- 4 calls per second from Outlets for which there has been no communication for the *Unconnected Broadcast Interval*
- 1,000 Riposte messages created per second at the Campuses.

Analysis shows that each ISDN gateway can support 11.09 calls per second. This requires six gateways to support 60 calls per second. For resilience, six are provided at each Campus.

Additional ISDN capacity might also be needed because of extra data within each call. As this does not increase the call set up rate, it can be accommodated by adding additional primary rate lines and ISDN primary rate cards to the existing Routers. Each Router has 13 slots of which six are used. Each slot can support two Primary rate ISDN lines

There are other loads placed on the ISDN network, including:

- Reference Data transfers [overnight?]
- Tivoli event traffic from the Counters
- Key Management traffic
- software download from the Campus to the Outlets

The most substantial of the systems management loads is the last, but this can be arranged to occur outside peak times and over several days. The others are thought to be small.

15.9.10.4.2 Frame Relay Connections

Frame Relay traffic from non-ISDN Outlets peaks at the same times as the ISDN traffic, as there is no difference in behaviour between the two types of Outlet.

Two Frame Relay Routers are provided at each Campus.

15.9.10.4.3 VPN Servers

The VPN Servers are sized on the expected traffic from Outlets, and the assumption that either Campus must be able to support the entire Outlet workload. Twelve VPN Servers are provided at each Outlet.

Further scaleability can be provided by any of the following.

- Provide separate "incoming" and "outgoing" VPN servers. This would double the number of Servers
- Add VPN servers and modify the assignment of routes to Servers.

15.9.10.5 Campus Links

The Network solution described in Chapter 9 “Networking Services” provides a bandwidth of 2 x 155 Mbps into each Campus. This is apportioned between the PVCs used for the inter-Campus links, the high-speed links to DWP and PO Ltd sites and Pathway at Feltham and the low-speed ISDN and Frame Relay traffic. It allows for an almost 100% growth over expected traffic volumes.

Should this prove insufficient, then further Fibres can be “lit” (brought into play) and more 155 Mbps circuits established. There are twelve cables in each connection to the Energis Network, and only two are used at present. Alternatively, because the backbone network uses SDH technology, the Campus circuits could be upgraded to the SDH speed of 622 Mbps.

There are limits on the number and bandwidth of the circuits supported by the SMAs. Each SMA1 has four slots, each of which can accommodate either a single 34 Mbps module or a 16 x 2 Mbps module. There are three spare slots. Expansion is by providing additional SMA1s, if more incoming fibres are lit, or replacing them by SMA4s with four times the module capacity.

15.9.10.6 Campus Internal LANs

There are a number of duplexed virtual LANs (VLANs) per Campus, supported by two Cisco Catalyst 5500 switches. Each LAN supports 100baseT Ethernet in a star connected configuration. VLANs can be extended across the Campuses.

Servers that connect to a LAN usually have two cards, one for each of the duplexed LANs, They cannot easily be enhanced to connect to more than two LANs. Thus, any performance problems identified with the Campus LANs are resolved by further partitioning of the Campus equipment between more VLANs, with high-speed routing between them.

15.9.10.7 Outlet LANs

Where there are more than two Counters in an Outlet, they are connected via a 3Com OfficeConnect LAN Hub as shown in Chapter 9 “Networking Services”.

15.10 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 14	Usability	Describes the measures taken to ensure a high usability of

			the Horizon systems
Next	Chapter 16	Security	Describes the measures taken to ensure the security of the Horizon systems and the data they hold
BUSVOLS	PA/PER/032	Horizon Existing Service Business Volumes	Source of volumetric data for services prior to BI3
BUSVOLSN	PA/PER/031	Horizon New Service Business Volumes	Source of volumetric data for NBS and DCS
HOSTSS	TD/STR/001	Host Systems Storage Strategy	Describes the approach used to map Application Host databases onto the Host filestore.
NFR		Non-Functional Requirements Register	Lists the SLAs pertaining to Horizon
PERFOV	PA/PER/005	Pathway Performance - Overview	Provides an overview of the performance measurement and analysis processes
PERFSERV	PA/PER/007	Pathway Performance - Services	Contains an analysis of the behaviour and hence performance of the principal system threads
VPNHLD	RS/DES/046	VPN High Level Design	Describes the scalability calculations for VPN Servers

Chapter 16 - Security

16.1 SCOPE

This Chapter outlines the contribution that Security concerns make to the Horizon architecture.

Security is a measure of the protection that the system provides against unauthorised attempts to access information and services, or to interfere in its operation.

The three main categories of attack against the security of a computer system are as follows.

- *Confidentiality* - unauthorised observation or inference of information (e.g. the need to prevent a claimant's neighbours or the press from knowing who's getting what benefits)
- *Integrity* - unauthorised manipulation of information (e.g. of the data passed to and from PO Ltd and the DSS). Loss of integrity can be caused by system or human failure as well as by malicious action.
- *Availability* - unauthorised denial of service to other users

Any loopholes in these could cause lasting reputational damage and financial loss to Pathway and/or PO Ltd.

A fourth aspect is *audit* and accountability; ensuring that users are held accountable for their actions by recording information about these actions. Many aspects of the first three threats can be avoided if users know that they will be held accountable for their actions.

16.2 STRUCTURE

The Chapter discusses the following subjects.

- The Security Reference Model used in OPEN*framework*
- The Business Issues surrounding the provision of security features in Horizon
- The Security Domains that are used
- The Authentication Services used
- Facilities for Access Control
- The use of Auditing
- The use of Cryptography

16.3 SECURITY REFERENCE ARCHITECTURE

The security reference architecture includes measures to assist in each of the areas of Confidentiality, Integrity, Availability and Audit. It is based around a set of security functions, as follows.

- Identification and Authentication of users, which provides knowledge of where users are accessing the system, their access routes, what they are authorised to do from these locations and by these routes
- *Identification and Authentication of System Components*, which ensures that these are not being subverted to assist in avoiding identification and authentication of users
- Control of what authorised users can do on the system, exercised in a way that reflects real world requirements. Unauthorised users should not be granted any access to the system.
- Ensuring *Data and Transaction Integrity* by appropriate means
- Monitoring and Reporting of security relevant activities in the system, with a reasonable degree of granularity
- Defence against any threatened external electronic attack (for example line taps on communication links)

16.4 BUSINESS ISSUES

Pathway is required to support a wide range of security policies. These are defined in [SPOL]. Security features support and enable the security measures defined in the *Security Functional Specification* ([SFS]), the *Access Control Policy* ([ACP]) and the *Audit Policy ([AUDP])*.

Some of the data held by Pathway originates with Her Majesty's Government, and is classified as RESTRICTED. Because of this, where security measures are provided they need to follow the advice of CESG. Other data is associated with financial transactions and the regulations of the Financial Services industry are applied.

Following a detailed risk assessment, the following security policies have been developed.

- Pathway's IT systems will ensure appropriate confidentiality, integrity and availability of data, whether in storage or in transit. Maintaining the integrity of the services and software components is also essential
- Physical and logical access to the system will be controlled, with access granted selectively and permitted only where there is a specific need. Access will be limited to persons with appropriate authorisation and a "need to know" requirement
- A user's claimed identify is verified before any access is granted to the system. Authentication mechanisms are also required to ensure that trust relationships can be established between communicating components within, and external to, Horizon
- All users of Pathway's services will be individually accountable for their actions. Accountability for information assets will be maintained by assigning owners, who will be responsible for defining who is authorised to access the information. If responsibilities are delegated than accountability will remain with the nominated owner of the asset.
- Audit mechanisms are required to monitor and detect events that might threaten the security of the Pathway services or any service(s) to which it is connected
- Alarm mechanisms are required to alert security personnel of the occurrence of security violations that could seriously threaten the secure operation of the services
- Pathway will monitor all developments and operations to maintain assurance that its services are performing in accordance with approved security standards and controls.

This will give a high level of confidence that all information is being protected during processing, transmission and storage

- Apparent attempts to subvert the security of the system, such as repeated failed Login attempts, will be brought to the attention of the security authorities by a system of alarms

16.5 SECURITY DOMAINS

Security architectures revolve around the concept of interworking "security domains". A domain, in this sense, is viewed as a collection of one or more Platforms and the interconnecting network which can be considered to be physically secure and which present a common interface to the rest of the world.

[SFS] and [ACP] define a set of Domains that map onto the functions described in the [SADD]. These are shown below and described extensively in [ACP], which uses the structure as the basis for the Access Control policies.

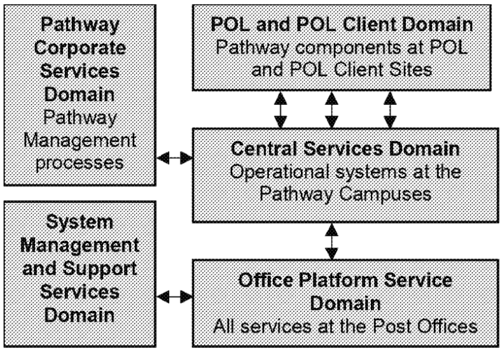
Pathway Corporate Services Domain
Pathway Management processes
POL and POL Client Domain
Pathway components at POL and POL Client Sites
Central Services Domain
Operational systems at the Pathway Campuses
System Management and Support Services Domain
Office Platform Service Domain
All services at the Post Offices

Figure 16.1 - Pathway Domains in the [ACP]

The Security Architecture provides a framework within which these policies can be implemented, and later changed if necessary. Thus, in line with other Chapters of this document the [ACP] view of domain structures is re-interpreted as shown here.

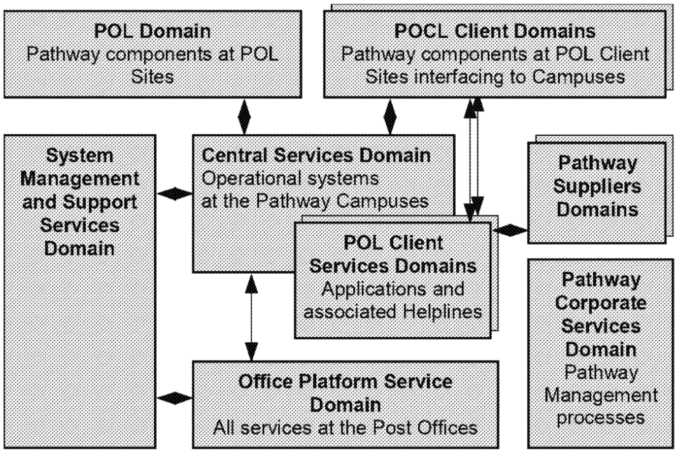
POL Domain
Pathway components at POL Sites
POCL Client Domains
Pathway components at POL Client Sites interfacing to Campuses
System Management and Support Services Domain
Central Services Domain
Operational systems at the Pathway Campuses
POL Client Services Domains
Applications and associated Helplines
Pathway Suppliers Domains
Pathway Corporate Services Domain
Pathway Management processes
Office Platform Service Domain
All services at the Post Offices

Figure 16.2 - Generic View of Pathway Domains

The key difference here is that all PO Ltd Clients are considered as equals, from an architectural point of view, and so are all suppliers to Pathway.

In practice, Horizon presents a complex architecture that does not map easily even onto this generic domain structure. However, the logical system architecture given in Chapter 4 “Overview” provides a sensible starting point. The following diagram shows a domain structure that reflects this architecture. It identifies the principal components of each domain, and some of the major sub-domains.

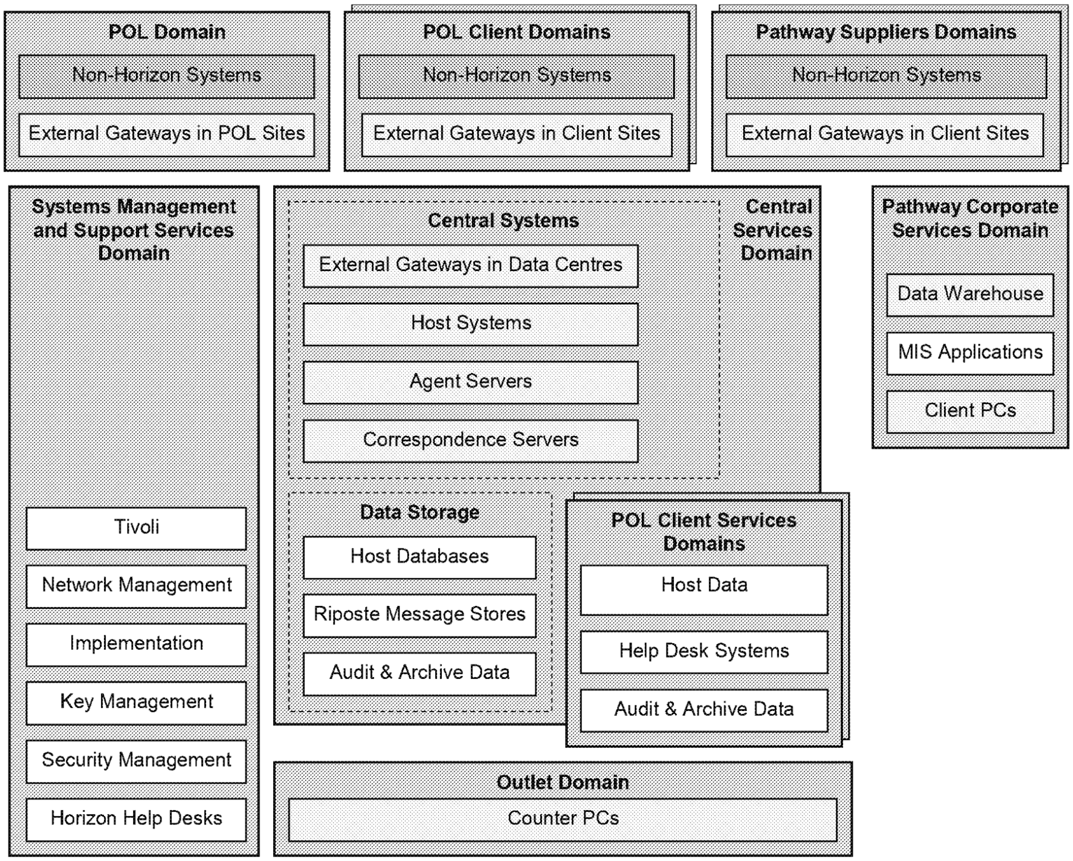

Figure 16.3 - Horizon Security Domains

These domains represent major areas of responsibility for services. Each has different characteristics that affect the type of access controls needed in that domain. The remainder of this sub-section summarises the architectural issues surrounding these domains.

The major security attributes of each of these domains are as follows.

16.5.1 External Domains

The following three domains are similar and contain similar sub-domains:

- PO Ltd Domain comprising the TIP sites
- PO Ltd Client Domains, including the NBS, DCS, OBCS and AP sites
- Pathway Suppliers, such as Oracle and Sequent, who provide system services or support

Each sub-domain includes the External Interface Gateway PCs and associated Routers located on the external sites. The principal need here is to prevent attack by hackers and others on the integrity and confidentiality of the data held within the System, or more importantly on the network as a whole.

In some cases, Pathway must interwork with non-Horizon systems installed on the external organisation's site, and these are included in the appropriate Domain.

16.5.2 The Central Services Domain

This comprises the principal Pathway supplied sub-domains.

16.5.2.1 The Central Systems Sub-Domain

This comprises the servers, including the External Interface Server PCs, located in the Campuses. The main security aim here is to control access to the systems that hold business data.

16.5.2.2 Data Storage Sub-Domain

This comprises the main data repositories owned and managed by Pathway. These include the Riposte message store, and the major application databases, although there are some overlaps and difficulties in the following areas.

- The Riposte message store is also found in, and forms a conduit to and from, the Outlet Systems domain
- The *data* held in the Host databases belongs to PO Ltd or its Clients, and Pathway must ensure adequate separation between the data owned by different organisations.
- Data held for audit purposes within the Archive service.

16.5.3 PO Ltd Client Services Domains

This Domain represents the data that supports PO Ltd Client requirements within the Central Services Domain. It represents the fact that data changes ownership as it progresses through the system. Pathway accepts responsibility for the data from the time when it arrives at an external interface until the time when it is made available to Counter staff. For transaction records, Pathway's responsibility extends from the time when the transaction is completed until the data is returned to PO Ltd or its Clients via the TIP Gateway.

Client services include:

- AP Clients
- Network Banking Engine (NBE) for NBS transactions
- Merchant Acquirer (MA) for DCS transactions

16.5.4 The Outlet Systems Domain

This comprises the Counter PCs installed in the Outlets. These are in a hostile environment, and measures are necessary to protect the data they contain against thieves and vandals.

16.5.5 System Management and Support Services Domain

This contains the central elements of the System and Network Management facilities for managing components in the other domains. It covers:

- Software Distribution and associated software Inventory Management
- Event management
- Resource management
- Network management of Routers, Hubs, Gateways and Firewalls
- Hardware inventory management supporting Software Distribution and Network management
- Horizon Systems Help Desk

In addition, the security management facilities, by which Pathway's security staff enforce the security policies, form part of this domain.

TME provides the Central System Management functions. These co-ordinate input from other management software including:

- BMC Patrol, which is used to provide event and resource management of the Sequent-based Host Central Servers and Data Warehouse Server
- HP OpenView (with CISCO Works), which is used for management of the network Routers.

A number of other services interact with operational and management services at the Campuses. These include:

- The Configuration Management system controlling information about software components for Horizon products prior to their distribution
- The PowerHelp system used to record and maintain information about calls to the Horizon Systems Help Desks and their progress
- The System Support Centre and Pathway supplier systems which provide 3rd and 4th line support functions
- The Dispatch-1 system which holds hardware inventory information

Finally, a set of Security Servers provides authentication and crypto Key Management services to other domains.

16.5.6 Pathway Corporate Services Domain

The Corporate Services domain supports Pathway's own management processes such as reporting, accounting, monitoring service levels and Pathway's fraud risk management and auditing processes. It includes the Data Warehouse that gathers information from the operational system, and the MIS system that runs on the same server. These systems are owned by Pathway and managed by FSCS.

It also includes the MIS Client Workstations that are used within Pathway to access information held in this Domain.

Access to the information held within these systems is granted to Pathway Management and, by arrangement, PO Ltd staff.

16.6 AUTHENTICATION SERVICES

16.6.1 General

Authentication is concerned with proving the identity of a user or a system component. Authentication facilities are required in a number of locations throughout the system architecture. They are defined in [ACP] and are as follows.

- Post Office Managers, who must authenticate when switching on their Counter PCs
- Counter Clerks at Post Offices
- Counter PCs themselves must authenticate when establishing a link to the Campuses
- Additional authentication is required the first time a Counter PC is switched on after it is installed.
- Operations and Support users
- Management users
- Users with direct access to the Host databases
- Post Office Managers who have mislaid their PMMCs and thus cannot carry out the Post Office Log On and who need to authenticate to the Horizon Systems Help Desk before being given a new token or PIN
- Pathway Management users accessing the MIS services

The remainder of this sub-section describes the various authentication methods and discusses how adequately the meet the needs of Pathway.

16.6.2 Structure

Component	Platforms
COSMAN Access Control Manager	Data Warehouse Server Host Central Server
One Time Password Application	One Time Password Workstation
Post Office Log On (POLO)	Counter PC
System Integrity Check Application	One Time Password Workstation
Terminal Access Controller Access Control System	Network Management Server

16.6.3 Post Office Log On

A stolen Counter PC presents two potential threats.

- There is personal data stored on it, which must be protected
- It could provide an opportunity for illicit access into the Horizon network

To counter these threats, the Riposte message store and certain other data on the Counter PC is encrypted as described below. The filestore is unlocked by a special POLO process that is used by the Post Office Manager during the initial boot sequence. This process uses the authentication APIs exposed by Microsoft in Windows NT. It is invoked automatically, as shown here.

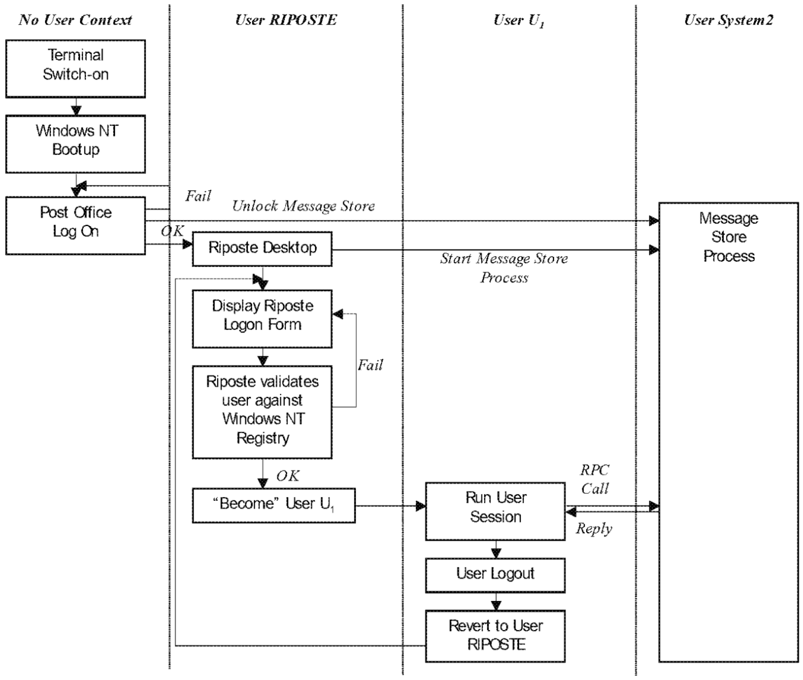

Figure 16.4 - Terminal Start-up and Logins

As soon as Windows NT has reloaded, it displays a Post Office Log On form. This requires that the Post Office Manager inserts his or her *Post Master's Memory Card* (PMMC) into the keyboard of the PC and enters a PIN. The authentication process validates the PIN against the information stored on the card. If this is successful, the POLO process uses information from the card to "unlock" the encrypted filestore areas, including the swap file and Riposte Message Store. The card can then be removed and returned to the safe. It is not possible to run Riposte until the message store is unlocked.

If the Post Office Manager loses the card, or it becomes corrupted, or he forgets his PIN, then he phones the Horizon Systems Help Desk to invoke the POLO Recovery Process.

The Counter PC then continues with its normal boot sequence, and enters the *CounterLoader* function that enables the Riposte Desktop to be started and restarted in a controlled fashion. This displays the first User Login screen.

16.6.4 Unattended Reboot

The POLO process described above is intended to prevent the use of stolen Horizon Counter PCs. However, certain software distribution processes require the Counter to be rebooted (sometimes a number of times). The timing of these distributions is made known to the KMA Server, which establishes a window during which the Counter isexpected to be rebooted. Then, following each reboot, the Counter contacts the KMAS to verify its identity as an alternative to undergoing a POLO process in the middle of the night.

16.6.5 Riposte Authentication

The Riposte user Login process runs under the security context of User "Riposte". This user has minimum privileges. It merely runs the Riposte Login mechanisms. These are implemented by Escher, largely to counter the Login and Logout times of the basic Windows NT system.

It is possible to close down and restart the *CounterLoader* application, for example via a Tivoli command, to enable new software to be loaded or to carry out other administrative functions.

16.6.5.1 Authentication of Counter Clerks

The Counter Clerk submits his User ID and password via this screen. Riposte uses standard Windows NT APIs to authenticate users, passing across their passwords which are then hashed and compared with the Windows NT stored value. In addition, the password is compared with the hashed value stored in the Riposte message store.

Windows NT uses a one-way encryption mechanism to store user passwords. All Riposte users, including the Post Office Manager, are mapped onto Windows users, and hence their UserIDs and (encrypted) passwords are stored in the Windows security database on each Counter in the Outlet.

In addition, Riposte stores the UserIDs and passwords within the Riposte message store, as Persistent Objects, so that they are available to other Counter PCs within the same Group. ("Conventional" Windows NT systems store these on the Domain Server, and thus users may log on at any Workstation within the Domain. Horizon does not use the Domain architecture in this way. Each Counter is effectively a single-member domain).

The passwords are hashed using the 160-bit one-way *Secure Hash Algorithm* (SHA) provided by the Win32 Crypto API. The password is hashed along with the user name and GroupID, so two users in different Outlets with the same name and same password will still have different hashed passwords.

Once the Counter Clerk has been successfully logged in, the Riposte Desktop process changes to the user's User-name context U_1. This is a normal (non-privileged) user, and hence the Desktop is constrained by the privileges of that user.

However, the Desktop process does not access workstation files directly, but acts as a client to the Riposte service that is running under the "system" user. Desktop calls on the Riposte service use RPCs. The Riposte service uses standard Windows NT facilities to "impersonate" the user U_1. Impersonation is a standard Windows NT facility whereby a thread executes in a security context different from that of the process that owns the thread. Access checks on any action performed by the thread are carried out under the context of the "impersonated" user, not the process-owning user.

16.6.5.2 User Log Off

When the user logs off, the Desktop log on form is redisplayed. A new user can then log on, without the overheads and delays of reloading the Riposte Desktop.

16.6.5.3 Session Mobility

Riposte stores information about logged-in users in the message store. Thus, should a user who is already logged in at one terminal try to log in again at a second, Riposte is in a position to terminate the first session. The user's context is transferred to the new terminal and they can carry on from where they left off.

16.6.5.4 User Administration in Riposte

Riposte supports facilities for the Post Office Manager to define as users the Counter Clerks who work in the Outlet. Other standard facilities are provided to change their passwords, and to delete users.

Other facilities enable the Post Office Manager to modify the attributes of a user:

- Whether the user must change his/her password on next Login
- Wwhat groups the user belongs to (managers or tellers)

16.6.5.5 One time Password

Riposte also supports a mechanism known as a "One Time Password". This is defined as mandatory for certain UserIDs on each workstation. It is designed for roving staff such as auditors or engineers who cannot be expected to know or remember a password for each system that they may use. At an Outlet, they telephone the Horizon Systems Help Desk and are given a One-Time password for that system.

The password is generated by a freestanding One-Time Password Workstation. The operator asks the intending user to read out a value generated during the Outlet installation process and subsequently locked away by the Post Office Manager. From this, the One Time Password Workstation generates a password that the operator then reads to the user.

16.6.5.6 System Component Authentication

Riposte components are signed using standard Microsoft facilities. Riposte will refuse to use any component that is unsigned or signed incorrectly.

16.6.6 Authentication of Counter PCs

The Gateway PC in each Outlet periodically establishes a link with a Campus, during which all outstanding messages in either direction are exchanged.

16.6.6.1 CHAP

CHAP (devised by Microsoft for its *Remote Access Service* (RAS)) was originally used to authenticate ISDN connected Outlets. This use has been superseded by the introduction of VPN. However, CHAP is stgill used for other ISDN connections, such as those between the Campuses and AP Clients.

16.6.6.2 VPN

Horizon uses a mechanism known as *Virtual Private Networks*, or VPN, which provides an encrypted tunnel between the Counter PC and Campus. This is installed at the TCP/IP level within the Gateway PC, and in a set of VPN Servers at the Campus. Sessions are established using a VPN Key distributed by the KMA Server and periodically updated. The ability to initiate and respond to an encrypted connection using this Key proves the identity of the Outlet.

16.6.6.3 Authentication of New Counter PCs

The POLO process described above assumes that the Counter PC is a fully accredited member of the Horizon network, and contains information that may be used to support these authentication processes

As described in Chapter 12 “Systems Management”, a Counter PC is delivered in a “vanilla” format with no inherent identify. There is a need to both *Identify* and *Authenticate* any Counter PC attempting to join the network for the first time.

Once the Gateway PC is powered up at an Outlet, it begins a boot process that attempts to contact the Boot Server at its target Campus. The Boot Server attempts to authenticate the Gateway PC.

- Where the Outlet is connected by ISDN, the authentication process is triggered by the CLIP of the incoming ISDN connection. This identifies the Outlet.
- Outlets connected by Frame Relay have an IP address pre-configured into the Outlet Frame Relay Router, and this identifies the Outlet.

The Boot Server is outside the VPN curtain, and so this dialogue is unencrypted.

The Boot server determines the Outlet identity and returns a Datagram containing the Outlet’s postal address. It then returns a (small) number of files that enable the Gateway PC to configure itself. One of these is an initial Post Office Key (POK).

The Gateway PC then reboots, and connects to the KMA Server (KMAS) via a special *VPN Exception Server* that accepts in-clear data but will only route it to the KMAS. The KMAS conducts a Diffie-Hellman exchange with the Gateway PC, and delivers some initial Key material including the FEK and a new POK. The FEK is written to the PMMC. The Gateway PC can then re-dial using VPN with its unique Key, and begin thefull Auto-configuration process.

16.6.7 Authentication in Windows NT

The processes described above are exceptional and are used for Counter PCs only. Where users need to access the Windows NT servers or workstations located in the Campuses or support centres the more normal Windows NT authentication methods are used.

The Windows NT architecture is as shown below.

This is a Working Document as defined by the Codified Agreement, and has no Contractual standing.

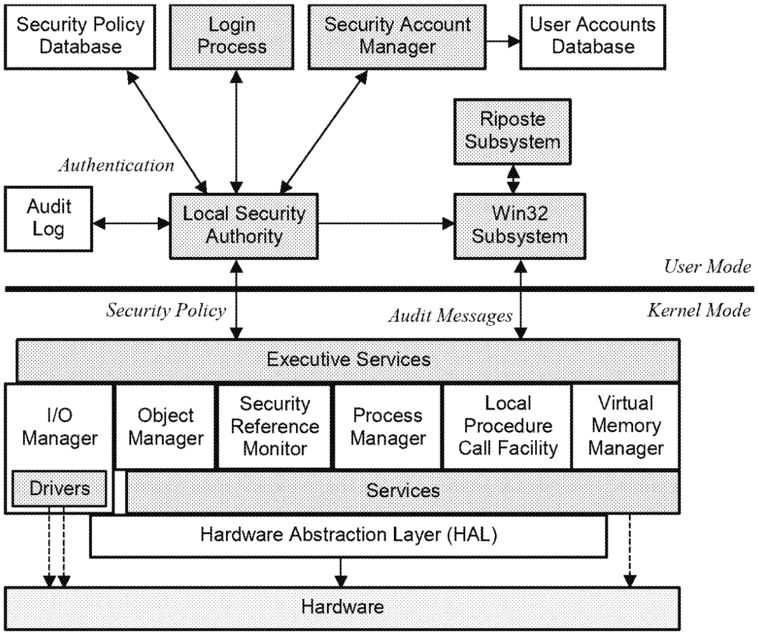

Figure 16.5 - Windows NT Security Components

16.6.7.1 User Identification and Authentication

Windows NT authentication mechanisms are based upon an object model in which each object (file, device) has associated security information that is matched against the credentials of any user who tries to access that object. The model requires that there is only one place in the system at which uses are identified and authenticated. This is the "trusted" WINLOGIN process, which is entered automatically when the user presses what is known as a *Secure Attention Sequence* (SAS) - Ctrl+Alt+Del. The SAS is handled only by the Windows NT kernel, and causes entry to WINLOGIN. It is not possible for any other program to interfere with this operation.

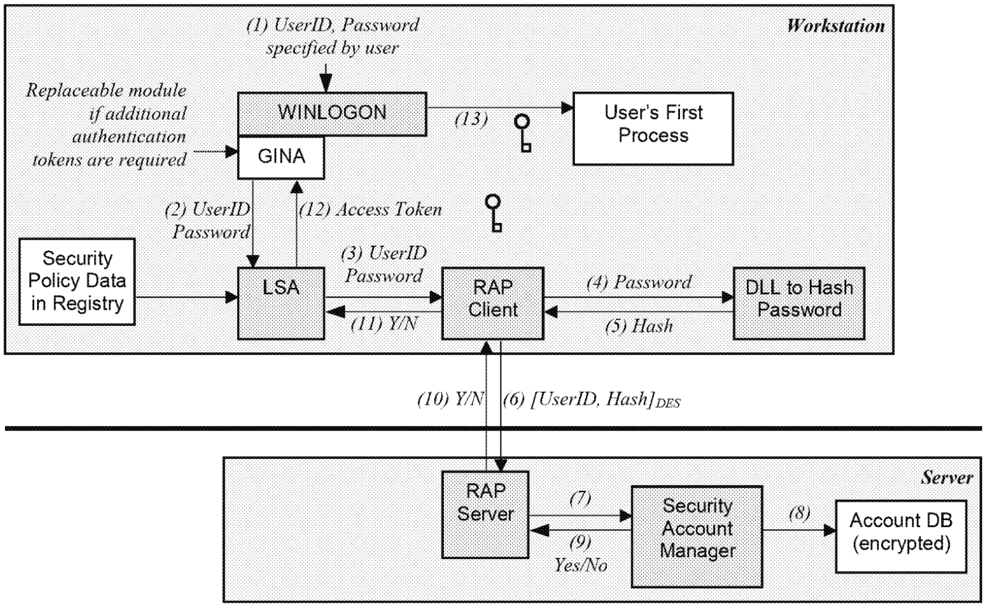

Figure 16.6 - Windows NT Authentication Process

16.6.7.1.1 Graphical Identification and Authentication (GINA)

WINLOGIN invokes a component known as the GINA. An organisation can replace this module in conjunction with Microsoft.

The GINA checks the UserID and Password supplied by the user. If relevant, the user can also specify a Domain within which he wishes to be authenticated.

16.6.7.1.2 Local Security Authority (LSA)

The GINA invokes a process known as the LSA, which imposes the security policy using information held in the Registry. It invokes the *Remote Authentication Process* (RAP), which is a client-server process able to operate both in the user's workstation (the case with a Counter PC) and in a remote Domain Server. In the latter situation, it uses a secure RPC mechanism between the client and server.

The RAP passes a hashed version of the Username and password to the verification process. If this takes place in a separate Server, the hashed value is encrypted using DES when it passes over the network. The verification process compares the hashed value with the value held in a password database. If the two match, then the user is authenticated. The LSA generates an "access token" which is returned to WINLOGON and is passed by that to the user's "first process", and from that to any other processes spawned on behalf of the user.

16.6.8 Authentication in SUN Solaris Servers

The SUN Solaris operating system is used in the following Platforms.

- Network Management System, which supports the HP OpenView and CiscoWorks applications
- TME Event Servers and Gateway Servers
- Firewall Modules

It supports standard UNIX login authentication.

16.6.9 Authentication in Sequent Servers

16.6.9.1 User Identification and Authentication

Sequent's Dynix supports the standard UNIX Login facilities that store users' passwords in a one-way encrypted form. Once users are authenticated, they are restricted to a COS/Manager shell that restricts the functions they can perform.

16.6.10 SecurID Authentication

16.6.10.1 General

[ACP] states that people accessing Horizon systems must identify themselves using hand held tokens if:

- they are at sites remote from the Campuses and are able to update the operational systems (for example, to perform systems management actions)
- they have access to the PO Ltd business data (except at Post Office Outlets)
- They are authorised to update system data, which can affect the running of the main operational systems. This includes anyone with UNIX root privilege, Windows NT users belonging to the administrators group and database administrators.

All accesses authorised in this way must be audited.

Horizon uses the SecurID tokens from Security Dynamics for this purpose. Agents are provided for:

- Windows NT
- Unix
- X-Windows

Details are given in [SECURID].

16.6.10.2 Structure

Component	Platforms
SecurID ACE/Server	SecurID ACE Server
SecurID Agent for NT	ACDB Client Workstation ACDB Server Agent Server AP Client Gateway - Local AP Client Gateway - Remote Audit Server Audit Workstation Auto Configuration Signing Server Boot Server Capacity Management Server CM Signing Server
SecurID Agent for NT	Correspondence Server DCS Agent Server DCS Management Server Domain Controller - Local Domain Controller - Remote General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote Horizon Help Desk Terminal KMA Server

KMA Workstation
KMS Admin Workstation
MIS Client Workstation
MIS Support Workstation
NBS Agent Server
Network Banking FTMS Local Gateway
Network Banking FTMS Remote Gateway
OCMS Client
OCMS Server
POCL Standby Gateway - Remote
POCL TIP Gateway Server - Local
POCL TIP Gateway Server - Remote
RDMC Administrator Workstation
SecurID Admin Workstation
Short-term Performance Database Server
SSC Support Server
SSC Support Workstation
Systems Management Access Workstation
VPN Exception Server
VPN Loopback Workstation
VPN Policy File Management Server
VPN Server

16.6.10.3 SecurID and Windows NT

Most users access the system via Windows NT workstations that form part of a Windows NT Domain. Each such workstation includes a *SecurID Agent*. This is a replacement for the GINA process shown in Figure 16.6. The user initially sees the standard Windows NT authentication dialog box. During authentication, it requests a passcode and a secret PIN from the user. The passcode is obtained from a SecurID card that displays a number that changes every minute. The PIN proves that the token belongs to the user.

The SecurID Agent sends the passcode and PIN, suitably obfuscated, to an ACE/Server process running within the Authentication Server at the Campus. This verifies the user's credentials, and returns a yes/no indication to the SecurID Agent.

16.6.10.4 SecurID and UNIX

A *SecurID Agent* is also located on the Sequent servers and SUN Solaris servers. It is a special shell that replaces the standard shell specified in the etc/passwd file. It requests the SecurID number and PIN in the same way as for Windows NT, and passes these to the ACE/Server in the same way. If authentication is successful, the ACE/Server returns the name of a standard shell to be executed.

16.6.10.5 SecurID and X-Windows

Some servers are accessed via X-Windows. For these, the user sees the standard SecurID prompts as part of the X-Windows Login sequence controlled by the **xdm** Login program.

16.6.10.6 ACE/Server

This runs on the SUN based SecurID Server. It maintains two encrypted databases: one with authentication details, and one an audit log of all administration actions and authentication attempts.

The SecurID Server at one Campus is the Primary; the other a Secondary. The Secondary is automatically updated with administrative changes and state changes made on the Primary.

16.6.10.7 TACACS Authentication

Terminal-level authentication is invoked automatically by the Router for Telnet authentication.

TACACS is used, with the TACACS server running on the Network Management Server. Intending users log in to the Router, which sends their authentication details (Username and password) to the TACACS Service. These details are one-way encrypted using MD5. This avoids clear text passwords appearing on the LAN (though they are on the external links in clear).

16.6.11 Authentication in Oracle Databases

The Oracle RDBMS makes use of two authentication methods:

- authentication by the underlying operating system
- authentication by the Oracle Database

All Tables within the Oracle databases are owned by a single “Pathway” user on the corresponding Sequent platform.

Most user processes are run automatically by the Maestro scheduler, and connect directly to designated ports on the Sequent platforms via SQL*Net, rather than via the standard UNIX Login ports.

Direct log-in to the Oracle database applications is restricted to Oracle support. Each of these has a unique UserID and password for the database (as well as a separate Windows NT UserID and password).

16.6.12 Telephone Authentication

16.6.12.1 POLO Recovery Authentication

Telephone authentication is also used for Post Office Managers who have lost their PMMCs or forgotten their PINs. A 15-character alphanumeric PIN is printed by the Gateway PC whenever the content of the PMMC is changed. This is stored in the Outlet's safe. When it is necessary to invoke the POLO recovery process, the Post Office Manager telephones the Horizon Systems Help Desk and the call is transferred to a special desk that deals with this authentication. After authentication, the Help Desk operator sets a flag in the KMA to permit recovery for the Outlet. The KMA is then invoked to deliver a new FEK to the Outlet, and this is written onto a spare PMMC.

If the communications line is not available, there is a fallback route. The Post Office Manager reads out a Recovery Code, and this is typed in by the Help Desk operator. If valid, the operator then reads out a Recovery Key to the Post Office Manager. This enables the Gateway PC to decrypt the recovery PMMC Keys. A new PMMC is then written.

16.7 ACCESS CONTROL

16.7.1 General

Access Control is applied at a resource level. It means verifying that a particular user has the right to access a given resource in a particular way.

Access control is defined in terms of *Roles*, each of which defines a number of functions that a user can use. Effective Access Control depends on having a clear definition of the roles and responsibilities of everyone who needs some form of access to the system. A user may be allowed to use several different Roles, which may or may not provide overlapping sets of functions. Some security systems provide specific support for Roles and for the mapping of services to Roles. Others do not.

Authorisation is the process of determining whether a user has permission to use a particular role, whether this is formally defined or not.

This sub-section defines the functions used to support the operational, management and support roles identified in the [ACP], and the main functions which people in those roles carry out.

16.7.2 Access Control Roles in Pathway

16.7.2.1 Types of Roles

Access control is implemented in terms of Roles. These are of the following types:

- *Post Office Roles*, including Post Office Manager, Counter Clerks and Auditor
- *Operational Roles*, which provide the means to control the Horizon systems during normal running
- *System and Security Management Roles*, which provide the means to maintain and monitor the system, including adding new software and users
- *Support Roles*, such as engineers and applications support

As many of the Horizon functions are automated, control of access by other computer systems is as important as control of access by people.

16.7.2.2 Support of Roles

The way roles and the associated access controls are implemented depends on the products used. For example, Oracle and Tivoli support roles in various ways, and so can use these directly in ACLs. Other products such as Riposte, UNIX and Windows NT support groups or user profiles that can be used to represent roles in a more or less satisfactory way.

Roles are usually associated with groupings of major functions. Defining separate roles allows different functions to be allocated to different users. However, this usually requires some administrative action.

16.7.3 Hardware Access Controls

However secure a computer system is set up, users who can boot a PC from a diskette drive can often override any of the constraints which apply that security policy. Thus, Platforms that provide access to operational systems have their ability to boot from the diskette drive disabled. If possible, the diskette drive itself is disabled. (This is not possible on some Platforms where encryption Keys are delivered on diskette.)

16.7.4 Software Access Control Enablers

16.7.4.1 Access Control in Windows NT

16.7.4.1.1 Access Control Lists and Access Tokens

Figure 16.6 shows how an Access Token is obtained during user authentication and is passed to the user's First Process. Subsequent processes are created by this first process, and the token is passed to them as they are created. When the user tries to access any system resource, his Access Token is checked against the security attributes of the object. If the two match, the user is permitted to access the object. This process requires the use of NTFS which supports access privileges alongside every file.

16.7.4.1.2 Windows NT Domains

Windows NT provides its own domain mechanism. Many of the Horizon servers and workstations run under Windows NT. This sub-section considers how these are assigned to Domains.

16.7.4.1.2.1 Domain Controllers

Each server or workstation can be assigned to a single domain. When users attempt to access one of these, they are authenticated by a *Primary Domain Controller* within the domain. This server contains details of all the users who may access the resources of the domain, and their privileges and attributes. It can be supported by a *Backup Domain Controller*.

The Domain Controller also holds details of other domains of which it is aware, and how much it trusts that domain. If it trusts another domain fully, then it will accept resource requests from members of that domain as if they had originated within its own domain.

The key issue for an enterprise is how these domains are organised.

16.7.4.1.2.2 Domain Structure Policies

The domain structure needs to be set up in a way that supports the Access Control Policies (see [ACP]).

- Users should only be registered as users on Campus servers if they need direct access to them. For example, Pathway management users should not be registered as users on systems such as the Correspondence Servers. They should also not be registered on systems that they always access via a remote client that handles its own authentication, for example Oracle.
- Access Control roles should not be available on systems that do not provide any applications or services within those roles.
- Similar systems (e.g. all Correspondence Servers) should be members of the same domain.

16.7.4.1.2.3 Horizon Windows NT Domain Structure

This is shown below. It is taken from [NTDOM], which elaborates on the structure. Note that it only shows Windows NT Servers; thus some of the sites shown in Figure 4.12 are not included in this diagram.

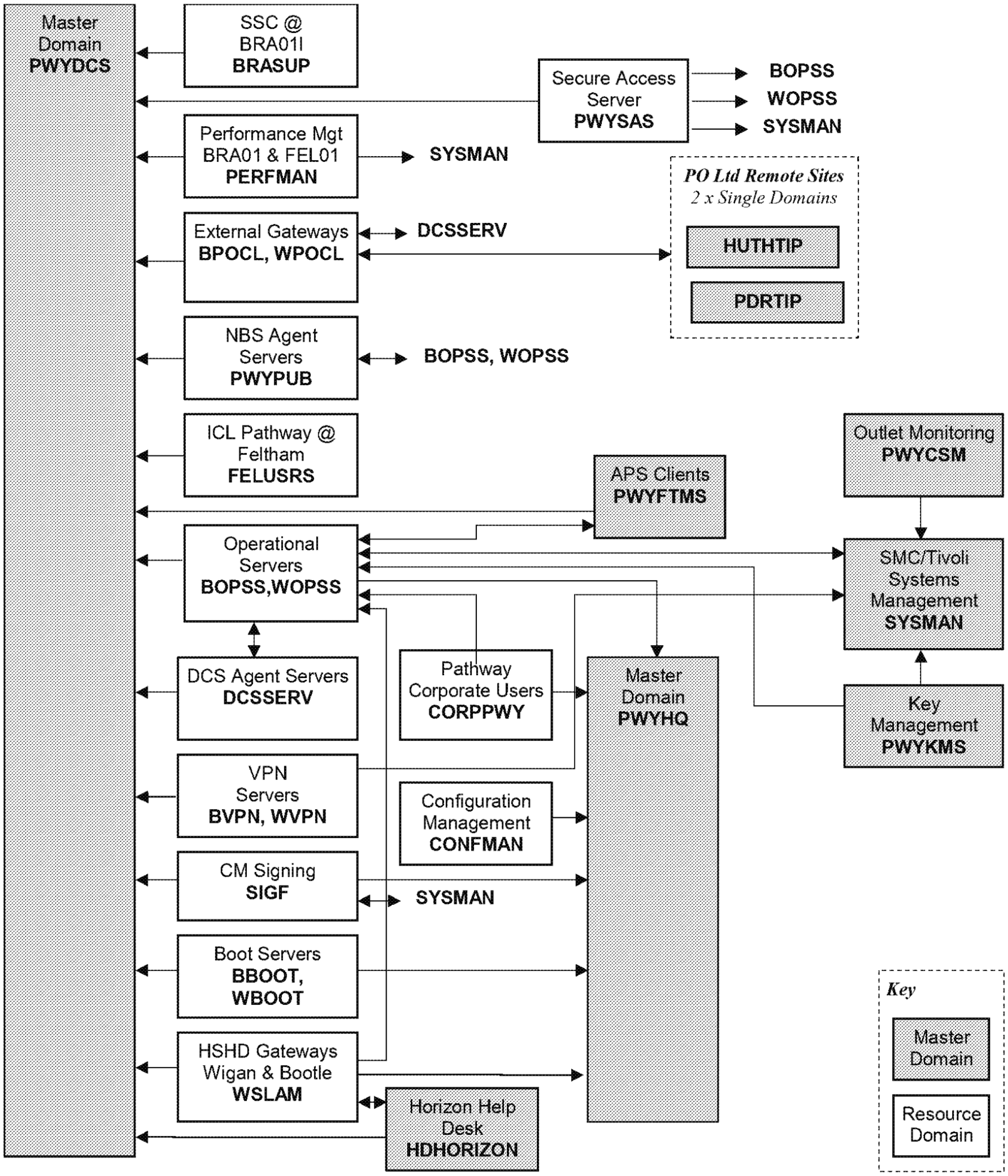
Master Domain PWYDCS
SSC @ BRA01I BRASUP
Secure Access Server PWYSAS
BOPSS
WOPSS
SYSMAN
Performance Mgt BRA01 & FEL01 PERFMAN
SYSMAN
PO Ltd Remote Sites
2 x Single Domains
HUTHTIP
PDRTIP
External Gateways BPOCL, WPOCL
DCSSERV
NBS Agent Servers PWYPUB
BOPSS, WOPSS
ICL Pathway @ Feltham FELUSRS
APS Clients PWYFTMS
Outlet Monitoring PWYCSM
Operational Servers BOPSS,WOPSS
SMC/Tivoli Systems Management SYSMAN
DCS Agent Servers DCSSERV
Pathway Corporate Users CORPPWY
Master Domain PWYHQ
Key Management PWYKMS
VPN Servers BVPN, WVPN
Configuration Management CONFMAN
CM Signing SIGF
SYSMAN
Boot Servers BBOOT, WBOOT
HSHD Gateways Wigan & Bootle WSLAM
Horizon Help Desk HDHORIZON
Key
Master Domain
Resource Domain

Figure 16.7 - Windows NT Domains in Horizon

“Trust” relationships between domains are shown by arrows; the “trusted” domain is the one pointed to by the arrow.

All users are individually registered in the Master Domain. All global groups are also registered in this Master Domain, and specific global groups are granted access to specific local resources. Individual users are not granted access to these local resources; instead, they are granted membership of an appropriate global group within the Master

Domain. Thus, the Master Domain retains the exclusive right to determine which users can access which resource.

16.7.4.1.3 Windows NT Secure Configuration

All Windows NT systems used run under Windows NT version 4.0 with Service pack 6a. Although this provides a high degree of security compared with earlier Microsoft operating systems, there are still some significant loopholes in the default configuration. These include:

- The availability of a "guest" user
- The existence of unprotected communications ports, and software such as *rlogin* and *ftp* which can be exploited to gain access to the system
- The existence of software, such as Task Manager and Windows Explorer, which give an intruder full access to the filestore and processes running on the system
- The fact that by default all files and registry entries are available to everyone

The basic "shrink wrapped" version of Windows NT offers a wide range of facilities on the assumption that the average user will not require a highly secure system on their desktop. This is not the case in Horizon. Counter systems are installed in Post Offices all over the country. There will be natural interest in the security of these systems, from mere hackers as well as those who attempt to subvert the Counter systems, or to hide the evidence of other fraudulent activity.

Thus, all Windows NT platforms use a *Secure NT Build* that enforces a number of restrictions, including the following.

- Disable the Guest account
- Only allow logged-in users to close down the system
- Use solely NTFS as it provides Access Control facilities not provided in the standard FAT filestore.
- Restrict use of the Registry Editor
- Turn on security auditing
- Set User Rights to the minimum necessary to support the necessary workload
- Remove use of the AT (schedule) command as processes started by it have the privileges of the Schedule user, not the issuing user
- Include the system in the appropriate Domains
- Remove the use of services such as *ftp*, Gopher, Remote Access Services and Web publishing services
- Remove NetBIOS bindings

Details are provided in [NTSEC].

16.7.4.1.4 BIOS

The BIOS on all Windows NT platforms is configured to prevent Booting from the diskette or CD drives. An administration password is used to control future access to these configuration features.

16.7.4.2 Access Control in Dynix

Dynix itself provides simplistic access controls that do not meet the security requirements. Thus, the Sequent systems implement the *COS/Manager* product which provides a GUI based interface to users requiring direct access to these servers. It is implemented as a shell that is entered following Dynix Login. COS/Manager provides a menu hierarchy that provides the sole means of access to operating system functions. The functions available to a user can be limited depending on the user's Role.

Access to "root" facilities is especially restricted, and requires a further authentication that is audited.

16.7.4.3 Access Control in Riposte

Riposte provides a number of access control facilities, and these are discussed in Chapter 5 "Application Architectures". Their principal purpose is to control the mapping of Buttons or Impulses onto applications in a controlled way. They also ensure that certain applications are only available in specified Roles, such as the applications reserved for use by PO Ltd Auditors.

Riposte uses the access control facilities of Windows NT to ensure that it is the only system service able to create messages. It adds its own attributes to each message created.

16.7.4.4 Access Control in Oracle

16.7.4.4.1 Databases

Each discrete Database used in the Host Servers will run in a separate UNIX Username. Databases support a list of permitted users and their access rights. Each user is assigned a schema.

16.7.4.4.2 Schemas

Each user declared to the Database has a schema that determines his or her view of the database. Thus, the schema provides a measure of access control on a per-user basis.

16.7.4.5 Access Control in Tivoli

All users of the Tivoli systems are registered at the Tivoli server and associated with appropriate Roles and groups. All access to Tivoli is via Windows NT workstations with ACE/Agent, which authenticate the user as described above.

16.7.5 Network Access Controls

Horizon systems exist in a number of locations:

- Bootle and Wigan Campuses
- Pathway HQ at Feltham
- Outlets
- FSCS Support Centres at Lytham St Annes, Stevenage and Belfast

They are accessed from a number of other locations, principally for support purposes, as identified in Chapter 12 "Systems Management".

16.7.5.1 Firewalls

16.7.5.1.1 General

Firewalls are mechanisms used to protect one part of a Computer network from another, by only allowing traffic to flow between a defined set of network end points on either side of the Firewall. It can carry out some other functions including the following.

- Preventing certain uses or machines from accessing certain servers
- Monitoring communication between networks
- Eavesdropping
- Providing a fine level of control on what types of packet can be sent across the Firewall.

16.7.5.1.2 Need for Firewalls

Some of the PO Ltd Clients with which Horizon interfaces are as concerned about Horizon's access to their network as Pathway is over the converse. If anything, they have more cause for concern, as Pathway installs computer systems (the External Interface Gateways) on their premises. The use of Firewalls is an appropriate technology that is acceptable to both parties. Firewalls restrict access into, out of and within the Campuses.

16.7.5.1.3 Types of Firewall

Chapter 9 “Networking Services” describes the types of Firewalls available, and the conclusions as to which types are used.

16.7.5.1.4 Location of Firewalls

Certain Firewalls are provided by PO Ltd Clients and located on their own premises. These are shown in green in Figure 4.12 of Chapter 4 “Overview”.

Others are deployed by Pathway, according to a business assessment of the risk of external interference with Horizon. These are described in Chapter 9 “Networking Services”. Their locations are shown individually in the diagrams in that Chapter, and Figure 4.12 of Chapter 4 “Overview” shows the position of all Firewalls. [FW] describes in detail the types of traffic permitted by each Firewall.

16.7.5.1.5 Configuration of Firewalls

[FWCONFIG] defines the exact configuration requirements for each Firewall. It takes into consideration the traffic types for various classes of external data access. These include:

- FTMS – NBT over NetBIOS
- Riposte – UDP to a specific port
- Tivoli – TCP/IP to a specific port
- ODBC to SQL Server – NetBeui and NetBIOS
- SecurID – known to Firewall-1
- NT File Sharing – NBT
- Frame Relay (to Boot Server only) – specific ports
- Telnet (for Firewall-1 maintenance)

16.7.5.2 Network Access Domains

The Horizon network is complex and includes systems used for a variety of purposes. Some of these are connected to “outside world” organisations through mechanisms such as electronic mail, as well as including systems used to access the central Horizon data. It is important that the network itself provides separation between these classes of access.

The major network domains are as follows.

16.7.5.2.1 Campuses

These are contained within a secure physical boundary, and most systems within the Campus are part of the general Domain. The exceptions are listed below.

16.7.5.2.2 External Interface Gateways Domain

These are accessed by external bodies, and hence are located on separate LANs that are separated by a Firewall from the main Campus LAN.

16.7.5.2.3 Key Management Domain

This comprises the Key Management Server. This needs special protection because of its position within the security architecture and is thus protected by a Firewall within the overall Campus network.

16.7.5.2.4 Pathway HQ in Feltham

Certain uses in this site require access to the Data Warehouse and MIS systems from Client PCs installed in Feltham. Other Pathway users in Feltham have access to the Fujitsu Services Corporate network, and it is necessary to separate this network from the Campuses. Thus, the Pathway management users with access to the Campus systems are restricted to a secure LAN in Feltham that is separated by a Firewall from the Corporate Network.

Software is developed in Feltham and fed into the main Horizon systems, for example as part of a major software upgrade or to fix particular problems encountered with the operational systems. These upgrades are restricted to passing through a single gateway (the CM Signing Server) which affixes a digital signature to any product passing into the Campuses.

16.7.5.2.5 System Support Centre in Bracknell

This contains the SSC Workstations that need access to the Outlets via encrypted links. These are not connected to the Fujitsu Services Corporate LAN; users have additional workstations, not linked to Horizon, which are.

The SSC also contains the Pathway test configurations. These are separated by a Firewall from the Campus networks.

16.7.5.2.6 FSCS Support and Management Centres (SMC)

These are considered to be part of the Campus networks, as they need access to all systems in each Campus. The links to the Campuses are protected by hardware encryption.

16.7.5.2.7 SMDB

This contains data extracted from the OMDB, but makes it available to a wider set of users than can access the OMDB. It exists within a *De-Militarised Zone* (DMZ) that prevents this wider set of users accessing other servers within the firewall.

16.7.5.2.8 NBS and DCS De-militarised Zones

Further DMZs are used to quarantine the servers that provide access to the NBE (in the case of NBS) and MA (for DCS). The network layout is defined in Chapter 9.

16.7.5.3 Access Lists

The ISDN Routers that are dialled up by Outlets use Access Lists to restrict the TCP/IP addresses that Outlets may access. Access is limited to:

- Correspondence Servers
- Tivoli Managenent Servers

16.7.6 Threat of Virus Infection

The threat of virus infection in most parts of the Horizon system is relatively low.

- Windows NT is used for all Workstations
- Diskette drives cannot be used within Outlets
- There are no E-mail connections to external systems
- Microsoft Word documents (which could contain Word macro virus) are not normally imported
- Operational files transmitted by file transfer contain data rather than executable code
- The main processing Platforms are Unix based.

There is, however, a need to protect against the introduction of viruses from the following external sources.

- Executable files introduced for maintenance purposes
- Microsoft Office documents
- HTML documents containing user Help information.

All Workstations other than those in Outlets have virus protection software (*VirusScan* from Network Associates) installed. This will be updated regularly as new versions are received.

All executable code is virus checked prior to being imported into any part of the system.

All Microsoft Office files (including HTML files) will be checked for macro viruses before they are imported into any part of the system.

16.7.6.1 Structure

Anti-Virus Software is to be installed on the following platforms.

Component	Platforms
Network Associates AV Server Management Console	Systems Management Access Workstation
Network Associates AV Suite - Server	AP Client Gateway - Local AP Client Gateway - Remote Audit Server DCS Management Server General Purpose FTMS Gateway - Local General Purpose FTMS Gateway - Remote Horizon Help Desk Gateway - Local Horizon Help Desk Gateway - Remote
Network Associates AV Suite - Server	Network Banking FTMS Local Gateway Network Banking FTMS Remote Gateway OCMS Server POCL Standby Gateway - Remote POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote SMDB Server SSC Support Server Staging Server
Network Associates AV Suite - Workstation	ACDB Client Workstation Audit Workstation CA Workstation

	Horizon Help Desk Terminal KMA Workstation KMS Admin Workstation MIS Client Workstation MIS Support Workstation OCMS Client One Time Password Workstation Operations Support Workstation RDMC Administrator Workstation SecurID Admin Workstation Service Management Workstation SSC Support Workstation Systems Management Access Workstation Tivoli Support Workstation

16.7.6.1.1 Network Associates Total Virus Defense Suite [sic]

Provided in both Workstation and Server versions, this represents the Network Associates Anti-virus software and latest virus information files. It is updated on a regular basis.

16.7.6.1.2 Anti-Virus Management Console

This runs on a dedicated workstation and is used to manage and initiate the distribution of new virus information files.

16.8 AUDITING

16.8.1 General

Facilities are needed to audit the business and other activities relevant to the integrity of Horizon. These make it possible to store, archive and subsequently restore the audit data. Facilities are provided to enable an auditor to trace audit data at a later stage.

The requirements for auditing are identified in two key documents:

▪ [ATFS]	Audit Trail Functional Specification
▪ [SFS]	Security Functional Specification

Audit facilities must meet the requirements both of the existing applications and of those of new applications that may be developed in the future. Generic facilities are used where possible.

16.8.2 Requirements

Audit is defined as:

> "The examination of an activity and the expression of an opinion on the quality of performance of the activity, conducted by people who are independent of the staff responsible for the performance and supervision of the activity."

The objective of an auditing function is to give a level of assurance of adherence to control requirements and to provide that assurance to a range of internal, legal, regulatory and financial roles.

There are three potential audiences for audit data.

- External auditors
- Security auditors
- Pathway Internal Audit

The main business requirement for audit facilities is to enable Pathway to satisfy the external auditors for PO Ltd and its Clients that Horizon can safely be entrusted with their business data. This *Business Function Monitoring* process involves identifying, collecting and reviewing information relating to the business activities of PO Ltd, its Clients (including DWP BA), Pathway and other staff who have legitimate access to the business processes. It includes auditors analysing historical information relating to PO Ltd and its Clients to detect fraud.

Security Auditors monitor system activities for compliance with Pathway's security requirements and policies, including the activities of Pathway's operations and management staff. *Security Event Monitoring* thus involves monitoring the activities of all users of Horizon, to ensure that:

- They only carry out their assigned activities
- Tthey do not carry out business related activities unless authorised to do so
- Aattempts by unauthorised users to access the Horizon system, or by authorised uses to carry out activities that they are not authorised to do, are detected and recorded.

Pathway Internal Auditors monitor the behaviour of the system and its internal operation to ensure that the business agreements with PO Ltd and its Clients are being adhered to. Subsidiary requirements cover the collection of audit data for fraud detection.

These classes of audit information are inter-related in that logging business activity is meaningless unless each activity recorded can be incontrovertibly associated with a single named individual. The security audit facilities provide the means to ensure that this is possible.

Audit information is recorded within a number of applications and infrastructure components as protection against fraud and against attempted damage to the systems.

Many of the stated requirements relate to particular business level audit tracks. Some are concerned with system level auditing and tend to be rather more generic. However, there are specific requirements that audit data must be provided to record:

- All accesses by an individual
- All access for a specific location
- All accesses of a specific type
- All accesses to specified sensitive data including details of the access type; when, why and where it was undertaken; by whom; and the outcome

Audit data should include log-on and log-off times for each user, recording of data transfers across service boundaries, and auditing of view, as well as update, access to system data.

Audit data needs to be generated as near as possible to the source of the event being audited. Where audit data in its raw state is moved from the location where it is first generated, it is necessary to keep a complete audit trail of the movements of that data. This includes any later restoration to a compatible application and media type for audit analysis. Data that has been manipulated (e.g. stored in a database, filtered, etc.) may be useful for routine monitoring. However, where audit data is to be used for investigations (particularly of fraud) or in Court proceedings, great care must be taken to establish its provenance and integrity.

Audit tracks must be secured so that their integrity is preserved even during system failures. Recovery actions following failures must be audited, as these are potential causes of data corruption.

The audit facilities are described more fully in [ADSR].

16.8.3 Sources of Audit Information

To meet the requirements of both Pathway's and Pathway's Customers, audit information should be logged in response to selected:

- Human activated events, such as Logins
- Automatic system events, such as file transfers from DSS
- Business related events such as user access to a particular data item

The generation of audit-related business information is discussed in Chapter 5 "Application Architecture".

The facilities available to generate audit information are as follows. They are of various qualities. A usable subset of this information is extracted from the Tivoli Event Server and transferred to the Audit Server for storage and analysis. The flow of event information is shown here.

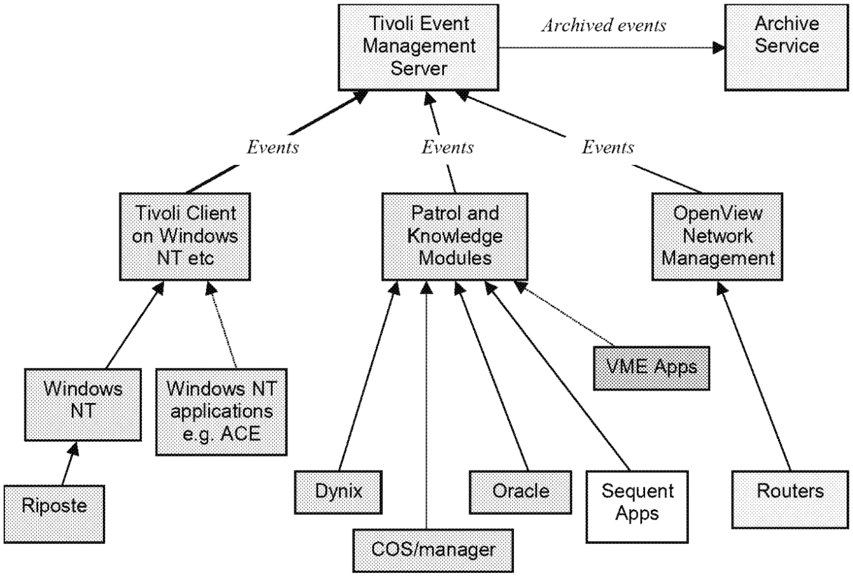
Tivoli Event Management Server
Archived events
Archive Service
Events
Events
Events
Tivoli Client on Windows NT etc
Patrol and Knowledge Modules
OpenView Network Management
VME Apps
Windows NT
Windows NT applications e.g. ACE
Riposte
Dynix
Oracle
Sequent Apps
Routers
COS/manager

Figure 16.8 - Audit Collation by Tivoli

16.8.3.1 Windows NT

16.8.3.1.1 Event Generation

Windows NT uses three logfiles to which records of happenings within the system are written.

- The System log contains errors, warnings or information generated by the Windows NT system and is a pre-set selection of events.
- The Security log records valid and invalid Login attempts and events related to resource use such as creating, opening or deleting files or other objects. The control

of security event auditing is set in the Policies menu of User Manager. The control of file and directory access audits is set through the Security menu in File Manager.

- The Application log contains errors, warnings or information generated by applications and its contents are determined by the application developers.

These records are examined using the Windows NT Event Viewer. Many record such events as the failure of a device driver or a data error from a network card. Windows NT suffers from a common problem with audit systems: a single problem can give rise to a large number of associated audit records that can tend to obscure the original problem.

16.8.3.1.2 Application Monitoring

Applications, including Riposte, can write records to the application log.

16.8.3.1.3 Security Event Monitoring

Security events are audited by first setting up an audit policy to monitor particular types of events. With a domain, this policy applies to the security log of the Domain Controller and all servers within the domain. With a workstation, it applies only to the workstation's security log.

Applications (such as Riposte) can generate their own security events. These are written in the first instance to the Application Log. The application developer defines the particular event type as security-relevant.

16.8.3.1.4 Event Collection

Tivoli is used to extract events from these logs and pass them back to the Tivoli Event Console from where it may be accessed by audit staff.

16.8.3.2 UNIX

Both Dynix and Solarisprovides rudimentary audit facilities, largely confined to material such as the standard UNIX *sulog*. On Dynix, COS/Manager increases the amount of audit data generated in response to user Login, Logout and service selection events.

BMC Patrol provides facilities to intercept Dynix events and convert them into Tivoli events. Components that need to use this facility require a Patrol Knowledge Module. These are needed for Dynix, Oracle, COS/Manager, and for particular applications.

16.8.3.3 Network Components

Routers can generate SNMP traps that are intercepted by HP OpenView and translated, if necessary, into Tivoli events.

Firewalls generate audit logs of connection attempts. These can be retrieved by HP OpenView.

16.8.3.4 External Systems

16.8.3.4.1 VME

VME CAS is used to monitor file transfers to and from these DSS systems, and to pass information back to Horizon.

16.8.4 Resilience of Event Collection

Tivoli cannot guarantee that events are neither lost nor duplicated. It is possible to lose events. For example, if the Tivoli Agent service fails, it is restarted by Windows NT but will lose events that occurred while it was restarting.

It is also possible for event records to get lost in Tivoli due to an "event storm" at the Tivoli event server. It is thus important that the traffic to the event server is properly sized to avoid such event storms. It is expected that most security events requiring immediate action by Pathway will occur at the Campuses, rather than Outlets. These will use the separate event servers for the Campuses, which will not be affected by Post Office events.

16.8.5 Audit Tracks and Audit Trails

It is important to differentiate between these two concepts.

- An *Audit Track* is a sequential record of activities made by a particular subsystem
- An *Audit Trail* is one or more such tracks. It enables an auditor to follow the treatment of related data transfers, movements or accesses by named individuals.

The emphasis in Horizon is on the handling of Audit Tracks. In general, audit trails are manufactured from audit tracks by manual association, and if possible by audit analysis and reporting facilities. The exact scope and nature of these will vary over time as auditors refine their needs and more sophisticated analysis facilities become available.

16.8.6 Audit Management

The generic audit model is shown here. This shows how audit data is managed once it is collected.

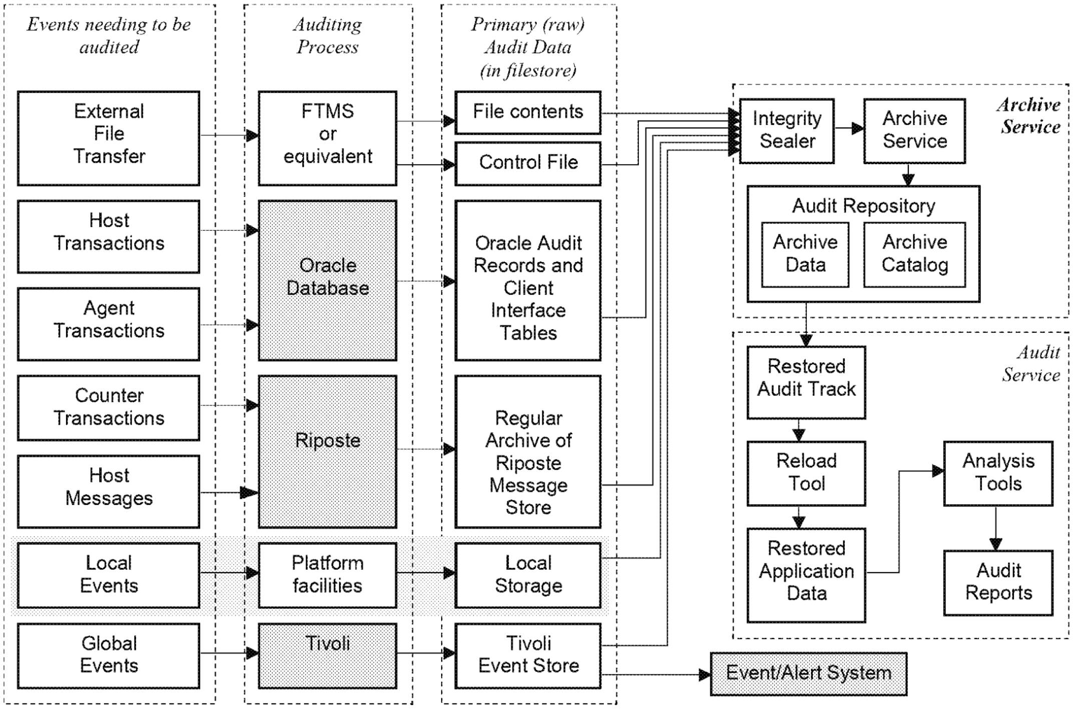

Figure 16.9 - Audit Data Handling

There are four major stages in audit collection and use.

- Audit data is extracted to filestore with a name which reflects it date of collection and provenance. The ensuing audit track is a "black box" so far as any subsequent storage is concerned, and can be sealed for integrity.
- It is written to bulk storage media by a process that need not know its contents or data type.
- It is restored in the same state, as can be verified from its seal.
- It is then loaded into an analysis application by a process that is associated with the application that generated the data in the first place.

16.8.6.1 Structure

Component	Platforms
Audit Agent	Correspondence Server
Audit Checksum Database	Audit Server
Audit Data Retrieval Agent	Audit Server Audit Workstation
Audit Extraction & Filtering Application - Client	Audit Workstation
Audit Server Application	Audit Server
Counter File Audit	Counter PC
FTMS ASB to ASW Local Connection Configuration	Audit Server
FTMS ASB to ASW Remote Connection Configuration	Audit Server
FTMS ASW to ASB Local Connection Configuration	Audit Server
FTMS ASW to ASB Remote Connection Configuration	Audit Server

16.8.6.2 Audit Data Generation

16.8.6.2.1 General

Audit records are generated by local audit facilities. These may be part of the component generating the record (as with Windows NT, Oracle etc.). In some cases, a local audit facility may collect audit records from several components; for example, Windows NT event logs are written to by Riposte and by applications, as well as by Windows NT itself. Audit records may also be collected by monitoring another product e.g. Tivoli picking up Windows NT events, Patrol knowledge modules picking up Oracle events.

Audit information is generated (or presented) as raw filestore files, whose structure is of no further concern to the audit process until that data is retrieved for analysis.

16.8.6.2.2 File Transfer Services

Both the raw file contents, as received from or sent to an external Client, and a Control file which records the date and time of the transfer and other details about it, are archived. The Control File is generated by the FTMS. It should uniquely identify the transferred file in its unencrypted, uncompressed state (for example by use of a seal or hash value) in case of any future dispute about the exact data transferred.

Control files for received files are generated at the Campus end of the transfer. Control files for transmitted files are generated at the external Client site, on the External Interface Gateway PC. These control files are transferred back to the Campus for archiving.

When it is necessary to archive the transferred file, this should be done at the Campus (i.e. it should not be re-transmitted from the remote External Interface Gateway). The Archive Service should copy the file from the transferring system, without the active involvement of the FTMS service, and after the transfer is complete, to avoid impacting any SLAs that the file transfer contributes to.

16.8.6.2.3 Host Transactions

Host applications process files or records received from External Client Systems, and generate messages to go to the Counters via Riposte. Host applications are responsible for generating audit data relating to messages received by on-line external sources (i.e. data not handled by File Transfer).

The application's Client Interface Tables are archived daily. These are used for data transferred to and from the Agents. Where the Host carries out significant processing on persistent data, it also does its own transaction auditing using standard Oracle facilities. Both of these are handled by the application's archive policy. Records are archived to filestore files that are then passed to the Archive Service.

Current applications write their archive data to tape directly from the Host. Should this information need to be retrieved for audit purposes, it will be retrieved to the Audit Server. This is a Windows NT server, and hence should be transferred to this (using NFS) and written to tape from this, rather than from the Host Central Server.

16.8.6.2.4 Counter Transactions and Host Messages

These are recorded automatically by Riposte, and replicated by the Correspondence Servers. New Riposte messages are archived daily. This includes those that are purely transient in nature. This provides a complete audit track of transactions carried out at the Counter and messages sent to the Counter by Host applications. These messages are extracted in the first instance to filestore. The files of "today's" messages are passed to the Archive Service.

It is tempting to filter out transient messages, and [ATFS] §2.1.2.1 implies that this is permitted. However, messages are sequenced, and if any is missing, an auditor is not to know that a transient message, rather than a significant one, was filtered out

Each day the RMS is "purged" of expired messages. Riposte expects that these be archived when they are purged. It is more effective, from the point of view of audit retrieval and analysis, to archive messages when they are generated rather than when they expire, and this is the mechanism that is used.

16.8.6.2.5 Local Events

The way in which these are recorded depends upon the local Platform capabilities. They are stored in the Platform's local storage (for example in the Windows NT event logs). They are not normally archived centrally in their raw format. For example, Windows NT logs are filtered by Tivoli when they are extracted. However, the capability is there to retrieve them in their entirely and this may be considered for a future Release.

16.8.6.2.6 Global Events

These are retrieved by Tivoli (for example from the Windows NT event logs) and passed back to the Tivoli Event Server. Data is extracted from there to filestore for archiving. The extraction process also generates a control file that defines the content and context of the archived data set.

These constitute the Systems Management Audit Track as defined in the [ATFS].

16.8.6.3 Audit Agent

This is a specialised Agent process, running on the Correspondence Servers. It takes a copy of each Riposte message added to the Correspondence Servers and writes it to the Audit Server for storage on DLTs.

16.8.6.4 The Archive Service

Business and Security Audit information (other than that which can be retained purely as local data) is collected by an Archive Service. This seals it, writes it to bulk storage (a Centera disk farm) and creates an *archive catalogue* which records the data stored. The Archive Service expects to receive both the archived audit data, and the Control Files that define the content and context of that data.

- Data presented to the Archive Service is stored unchanged. Thus if there is a need to filter it, for example to remove redundant or replicated records, this should be done when the archive information is first generated. However, this must be done in a way which preserves the integrity and use of the archived data, and any such filtering must thus be agreed with PO Ltd and its affected Clients.
- Data is presented to the archive service, and restored, as complete files, and hence these need to be organised for efficient retrieval. For example, files can be identified by a name that indicates the date of collection and data origin (Riposte, FTMS, Oracle etc.); together with a tag that indicates that the file is available for archiving.

16.8.6.4.1 Audit Checksum Database

The Archive Service appends an integrity seal (e.g. an SHA 160-bit hash value) to files before storing them, and keeps this hash value independently of the file. This can then be used to verify that the file when subsequently retrieved is the same as the file as written.

The Archive Service runs on a powerful Windows NT server with access to large bulk storage facilities.

Data is written at each Campus. In some cases, the same or equivalent data is generated at each campus. Where this is not the case, the collected data is transferred to the other Campus via the Inter-Campus link before it is stored.

16.8.6.5 Audit Track Recovery

16.8.6.5.1 General

The Archive Service stores Flat Files, and can retrieve these as Flat Files if necessary. Each application which "owns" the file structure must provide a process to reload the data from this file into some database storage mechanism.

16.8.6.5.2 Audit Extraction Client Application

An application, running on the Audit Workstation, is used to initiate the retrieval of audit information. It uses information stored on the Audit Server, including the Audit Checksum Database, to determine the location of the relevant audit tracks.

16.8.6.5.3 Access to Riposte Data

Riposte records are retrieved in their raw form, and loaded to an empty RMS on the Audit Server in a form that enables the standard Riposte facilities (Rquery) to be used to browse it. To minimise the size of the RMS, the reload process can filter out records of no interest to the auditor. For example, it should be possible to only load records pertaining to a particular Outlet or set of Outlets.

The Riposte Message Journals contain all records of transactions taking place at the counters, as well as significant amounts of data passed to Outlets. Riposte data is retained in both the Counters and Correspondence Servers. The usual method of access by PO Ltd Auditors and PO Ltd Emergency Auditors will be within the Outlet itself.

Auditor Roles are made available by Riposte, and nominated users may log in with these Roles at any Counter in an Outlet. They will be required to specify a one-shot password that will be made available to them when they telephone the Horizon Systems Help Desk from the Post Office. The Role will determine the classes of data that the auditor is permitted to view. Users logged in with one of these Roles have access to standard Riposte menu-driven facilities that enable them to display and print reports of transactions carried out at the Outlet from the Riposte Journal.

In exceptional circumstances (e.g. if an Outlet is destroyed or all the Counter PCs in it are stolen or vandalised) PO Ltd Auditors and Emergency Auditors may need access to data stored at the Campuses. This is possible via a PC connected to a Correspondence Server.

16.8.6.5.3.1 Access to Oracle Data

Oracle data is archived in a form that enables the database structure to be recreated. Thus if this data is retrieved, it can be used to populate an empty Oracle database on the Audit Server and standard Oracle tools (e.g. Discoverer 20000) can then be used to browse the restored data.

The Oracle reloader, too, should be able to filter out records for (e.g.) Outlets which are not of interest to the auditor.

16.8.6.5.3.2 Access to Flat Files

These are restored onto the Audit Server and can be browsed using any appropriate tool.

16.8.6.5.3.3 Access to Tivoli Data

This is archived in a CSV format, and is restored in that format. It can be browsed via a tool such as Notepad.

16.8.6.6 Audit Trail Analysis

Both regular monitoring and the need to respond to alerts will require the auditor to look at more detailed audit tracks and other data to trace activities. In addition to the above, facilities may be provided, dependent on the application which generated it, to filter, transform (e.g. sort) and otherwise manipulate the data into *Audit Reports*

These facilities do *not* include the ability to modify the raw data. This must be retained unchanged until it is deleted in accordance with the Audit Policy. The use of an integrity seal on the archive files helps to ensure this.

Different types of Auditor require access to different types of data.

16.8.6.6.1 PO Ltd Client Auditors

Auditors appointed by PO Ltd's Clients need similar filtered access to the Riposte journal, and also to the audit tracks representing their own Flat File access to Horizon.

16.8.6.6.2 Security Auditors

Pathway's Security Auditors must have access to Horizon event records. The main ones identified are as follows.

- User administration, user Login records. These are generated by operating systems, system management and middleware products at various Pathway systems as well as the ACE/Server. Windows NT records can be retrieved by Tivoli and fed into the Data Warehouse.
- Records of serious security incidents that were sent to Tivoli as an alert.
- System administration event logs. These are mainly generated by COS/Manager and Windows NT. They are retrieved by Tivoli and fed into the Data Warehouse.
- Other administration logs e.g. Oracle, Riposte, Tivoli, HP OpenView.
- Network management logs.
- Supporting event records e.g. PowerHelp, Software Distribution authorisation at Feltham, manual records etc.
- Records of security specific events such as Key Management ones.
- Access to records in "near real time".

In many cases, the security auditor needs access to archives of the audit logs, not just the current logs.

Business Objects can be used for access to audit information stored in the Data Warehouse.

Access rights should be granted so that specialised, security audit tools can be run to review the security of specific environments and analyse environment-specific audit data.

16.8.6.6.3 Internal Auditors

Pathway's internal auditors require access to the Riposte journals and to information held in the Audit Service and MIS system.

16.8.6.7 Other Reporting, Query and Analysis Tools

Additional tools can be provided in later Releases, where a business case can be made for them, to provide a wide range of reporting, query and analysis functions. For example, these could enable auditors to:

- Obtain regular, ad-hoc and exception reports. For ad-hoc reports, they need to allow selection of records by different criteria/values of particular fields in the records
- Query logs when tracing business, system or user activities
- Query underlying data
- Extract data for forward transmission to PO Ltd etc.

A small number of tools should be used, where possible, to handle the variety of auditor's needs.

16.8.7 Security Alarms

In general, security audit material is used *ex post facto* to look for historic problems. Audit Alarms, on the other hand, are generated in response to certain security events that need to be investigated in "near real time".

The local audit facility normally stores audit records in its local audit track. It may also pass selected records to the event system. This may cause alerts to warn a human user of selected security incidents and possibly also provide records to an audit collection system for regular monitoring. It is a system configurable option whether an Event is treated as an Alert or not. For example, there may be a need for a specific reason to generate an Alert when user x logs on, whereas normally a user Login would not be an alerting function. This type of reconfiguration should be dynamic.

The event system displays events requiring alerts to a system management workstation used for monitoring the Pathway system. The person there rings up a security auditor if a serious security incident has occurred.

Tivoli events are held in the Tivoli event server for a period, and then moved to the OMDB, which is located on the Tivoli Inventory Server. Different views of the set of events can be provided for different uses and are accessed via a Web server and Internet Explorer. A special “security console” for security events is located within the secure area at Feltham.

16.9 CRYPTOGRAPHY

16.9.1 Requirements for Encryption

Cryptography is used for three purposes.

- To protect data on communications links that pass outside the control of Pathway or its suppliers or Customers.
- To protect the integrity of individual messages from creation to use
- To protect the confidentiality of data stored on physically insecure systems such as Counter PCs.

The types of data held or transmitted within the system are defined in [ACP]. Pathway needs to provide measures to protect the integrity or confidentiality of some of these, as follows.

16.9.1.1 Business Data

This includes Reference Data to support EPOSS and transaction data resulting from Post Office Counter activities. It is stored at the main operational systems and in archives. Some is available for management purposes at the Data Warehouse.

16.9.1.1.1 Integrity of Automated Payments

There are two protection requirements:

- Automated payment transactions must be digitally signed at the originating Counter PC. They must be verified on receipt at the Campus by the Agent that feeds them into the AP Host service to guard against tampering as they pass over Outlet link. The verification information must be retained so that verification can optionally be repeated by PO Ltd Clients.
- Files of automated payments and related traffic must be integrity protected.

16.9.1.1.2 Filestore Confidentiality in Outlets

It is expected that Counter PCs will be stolen. They contain personal information about beneficiaries, as well as application security values, cryptographic key material and security control information. All of this data must remain confidential. Specifically, the relevant parts of filestore on Counter PCs must be encrypted.

16.9.1.1.3 Real-Time Transaction Data

Messages generated by the NBS and DCS transactions contain sensitive data (primarily the content of Track 2 on the customer's bankcard). This needs to be protected both in transit and in any records of the transaction stored for audit purposes.

In addition, NBS transactions contain PIN values. Although encrypted within the PIN Pad, these need to be translated to a new Key value before passing them to the NBE.

At the application level, these requirements will be met by digitally signing (and verifying) all [R], [A] and [C] messages exchanged between the Counter and the NBS Agents. For messages generated at the Counter, the signature applies to the XML content of the message, including the PIN Block (if applicable) and encrypted data values (if applicable). For messages generated in the Campuses, the signature is verified when it is returned to the Counter. Transaction messages that fail the signature verification will be cause a "decline" [A] to be returned, and an associated security and application event will be recorded in the System Log files (for onward forwarding to the Security and System management authorities). The signature mechanism (for messages from Outlets to the Campus) uses the *Digital Signature Algorithm* (DSA) with an Outlet unique (private) signing key. This key applies to all Counters within an Outlet. A similar key will sign messages from the Campus to the Outlets, however there will only be one such key.

Further checks are applied to PIN values, including verifyingthe serial number of the PIN Pad on each transaction.

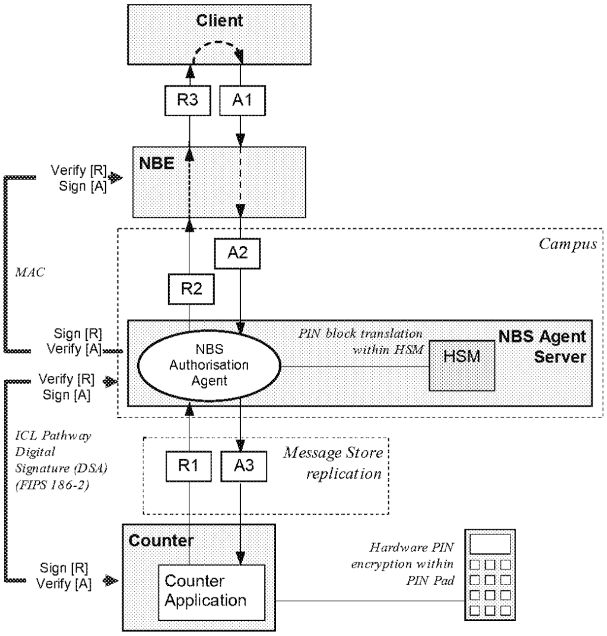

Figure 16.10 – Protection of Authentication Messages

Confirmation [C] messages undergo a more complex process.

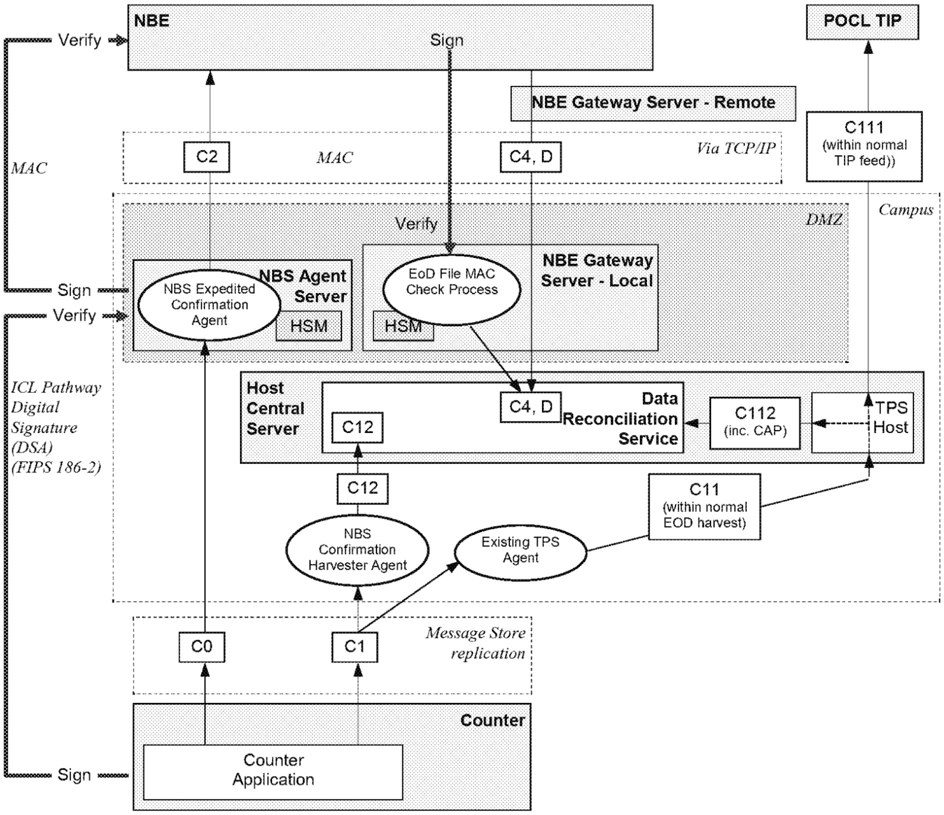
NBE
Sign
Verify
POCL TIP
NBE Gateway Server - Remote
C111
(within normal TIP feed))
C2
MAC
C4, D
Via TCP/IP
MAC
Campus
DMZ
Verify
NBS Agent Server
NBS Expedited Confirmation Agent
HSM
EoD File MAC Check Process
HSM
NBE Gateway Server - Local
Sign
Verify
ICL Pathway Digital Signature (DSA) (FIPS 186-2)
Host Central Server
C12
C4, D
Data Reconciliation Service
C112
(inc. CAP)
TPS Host
C12
C11
(within normal EOD harvest)
NBS Confirmation Harvester Agent
Existing TPS Agent
C0
C1
Message Store replication
Counter
Counter Application
Sign

Figure 16.11 – Confirmation Message Processing

16.9.1.2 Operational Systems Data

This includes the software that supports the Horizon applications and infrastructure, configuration information defining how these are used, Tivoli scripts, system event logs, etc.

16.9.1.2.1 Integrity of Software in Delivery

Software updates delivered through the Tivoli mechanism must be protected against undetected changes. The provenance of the software must be guaranteed.

16.9.1.2.2 Integrity of Software In Situ

After installation, application software on Counter PCs must be protected against undetected changes in situ.

16.9.1.3 Security Information

This includes information about users, their security tokens, Crypto Keys, audit logs etc.

16.9.1.3.1 Confidentiality of Authentication Material

Any information used to verify the identity of users or other system components should be one-way encrypted in storage, and where necessary should be encrypted in transit.

16.9.1.3.2 Confidentiality and Integrity of Key Material

The confidentiality of Private Keys and Secret Keys must be protected at all times. In practice, this means that whenever such keys are exchanged over communications links they must be encrypted. This includes delivery over the central LANs and delivery between central sites. Where Secret Keys are held in system memory on a Windows NT system that is outside Pathway's physical security controls, or a similarly secure environment, the system's swap file must be encrypted.

The integrity of Public Keys must also be preserved.

16.9.2 Types of Encryption

16.9.2.1 Symmetric Encryption

In this, the same key is used to decrypt the data as was used to encrypt it. This key must be known only to the sender and the recipient. The fact that it must be transmitted from one to the other means that there is scope for its compromise unless the key transmission process is adequately protected.

The two parties to a symmetric encryption exchange may not be in a position to determine their shared Key other than over the communications link that they protect. Where this is the case, they use *Diffie-Hellman* techniques to generate and agree a shared secret prior to using it as a session Key.

Symmetric encryption is used for both hardware and software level link encryption, and for encryption of filestore on Counter PCs. The algorithm used is *Red Pike*.

16.9.2.2 Asymmetric Encryption

In this, the data is encrypted with one key and decrypted with another. One of these is the *Private Key*; the other a *Public Key*. Only the owner of the Private Key can decrypt data encrypted with the Public Key. Thus, anyone can encrypt a message using the Public Key and be sure that the encrypted message can be decrypted only by the intended recipient. On the other hand, if the owner of a Private Key encrypts a piece of data using that Private Key, it can be decrypted by anyone using the Public Key. The fact that the decryption process yields some valid data proves that the original message came from the owner of the Private Key, and thus the encrypted data can be construed as a “signature” of the Private Key owner.

Asymmetric encryption is thus used for sealing messages for integrity. It is not used for data encryption.

16.9.2.3 Digital Signatures

This is similar to Assymetric Encryption, in that a two-part Key is used. One part is kept private, and the other is public. The owner of the Private Key uses it to generate a "signature" that it then attaches to some other data. A recipient of this data can then use the associated Public Key to verify that the message in fact originated at the owner of the Private Key.

The algorithm used is the X.509 *Digital Signature Algorithm* (DSA). It is implemented within the Layer7 software. Standard mechanisms are provided, implemented in the File Sign/Verify Library.

16.9.2.4 One-Way Encryption

This is used to encrypt data such that it can never be decrypted. It is used for verifying secret data, such as passwords. The original value is one-way encrypted and the result held within the computer system. If a user supplies a value that yields the same encrypted value, then it can be assumed that the data supplied was the same as the original data.

Another use for one-way encryption is to generate a seal for a piece of data. A hash value is generated which is dependent on the entire content of the data to be protected. If the hash value is generated later, and found to be different to the original seal, then it can be assumed that the data has been tampered with.

One-way encryption is used for both of these purposes. The algorithm used is the *Secure Hash Algorithm* (SHA).

16.9.2.5 Virtual Private Networks

This is used to encrypt all traffic flowing between Outlets and Campuses. It is a variant of Asymmetric Encryption, but differs in that each end is given a Public/Private Key Pair that is certified by a separate CA. At the start of a communications session, the two parties exchange their Public Key Certificates. They validate them against the CA Public Key, and use them to generate a shared secret session Key that is then used for symmetric encryption of the message traffic.

This mechanism is supported by the Utimaco VPN product. It uses RSA principles and implements the Red Pike encryption algorithm.

16.9.3 Constraints on Use of Encryption

16.9.3.1 CESG Guidelines on Encryption Algorithms

The use of cryptography within the UK on Government systems is subject to advice from CESG. Where cryptography is used to control access to information which has a UK national security classification, CESG are empowered to define the cryptography mechanisms and algorithms to be used.

Certain data held within the system is classified as RESTRICTED, and thus CESG rules apply. These mandate the use of a CESG devised algorithm known as Red Pike for protection of data in storage, and either Red Pike or RAMBUTAN for link encryption. Red Pike is a software implementation. RAMBUTAN is a hardware implementation, and hence is not available on all types of link.

Other algorithms are used to protect other attributes, such as passwords. It is understood that there is no requirement for specialised password encryption algorithms.

CESG also permit the use of the *Digital Signature Algorithm* (DSA) for signing messages and the *Secure Hash Algorithm* (SHA) for computing data seals.

16.9.3.2 Certification Authority

Users of Public Keys need to know that the key actually belongs to the stated owner. This is assured by enclosing it in a *Public Key Certificate*, which includes the key itself as well as a *certificate* signed by a Certification Authority (CA) which certifies the validity of keys used within the system.

The CA Private Keys are highly protected. By their nature, they cannot be held in certificates. They are kept away from any computer system in physically highly secure storage (such as a safe), except for the one currently in use in a CA system. A CA Private Key starts expiring when it is transferred from secure storage to the Pathway Certification Authority Workstation Platform, even though this Platform is itself off-line.

16.9.3.3 Routine Key Expiry

Cryptographic keys have a limited life span. All keys held within a computer system must be able to be changed at regular routine intervals defined by the security policy. The shortest normal life is two years. Warnings are given when a key is close to expiring.

CA Private Keys, because they are held off-line, can live longer. This is necessary because changing the CA key means that every key in the system also needs to be changed.

16.9.4 Key Management

16.9.4.1 Structure

Component	Platforms
Key Generator (DSA)	KMA Server KMA Workstation Offline Key Generation Workstation
Key Generator (L&G)	KMA Server KMA Workstation
Key Generator (Red Pike)	CA Workstation KMA Server KMA Workstation
Key Generator (Red Pike) Key Management Application (KMA) Key Store Service	Offline Key Generation Workstation KMA Server Agent Server CA Workstation DCS Agent Server DCS Management Server KMA Server NBS Agent Server Network Banking FTMS Local Gateway Pathway Software Depot PIN Pad Key Generation Workstation
KM Client Agent KM Common Functions	PIN Pad Key Generation Workstation Agent Server CA Workstation Counter PC DCS Agent Server DCS Management Server KMA Server KMA Workstation NBS Agent Server Network Banking FTMS Local Gateway Offline Key Generation Workstation Outsourcing Software Depot PIN Pad Key Generation Workstation PIN Pad Proving Workstation Tivoli Support Workstation
KM Dist Receiver Mon Dispatcher	Counter PC NBS Agent Server Outsourcing Software Depot
KM Interactive Channel Service	KMA Server PIN Pad Key Generation Workstation
KM Interactive Channel Client KM Proxy Server KM Reports	Counter PC VPN Exception Server KMA Workstation KMS Admin Workstation
KMA Agents Common	KMA Server

KMA Bundle Handler	CA Workstation
KMA Bundle Handler	KMA Workstation
KMA Certification Authority	CA Workstation
KMA Common Functions	KMA Server
KMA Database	KMA Server
KMA Help Desk GUI	Tivoli Support Workstation
KMA Server Application	KMA Server
KMA User Interface	KMA Workstation
KMA Workstation Application	KMA Workstation
KMC Automatic Channel - Server-side	Agent Server
KMS Agents	Agent Server
Managed Key Service	Offline Key Generation Workstation

16.9.4.2 Crypto Key Life Cycle

Keys have a well-defined life cycle as follows. This is based upon the ISO 11770 model.

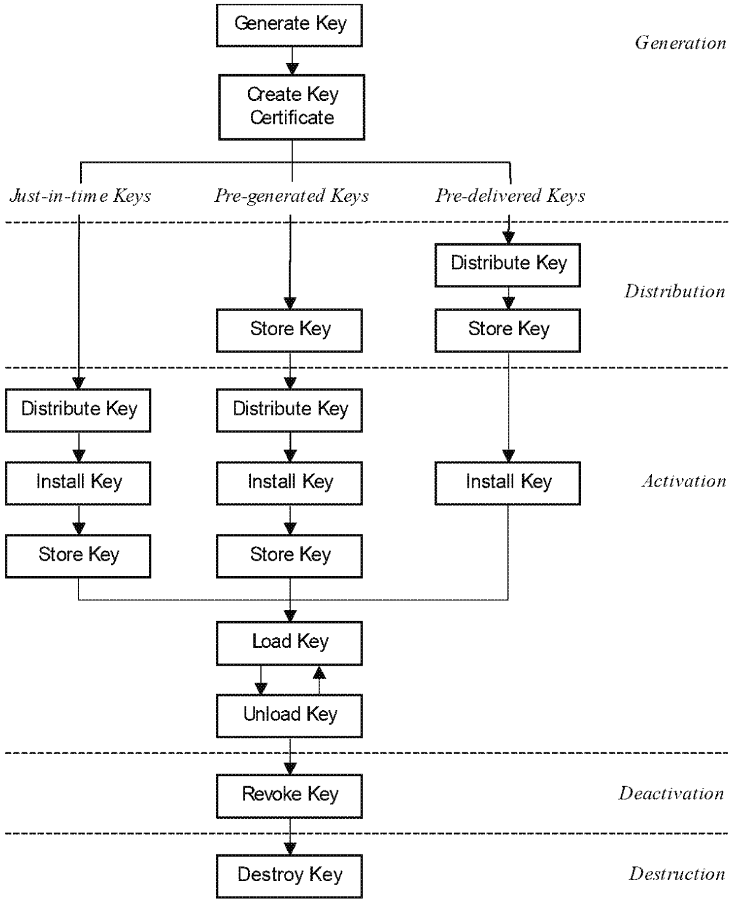

Figure 16.12 - Key Management Processes

Key Management is covered in detail in [KMHLD].

16.9.4.3 Key Distribution Types

Keys can be one of three types.

16.9.4.3.1 Just In Time Keys

These are generated (and distributed, if necessary) immediately prior to activation.

16.9.4.3.2 Pre-Generated Keys

These are generated well in advance of the need to use it, and is stored at a central location until it is due to be activated. Pre-generated Keys are often used where the generation process itself is lengthy. An example is the pre-generation of AP Keys.

16.9.4.3.3 Pre-Delivered Keys

These are generated and delivered to the point of use well in advance of the need to use it. The public components of the PA Public/Private Key Pair held on Counter PCs are examples of this.

16.9.4.4 Key Generation

Keys are created using an appropriate algorithm. Newly generated keys are in a *Pending Active* state.

Some of the keys used are generated by CESG, and delivered and installed using a secure manual process.

Most Keys are generated on the the KMA Server. In some cases they are generated on the Platform on which they are used, or on one close to it. Any Platform that will need to generate Crypto Keys is fitted with a ComScire Random Number Generator. This enables it to generate the entropy needed to protect the Keys.

16.9.4.5 Key Distribution

Distribution involved delivering the Key to the location at which it is to be used. The state remains *Pending Active*.

16.9.4.5.1 Distribution via the Automatic Channel

Keys are normally distributed automatically using the Riposte messaging service. Riposte is implemented on all (Windows NT) Platforms that handle or require Key material. Riposte APIs are provided. These enable the Crypto code to:

- Ascertain its current key set
- Nominate a procedure to be invoked when new key material arrives.

Private Keys sent over this channel are encrypted using a *Transmission Key* (TK), This is delivered manually, on diskette, to any Platform that needs one. Any such Platform must be supplied with a diskette drive.

16.9.4.5.2 Distribution via the Interactive Channel

In certain cases, a Riposte service is not available when a Key needs to be distributed. This is the case with the first use of the PMMC, and when VPN is first used in an Outlet. Instead, the *Interactive Channel* is used. This runs over TCP/IP, and uses a Diffie-Hellman exchange to ensure that both ends of the link are in possession of a secret Key. Monitoring of the use of the Interactive Channel is carried out using Riposte once the Riposte service is running.

16.9.4.5.2.1 KM Interactive Channel Client

This is a Counter component that communicates over TCP/IP with the KMS Application at the Campus. Communication is indirect, going via a KM Proxy Server on the VPN Exception Server to ensure that the channel is valid. This uses the EVPN key.

16.9.4.5.2.2 KM Proxy Server

This runs on the VPN Exception Server, and moderates the interactive channel traffic.

16.9.4.5.2.3 KM Interactive Channel Service

This constitutes the server end of the interactive channel.

16.9.4.5.3 Distribution by Other Means (Manual Channel)

In certain cases, Keys are distributed on a diskette or other removeable media by a human courier.

For example, symmetric keys used by hardware link encryption devices are distributed and installed manually, though the KMA records their existence.

Keys distributed by manual means are usually encrypted using a *Key Encrypting Key* (KEK).

16.9.4.6 Key Activation

Activation involves bringing the Key into use. There are two sub-states of this: *Loaded*, in which the Key is held in processor memory and is available for use, and *Not Loaded*, where it is not.

16.9.4.6.1 Manual Key Activation

Wherever feasible, Private Keys are not held in filestore on the Platforms on which they are used. Instead, they are input manually or via diskette by the Key Custodian during boot up of the Platform concerned, and held in memory on that Platform. A *Key Store Booter* process runs on any Platform (other than a Counter PCd) that needs manual key loading. It is invoked during platform start-up, and is responsible for verifying that the media used and the Keys on it are valid and up-to-date. It loads the relevant Keys into memory.

16.9.4.6.2 Automated Key Activation

Pre-delivered Keys are held in encrypted filestore activated by means of the Riposte Key Management APIs. They are stored in Riposte as Persistent Objects that specify a validity date.

16.9.4.7 Key Deactivation

Deactivation happens when the Key ceases to be used for its primary purpose and is *Revoked*. This may arise because it has expired or because it has been compromised.

16.9.4.7.1 Latency

Some Keys may continue to be used after they are revoked. Keys used for message signing have a *latency* period, in that a message signed with a particular Key may not have that signature verified for some considerable time. During that time, they signing Key may have expired, but the signature must still be valid.

16.9.4.7.2 Key Compromise

If it is suspected that a key is compromise, it must be possible to take immediate steps to change to new values and make the old keys unusable. Potentially compromised Private Keys are revoked through their Public Key. Revocation messages are used to send revocation notifications, signed by the CA, to wherever they are needed (Outlets and/or central verifying servers). Revocation is done by specifying the Public Key to be revoked, not the specific certificate containing the Key, so revocation implies that *all* certificates containing a particular Key must be revoked. CA Keys can be revoked by the CA using a different CA Key. To counter a denial of service attack, a CA Key can only be revoked under the signature of a later CA Key.

File Transfer agents are expected to forward revocation messages, following receipt, with the next file transmitted.

16.9.4.8 Key Destruction

Destruction happens after the Key's latency period, and involves erasing all copies of the Key.

16.9.5 Key Management in Horizon

16.9.5.1 Key Management Application

There is a *KMA Server* (KMAS) in each Campus. A *Key Management Application* (KMA) runs on these servers. It manages the Keys needed by other crypto processes. The Key management database is held in the EMC disk array that holds the Host Central Server data, and is hence automatically replicated across the inter-Campus link.

16.9.5.2 Key Management Agent

A *Key Management Agent* (KM Agent) runs on each Platform that needs access to Crypto Keys. It supports the following functions.

- Install Key from the distribution channel
- Verify and Install a Certificate Relocation List (CRL)
- Load Key
- Unload Key
- Revoke Key
- Destroy Key

16.9.5.3 Key Management Workstation

A KMA Workstation (and backup) is provided to enable the Key Custodian to carry out his duties.

A separate KMS Admin Workstation is provided for the administration of the KMA Database.

16.9.5.4 Key Protection

Keys must be protected in transit to their designated locations, and in use. Public Keys are protected against protection by a Digital Signature that includes a seal (hash) of the Key.

Private Keys are protected by encryption under another Key, called a *Key Encryption Key* (KEK). For example, they may be held in an encrypted filestore area. The KEK is usually stored off-line, for example in a diskette or in the PMMC.

16.9.5.5 Key Store Service

This is a KMS component that resides on each platform for which the KMA distributes keys. It maintains active keys in filestore for use by the Layer7 code.

16.9.6 Use of Encryption

Encryption is required to protect the following data transfer operations. [KMP] lists the Platforms that require Key management functions. Those affected at BI3 are as follows.

Protection Domain	Sending Platform	Key Name	Receiving Platform	Key Name	Number
Software Issue	Auto-Configuration Signing Server SI Signing Server	SIPR	Counter PC	SIPU	1
Automated Payment Records	Counter PC	APPR	Agent Server	APPU	20,000
Counter PC Filestore Encryption	Counter PC	FEK POK	n/a	N/a	20,000
Counter PC Key protection	KM Server/Workstation	TK	Counter PC		20,000
VPN	VPN Servers VPN Exception Server Counter PC - Gateway	NVPN	N/a	N/a	20,000
L&G	Counter PC	L&G(E)	N/a	N/a	20,000
NBS/DCS messages to Campus	Counter PC	OCPR (aka APPR)	Agent Server	OCPU (aka APPU)	20.000
NBS/DCS messages to Counters	NBS/DCS Agent Server	COPR	Counter	COPU	1
NBS Agent to NBE (MAC)	NBS Agent Server	NBMCC/ NBTDC	NBE		1 per Agent
NBE to NBS Agent (MAC)	NBE	NBMCN	NBS Agent		1 per Agent
NBS/DCS sensitive data encryption	Counter PC	NBTDO	Agent Server	NBTD O	1
NBS PIN Block encryption	Counter PC	NBPO	Agent Server		1 per Counter
NBS Agent PIN Block translation	NBS Agent	NBPC	NBE		1 per Agent
Campus-NBE Link level encryption	Hardware	NBLE	Hardware		
DCS servers filestore encryption	DCS servers	NFEK	n/a	NFEK	8

Table 15 - Transfers Protected by KMS

16.9.6.1 Software Distribution

Software is generated in the Pathway site at Feltham and transmitted to FSCS for distribution. It is first signed by the CM Signing Server or Auto-Configuration Signing Server, using the SI Private Key (SIPR). This is delivered via the Automatic Channel.

The signature is verified by the Outsourcing Software Depots. The software package includes the PKC that holds the corresponding Public Keys (SIPU). Verification occurs immediately prior to distributing the software to its destination platforms.

Pathway has the ability to sign desktop applications, such that their authenticity and integrity can be automatically verified by Riposte when they are loaded onto the Desktop. Software is signed using standard Microsoft cryptography, with a 512 bit RSA key. Microsoft has authorised Escher Group to sign software that Windows NT will verify, when asked to do so via the Windows NT CryptoAPI. Escher has similarly authorised Pathway to sign software distributed to Campuses and Outlets. This chain of trust thus depends on:

- Microsoft's Private Key, held securely in Redmond, and a Public Key embedded in Windows NT
- Escher's Private Key, held securely in Boston Massachusetts, and a Public Key held in a Public Key Certificate signed by Microsoft
- Pathway's Private Key, held in a secure central site, and a Public Key held in a PK certificate signed by Escher and distributed to appropriate Platforms using Riposte.

16.9.6.2 Automated Payment Records

Riposte messages recording automated payments are signed at the Counter PC using an AP Private Key (APPR) that is delivered using the Automatic Channel. The signature remains encapsulated with the message until it arrives at the AP Client. The AP Public Key (APPU) is delivered to each AP Client in a Public Key Certificate signed by the current CA Key. It enables the Client to verify the signature on AP payment records.

16.9.6.3 NBS Key Usage

The following diagram shows which keys are used when processing [R] messages. In this case, certain material comprising the messages originates at the PIN Pad.

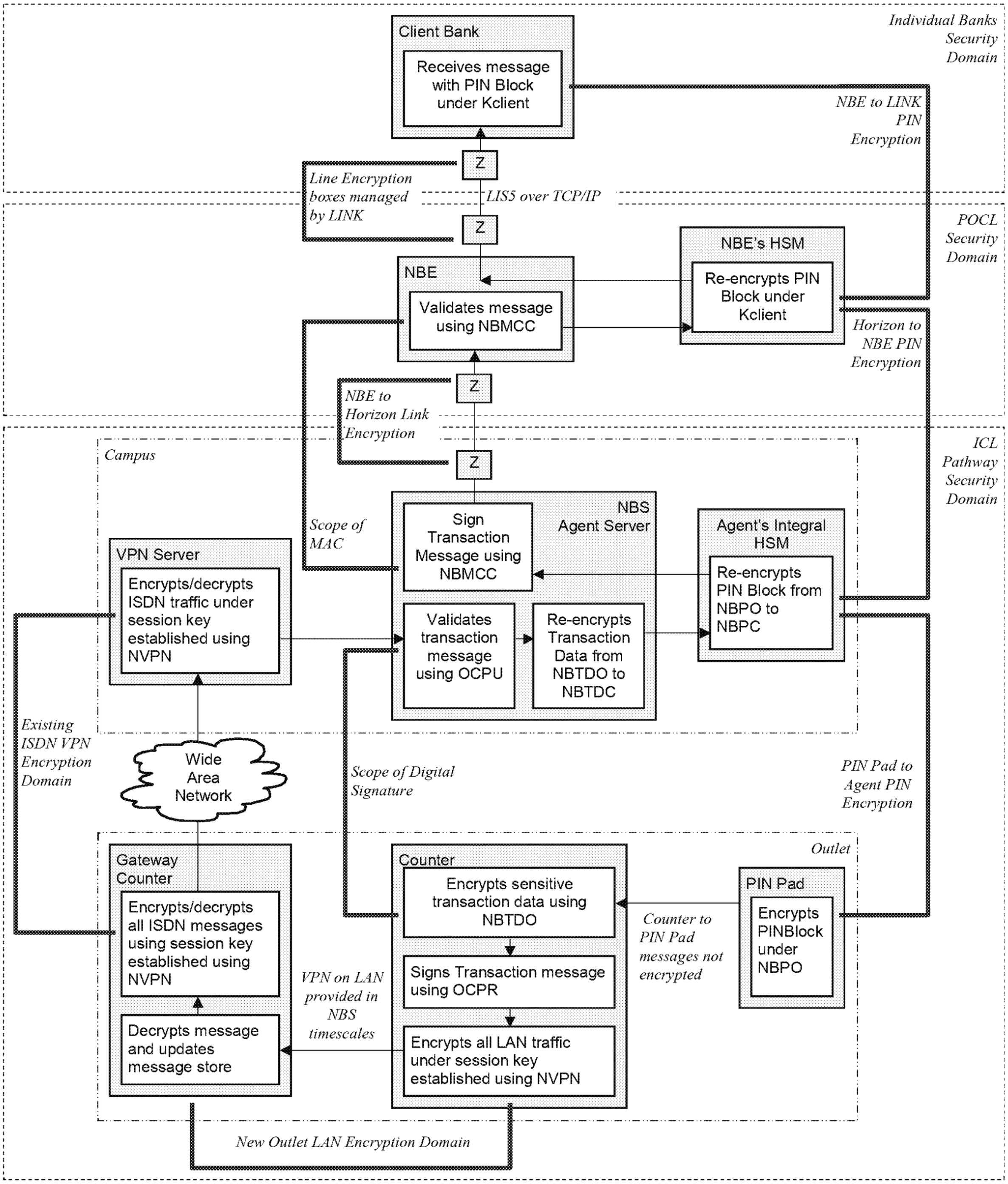
Individual Banks Security Domain
Client Bank
Receives message with PIN Block under Kclient
NBE to LINK PIN Encryption
Z
Line Encryption boxes managed by LINK
LIS5 over TCP/IP
Z
POCL Security Domain
NBE's HSM
Re-encrypts PIN Block under Kclient
NBE
Validates message using NBMCC
Horizon to NBE PIN Encryption
Z
NBE to Horizon Link Encryption
Z
ICL Pathway Security Domain
Campus
Scope of MAC
NBS Agent Server
Sign Transaction Message using NBMCC
Agent's Integral HSM
Re-encrypts PIN Block from NBPO to NBPC
VPN Server
Encrypts/decrypts ISDN traffic under session key established using NVPN
Validates transaction message using OCPU
Re-encrypts Transaction Data from NBTDO to NBTDC
Existing ISDN VPN Encryption Domain
Wide Area Network
Scope of Digital Signature
PIN Pad to Agent PIN Encryption
Outlet
Gateway Counter
Encrypts/decrypts all ISDN messages using session key established using NVPN
Decrypts message and updates message store
VPN on LAN provided in NBS timescales
Counter
Encrypts sensitive transaction data using NBTDO
Signs Transaction message using OCPR
Encrypts all LAN traffic under session key established using NVPN
Counter to PIN Pad messages not encrypted
PIN Pad
Encrypts PINBlock under NBPO
New Outlet LAN Encryption Domain

Figure 16.13 – Use of keys in [R] and [C0]/[C2] Messages

The following diagram shows the simpler structure used when processing [C] messages. In this case, the material comprising the messages originates at the Counter and does not contain the PIN etc.

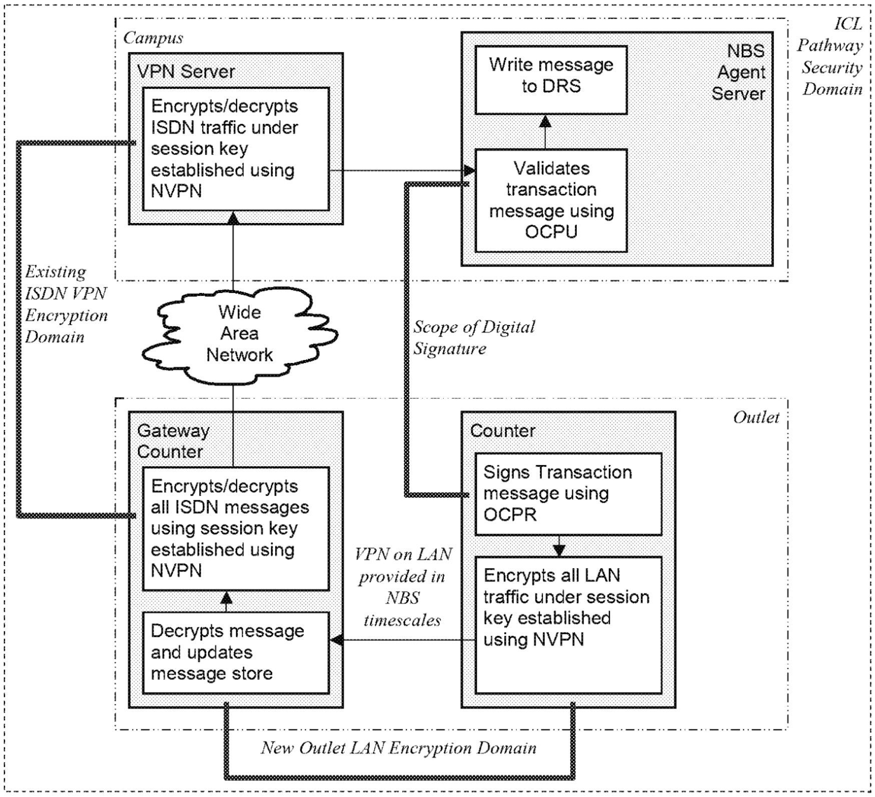
Campus
VPN Server
Encrypts/decrypts ISDN traffic under session key established using NVPN
Write message to DRS
NBS Agent Server
Validates transaction message using OCPU
ICL Pathway Security Domain
Existing ISDN VPN Encryption Domain
Wide Area Network
Scope of Digital Signature
Outlet
Gateway Counter
Encrypts/decrypts all ISDN messages using session key established using NVPN
Decrypts message and updates message store
Counter
Signs Transaction message using OCPR
Encrypts all LAN traffic under session key established using NVPN
VPN on LAN provided in NBS timescales
New Outlet LAN Encryption Domain

Figure 16.14 – Use of keys in [C] Messages

The following diagram shows which keys are used when processing the [A] messages. In this case, messages are only sent from the NBE to the Counters via the, (appropriate) Agent layer.

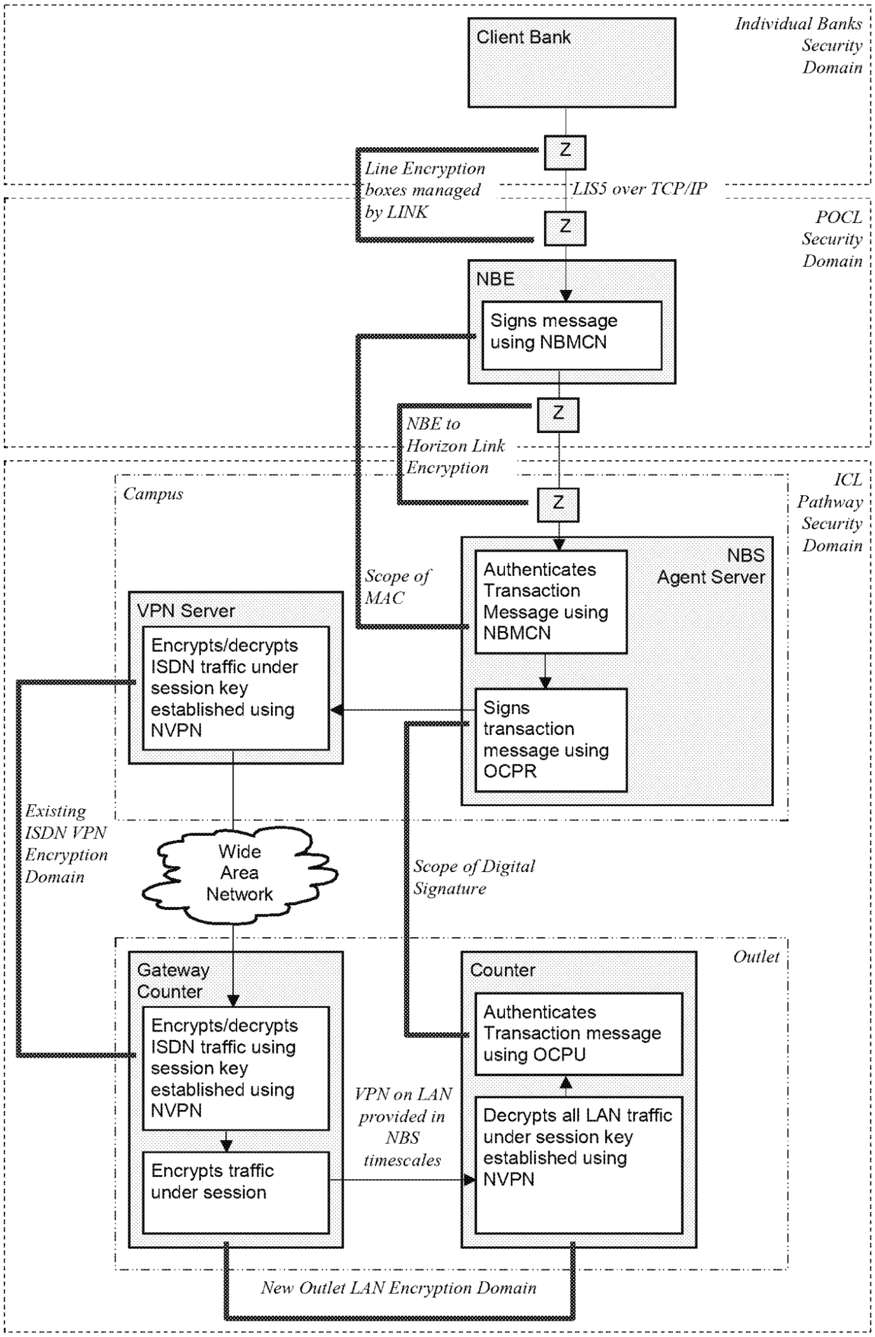
Client Bank
Individual Banks Security Domain
Z
Line Encryption boxes managed by LINK
LIS5 over TCP/IP
Z
POCL Security Domain
NBE
Signs message using NBMCN
Z
NBE to Horizon Link Encryption
Z
Campus
ICL Pathway Security Domain
NBS Agent Server
Authenticates Transaction Message using NBMCN
Scope of MAC
VPN Server
Encrypts/decrypts ISDN traffic under session key established using NVPN
Signs transaction message using OCPR
Existing ISDN VPN Encryption Domain
Wide Area Network
Scope of Digital Signature
Outlet
Gateway Counter
Encrypts/decrypts ISDN traffic using session key established using NVPN
Encrypts traffic under session
VPN on LAN provided in NBS timescales
Counter
Authenticates Transaction message using OCPU
Decrypts all LAN traffic under session key established using NVPN
New Outlet LAN Encryption Domain

Figure 16.15 – Use of keys in [A] MessagesCounter PC Filestore Encryption

Most Horizon systems holding data that requires protection are located in physically secure areas. They are not considered to need any further protection.

The principal exception is the Counter PC. It is certain that some of these machines will be stolen from Outlets. Any sensitive data held on them should not be readable by the thief or anyone else, and it must not be possible to use a stolen Counter PC to access the Horizon network.

16.9.6.4.1 Filestore Encryption

This is satisfied by encrypting sensitive data on the disk, using the symmetric Red Pike algorithm. Data encrypted includes the swap file (which may contain Key values in clear) and the Riposte Message Store. The *Filestore Encryption Key* (FEK) is generated during Outlet installation and stored in encrypted form on the Post Master's Memory Card (PMMC). The encryption Key is a PIN value that is also generated during the installation process and printed on the Counter PC's printer. The Post Office Manager must use the PMMC and specify the PIN when switching on a Counter PC.

16.9.6.4.2 TeamWARE Crypto

Filestore encryption is performed by *TeamWARE Crypto* (TWC), which sits under Riposte and other disc "users". It is linked into the disk subsystem. TeamWARE Crypto has been enhanced for Pathway to use the Red Pike algorithm. The enhancement also includes encryption of the Windows NT Swap File, and enhancements of the Crypto API to operate with Riposte

However, note that:

- The advent of the KMS and associated crypto facilities means that TeamWARE Crypto must not be used for any future encryption operations other than those for which it is currently used.
- TeamWARE Crypto is no longer supported by Fujitsu and hence its use even for these existing purposes will be reconsidered

16.9.6.4.3 POLO Recovery

Pathway's recommendation is that Counter PCs are switched on at all times., and so the boot-up process will be rare. Should the Post Office Manager mislay either his PMMC or PIN, he must telephone the Horizon Systems Help Desk and authorise the delivery of replacement keys via the Interactive Channel.

Keys are changed every two years. This involves inserting the PMMC into each Counter PC in turn, at a quiet period, and invoking a desktop application to load the new values. This process will cause the Counter PC filestore to be re-encrypted.

16.9.6.5 DCS Servers Filestore Encryption

The other major use of TeamWARE Crypto is in the DCA Agent Servers. These hold data, including sensitive data, "in clear" as this is required by the Retail Logic software. Filestore encryption is used to protect this data.

16.9.6.6 Transmission from OBCS$_D$ to Horizon

Pathway accepts ESNCS information within the VME ESNCS machines on the DSS sites. Pathway is responsible for the integrity of that information from then on.

The protection used is aimed at protecting the integrity of the transmitted data. The binary values in file hash total and sub-total records are software encrypted and integrity protected at application level under Red Pike using manually loaded Key Values. In particular a (non-cryptographic) cyclic redundancy check over the whole file and the financial total fields are protected

The link to the Campuses is over the Energis ATM network using Frame Relay over 2 Mbps links.

16.9.6.7 PO Ltd TIP and Reference Data Link

TIP is the primary mechanism by which PO Ltd will collect records of all transactions that occur at all Outlets. Reference Data is sent to Pathway to record changes to Outlets, and to other data that affects the operation of the Counter services. The link uses 2 Mbps Frame Relay PVCs over the Energis ATM network.

TIP data and Reference Data is integrity protected by digital signature in both directions. Signing is chosen in preference to symmetric sealing because it is clearer in determining responsibility when key compromises happen.

16.9.6.7.1 TIP Data

TPS Data to TIP is sealed on the local PO Ltd TIP Gateway using the PWY TIPPR. This is delivered to the Gateway via the Automatic Channel. The seal is verified on the remote Gateway, using the PWY TIPPR. This is also distributed via the Automatic Channel, along with the CAPU and any revocation information.

16.9.6.7.2 Reference Data

Reference Data from PO Ltd is sealed on the remote POCL TIP Gateway using the POCL TIPPR. This is delivered to the Gateway via the Automatic Channel. The seal is verified on the local Gateway, using the POCL TIPPR. This is also distributed via the Automatic Channel, along with the CAPU and any revocation information.

16.9.6.8 Outlet Links

The links to the Outlets from the Campuses are protected using the VPN mechanisms described in Chapter 9 "Networking Services". They use the Red Pike algorithm. New Keys are distributed to VPN servers using the Automatic Channel, encrypted under a PIN that is delivered manually.

VPN Keys are delivered to Counter PCs via the Interactive Channel.

16.9.6.9 Hardware Protected Links

16.9.6.9.1 Inter-Campus Links

There are a number of different data flows between the two Campuses:

- Riposte Message Store replication
- Oracle SQL*Net traffic
- Symmetrix remote disc mirroring
- Key distribution
- Systems management traffic
- Operations traffic

The physical characteristics of the high-speed connections between the Campuses give a significant level of inherent security. Furthermore, given the speed of these links, there are no commercially available in-line encryption devices available. However, certain data is very sensitive (e.g., encryption keys) and such traffic will be software encrypted before transmission.

16.9.6.9.2 Horizon Systems Help Desk and System Management Workstations

These are the management links from Pathway for support of both central site systems and Counter PCs. It includes links from FSCS into the Campuses.

System modifications (e.g. repairing of faults) can be done through these links, so authentication should be strong (proofed against eavesdropping) and thus data should be transmitted integrity protected at least as far as the Campus. More generally, system management functions can cause changes to security sensitive data on Campus machines, forming a serious security threat. Static link-level encryption is used on these lines, as illustrated in Chapter 9 "Networking Services", using Zergo supplied RAMBUTAN encryption units. These are available for 128 Kbps and 2 Mbps line speeds. The links used operate at 128 Kbps or 256 Kbps. Keys are generated by CESG and installed by FSCS using standard Zergo operating processes.

16.9.6.9.3 External Support Links

Chapter 12 "Systems Management" Identifies the requirements to enable remote support and management of system components from outside the Campuses. Most of these links are protected by hardware encryption, as shown in the following Table.

Company	Location	What Supported	Access Needed	Protection
Cisco	UK and Brussels	Software on Routers	Some Cisco engineers need "enable" access so that they can update Router configuration	ISDN, CLIP etc., not encrypted
EMC	UK, Cork and USA	Symmetrix disc unit (first line support)	Details not yet clear - is DSS data visible? (thought not?); can update disc configuration	Modem/ISDN? (would need encryption if DSS data)
General Signals	UK	Software/hardware support of network communications linking Symmetrix to Energis	Details not known; are they close enough to come to Campus?	ISDN/modem
SSC	Bracknell	3rd line support of some applications and middleware e.g. PO apps, Riposte, cryptographic s/w	Read only access to many operational Campus systems	Hardware based RAMBUTAN
FSCS Belfast	Belfast (on site only, home based access not allowed)	Operational system management at Campuses and VME	Sequent and some/all? NT at Campuses; VME applications Access as [ACP]	Hardware based RAMBUTAN
		Management systems and applications	Data Warehouse, SLAM etc.	Hardware based RAMBUTAN
FSCS SMG	Stevenage, Lytham. Bracknell	System management - Tivoli etc.	Management servers, Correspondence Servers	Hardware based RAMBUTAN

Table 16.1 - Protection of Support Links

16.9.6.10 Crypto Keys

The following table shows the keys used in Horizon, the platforms on which they are installed, and the routes used to deliver them.

Component	Platforms
Crypto Keys - (APPR)TK via Automatic Channel	Counter PC
Crypto Keys - (GDK)TK via Automatic Channel	Counter PC
Crypto Keys - (KIPR)KMAK	KMA Server
Crypto keys - (KMA Key)TK via SQL	KMA Server

	KMA Workstation
Crypto Keys - (NBTDO)TK via Automatic Channel	Counter PC DCS Agent Server NBS Agent Server
Crypto Keys - (NVPN)PIN via Automatic Channel	Counter PC VPN Loopback Workstation VPN Server
Crypto Keys - (NVPN)PIN via PMKM	VPN Loopback Workstation VPN Server
Crypto Keys - (NVPN)TK via Automatic Channel Crypto Keys - (SIPR)TK via Automatic Channel	Counter PC Auto Configuration Signing Server CM Signing Server
Crypto Keys - AP Client Remote Crypto Keys - APPU PKC via automatic channel	AP Client Gateway - Remote Agent Server DCS Agent Server NBS Agent Server PIN Pad Key Generation Workstation
Crypto Keys - Audit Server Crypto Keys - CAPR (Black) via Diskette Crypto Keys - CAPR (Red) via Diskette Crypto Keys - CAPU Checks via Automatic Channel	Audit Server CA Workstation CA Workstation CA Workstation Counter PC KMA Server KMA Workstation
Crypto Keys - CAPU Set via Tivoli	Agent Server DCS Agent Server
Crypto Keys - CAPU Set via Tivoli	NBS Agent Server PIN Pad Key Generation Workstation
Crypto Keys - CAPUs (Initial) via Build or Tivoli	Outsourcing Software Depot Pathway Software Depot POCL TIP Gateway Server - Local POCL TIP Gateway Server - Remote
Crypto Keys - CRL via Automatic Channel	Agent Server Counter PC DCS Agent Server NBS Agent Server Outsourcing Software Depot Pathway Software Depot PIN Pad Key Generation Workstation POCL TIP Gateway Server - Local
Crypto Keys - CRL via Manual Crypto Keys - CRL via zip drive	POCL TIP Gateway Server - Local CA Workstation KMA Server
Crypto Keys - DLLKA via Interactive Channel Crypto Keys - DLLKA via PMMC Crypto Keys - DLLKA/B from L&G via Diskette	Counter PC Counter PC - Non-Gateway KMA Server KMA Workstation
Crypto Keys - DLLKB via Automatic Channel Crypto Keys - EVPN (common) via Build or Tivoli Crypto Keys - FEK (Outlet-specific) from Gwy via PMMC Crypto Keys - FEK (Outlet-specific) via Interactive Crypto Keys - FTPPR (Black) via Diskette	Counter PC Counter PC Counter PC (non-Gateway) Counter PC AP Client Gateway - Local Network Banking FTMS Local Gateway
Crypto Keys - FTPPR (Red) via Build	AP Client Gateway - Local Network Banking FTMS Local Gateway
Crypto Keys - FTPPU via Build Crypto Keys - GDK via Diskette Crypto Keys - In-line SAPU PKC via Riposte Crypto Keys - IPOK Set via Diskette	AP Client Gateway - Remote KMA Workstation Counter PC Boot Server KMA Workstation
Crypto Keys - KIPU PKC in-line via Interactive Channel Crypto Keys - KIPU PKC In-Line via zip drive Crypto Keys - NVPN (Outlet specific) via Interactive Crypto Keys - NVPN (Outlet specific) via Interactive	Counter PC CA Workstation Counter PC Counter PC - Non-Gateway Counter PC - Standalone
Crypto Keys - NVPN set via diskette	KMA Server KMA Workstation
Crypto Keys - POCL TIP Remote Gateway Crypto Keys - POCL TIPPR (Black) via PMKM	POCL Standby Gateway - Remote POCL Standby Gateway - Remote POCL TIP Gateway Server - Remote
Crypto Keys - POCL TIPPR (Red) via PMKM	POCL Standby Gateway - Remote POCL TIP Gateway Server - Remote

Crypto Keys - POCL TIPPU PKC via Build Crypto Keys - POK (Initial) via BSF Crypto Keys - POK (Outlet specific) via Interactive Crypto Keys - POK (Outlet specific) via PMMC Crypto Keys - PWY TIPPR (Black) via PMKM Crypto Keys - PWY TIPPR (Red) via PMKM Crypto Keys - PWY TIPPU PKC via Build Crypto Keys - SA KEK via Diskette	POCL TIP Gateway Server - Remote Counter PC Counter PC Counter PC - Non-Gateway POCL TIP Gateway Server - Local POCL TIP Gateway Server - Local POCL TIP Gateway Server - Local Agent Server DCS Agent Server NBS Agent Server PIN Pad Key Generation Workstation
Crypto Keys - SAPR via Build	Agent Server NBS Agent Server PIN Pad Key Generation Workstation
Crypto Keys - SAPU PKC via Build	Agent Server DCS Agent Server NBS Agent Server
Crypto Keys - SI Verifying Crypto Keys - SICERT via Build	Counter PC - Standalone Auto Configuration Signing Server CM Signing Server
Crypto Keys - SIPR (Black) via Build	Auto Configuration Signing Server CM Signing Server
Crypto Keys - SIPR (Red) via PMKM	Auto Configuration Signing Server CM Signing Server
Crypto Keys - SIPU PKC via AutoConfig or Tivoli Crypto Keys - SIPU PKC via Automatic Channel	Counter PC Outsourcing Software Depot Pathway Software Depot
Crypto Keys - SIPU PKC via Build	Auto Configuration Signing Server CM Signing Server
Crypto Keys - TK (Outlet specific) via Interactive Crypto Keys - TK (Outlet specific) via PMMC Crypto Keys - TK via Manual Crypto Keys - TK via Manual	Counter PC - Gateway Counter PC – Non-gateway Audit Workstation DCS Agent Server KMA Server NBS Agent Server
Crypto Keys - VPN CRL via Automatic Channel	Counter PC VPN Exception Server VPN Loopback Workstation VPN Server
Crypto Keys - VPN CRL via PMKM	KMA Server VPN Exception Server VPN Server
Crypto Keys - VPN PIN via Manual	VPN Loopback Workstation VPN Server
Crypto Keys - VPN Sec Data Crypto Keys - VPN Server	CA Workstation VPN Exception Server

16.10 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 15	Performance	Discusses the measures taken to ensure high levels of performance, throughput and response times in Horizon
Next	Chapter 17	Potential for Change	Discusses the ways in which Horizon can be enhanced in response to new business requirements or changes in the underlying technology
ACP	RS/POL/003	Access Control Policy	Defines the ways in which access to the Horizon systems are to be controlled. The purpose of the security architecture is to provide the means to control access in this way.
AUDITARC	TD/ARC/016	Audit Architecture	Defines the architecture for the provision of audit collection, retrieval and analysis within Horizon
CRYPT	RS/DES/001	Cryptography Design	Describes the use of cryptography within Horizon.
CRYPTA		Cryptographic Architecture	Outlines the architecture for the use of cryptography within Horizon
FW	TD/DES/038	Firewall Requirements	Discusses the nature of Firewalls, the requirements for their use in Horizon, and the points at which they will be introduced. A more up to date description of these, and

			other aspects of the Network, is given in [NWD].
KMHLD	RS/DES/010	Key Management High Level Design	Describes the mechanisms used to manage Crypto Keys
KMP	RS/DES/020	Key Management Platforms	Discusses the Platforms that are involved in managing Key distribution, or on which Keys need to be installed.
NTDOM	RS/DES/005	Proposed NT Domain Design	Describes the Horizon Windows NT domain strategy
NTSEC	RS/DES/037	NT Platform Security Framework	Describes the mechanisms used to configure NT Server and Workstation platforms securely
NWD	TD/DES/059	Network Infrastructure High Level Design - NR2 and NR2+	Describes the networking design for CSR, and the extensions for CSR+, including its security features such as Firewalls
RKM	TSC/CRY/007	Requirements for Key Management	Defines the areas in which crypto Key Management is needed
SECURID	RS/DES/004	Use of SecurID Token Authentication for Release 2	Defines the ways in which the SecurID tokens are used to control access to Horizon systems, in conformance with [ACP].
SFS	RS/FSP/001	Security Functional Specification	Defines the security measures agreed with PO Ltd
SPOL	RS/POL/002	Pathway Security Policy	Defines the security policies to be taken into account in the operation of the system. A major purpose of the security architecture is to support these policies, and enable them to be changed in the future as business needs evolve.
VPN	TD/ARC/019	VPN Architecture	Describes the VPN mechanisms, in particular their Key Management facilities and the ways in which VPN is "bootstrapped" into place at existing Outlets

Chapter 17 - Potential for Change

17.1 Scope

This Chapter discusses the features within the Horizon architecture that enable changes to be made to the operational systems and the applications that they support. This quality, *Potential for Change,* is a measure of the ability of the IT system to adapt to changing user or business requirements, or to new technology.

17.2 Business Reasons for Change

A system that is responsive to change is one that can be updated quickly and at low cost. Changes that have not been predicted will not be catered for by the system or its processes, except by chance. The ability to adapt an organisation's processes and IT systems quickly may be critical to its survival.

An early instance of this is the use of sequenced Releases to deliver the full set of functionality in a staged manner. Being able to deliver staged Releases is a fundamental part of any Project that aims to support change. Earlier versions of this Document described the CSR Release. This Version describes the additional features added up to and including BI3.

Both Pathway and PO Ltd see the Horizon infrastructure as an enabler for new forms of business. These new business requirements are captured via the Business Development process described in Chapter 3 "IT Perspectives". Pathway must ensure that it has the processes for managing change, and that the systems development processes have the capability for adapting the IT services to enable changes to be carried out within timescales required by the Business.

This Version of the TED is produced as the end of Pathway's current Contract with PO Ltd comes into sight. Any extension to this Contract must fit within PO Ltd's business objectives and constraints, including a realisation that the delivered solution may be over-engineered in some cases given the changes to the business requirements during the lifetime of the Contract. Pathway has ageed with PO Ltd to seek ways to re-architect the Horizon system so as to reduce both its running costs and the cost of developing new business opportunities. This Chapter discusses some of the options for re-architecting.

17.3 MANAGING CHANGE

17.3.1 Business Related Changes

17.3.1.1 New Business Applications

Both PO Ltd and Pathway are constantly looking for new high-value business applications that can improve the business position of Outlets. Where possible, these will conform to the application models that already exist and that are discussed in Chapter 5.

17.3.1.2 Application Obsolescence

Some applications will become obsolete. They will be removed for business reasons. An example is OBCS application, which is likely to become redundant when all benefit claimants are moved across to payment via ACTs.

17.3.1.3 Revised Back End Architecture

A significant part of the re-architecting mentioned above is the recognition that both Pathway and PO Ltd have developed processes, and supporting IT applications, that carry out largely the same functions.

- Pathway's RDMC system and PO Ltd's RDS could usefully be merged with a consequential saving to both parties
- Pathway's TPS passes information to PO Ltd's OpTIP where it is re-validated, aggregated and passed on to a number of other PO Ltd back-end systems. TPS could carry out the aggregation and distribution itself.

Many of the opportunities of this type were first identified during the ERA work that was carried out in 1999 and 2000. The challenge now is to achieve the goals set by ERA, but recognizing that they will involve significant migration activities.

17.3.1.4 Economic & Monetary Union

Should it happen, the introduction of the Euro in the UK would have a large impact on businesses throughout the UK. There is likely to be a need to handle both existing Sterling and Euros within the same cash drawer; to be able to quote prices in both currencies for goods sold via EPOSS; and to account in both currencies at the end of the day. Pensioners in Orkney are crying out for these changes.

17.3.2 Technical Changes

17.3.2.1 Smart Cards

S30 introduces support for Debit Cards, though at this stage with verification carried out by the Counter Clerk based on the customer's signature. The Clearing Banks have committed, with the retail industry, to introduce cards with an embedded chip, with verification carried out by the customer typing in a PIN value, by the end of 2004. The basis for this technology switch will be the EMV set of standards. The PIN Pad readers introduced to support NBS can handle smart cards *per se,* but a firmware upgrade is required to support the EMV protocols.

17.3.2.2 UNIX Versions

The Host Central Servers and Data Warehouse Servers run under Sequent's Dynix operating system. Sequent is now owned by IBM, and IBM have decommitted to ongoing support for Dynix. Third party products such as Oracle are already not being ported to the latest versions of Dynix.

In the light of this, and of the significant support costs for Sequent/Dynix servers, it is sensible to move these central systems away from Dynix and towards a hardware architecture that supports a more widely available UNIX vesion – Solaris.

17.3.2.3 Windows NT Version

17.3.2.3.1 New Service Packs

Microsoft deliver bug fixes and enhancements to specific Windows NT versions in what are known as "Service Packs". These are issued on a take-it or leave-it basis, and there is no option to apply only the fixes for bugs that have been encountered by Horizon.

There is no standard for the way in which Service Packs operate. It cannot be assumed that a Service Pack will simply replace files and amend values in the Windows NT registry. Microsoft are at liberty to do absolutely anything they see fit including running executables and changing the internal format of files which are critical to the operation of Windows NT. This means that the technique for regression is to some extent dependent on the individual Service Pack.

The Horizon strategy, as with other software changes, is to use the Tivoli Software Distribution facilities described in Chapter 12 "Systems Management". These mechanisms have the benefit of enabling a new Service Pack to be installed with relatively little manpower cost, though potentially (given the nature of the links to the Outlets and the size of Service Packs) at considerable communications link costs and time. Where it is likely that a Service Pack maybe brought into use in the foreseeable future, it is included in the Celestica build.

This technique has been successfully used to upgrade the Counter estate from SP3 to SP6a as part of the migration to BI2. Whether or not it is feasible to introduce a specific Service Pack in this way can only be deduced following extensive investigation and testing. Should it not prove possible to introduce it in an automated manner, then manual upgrade in every Outlet will be required, at considerable extra cost. Given the security measures included in the Counter PCs, the only feasible ways to manage this is by replacing all the existing Counter PCs and taking the old ones back to the factory for refurbishment.

17.3.2.3.2 Windows NT 2000

Version 4.0 is the last version of Windows NT and is still used by a wide range of commercial organisations for both their desktop and server requirements. Pathway is thus squarely in line with industry trends in the operating system strategy that it is using.

However, Microsoft only gains revenues by customers buying new software, not by them continuing to use existing software. Both Windows NT 2000 and Windows XP are now available. Support for Version 4.0 will cease at some point.

Windows NT 2000 introduces a wide range of new features, some of which may make it attractive to Pathway in the longer term. These features include the following.

- Active Directory services, which subsume the Registry and is replicated over a network
- Remote Boot facilities, which could replace the Auto-Configuration process
- Crypto Key Management services (though these are likely to be limited to key lengths permitted by US export legislation)
- Performance improvements, particularly in the handling of *Critical Sections*

Some of these may also be attractive to Escher, who may begin to assume Windows NT 2000 facilities in future versions of Riposte. Any such assumptions would put great pressure on Pathway to move the Counter and Server infrastructure to Windows NT 2000

Some facilities introduced at BI3 only run on Windows 2000. These include the use of the SSH Remote Support software, and the RADIUS servers that manage FRIACO-connected Counters. The introduction of these facilities has led to a useful understanding of the issues involved in Windows 2000, and in particular the development of a Secure Build for this platform. The number of changes, and the likely complexity of the Windows NT 2000 system, make it such that great care will be needed before it can be introduced across the NT estate.

17.3.2.4 Enhancements to Riposte

BI3 is built around Riposte Message Server Version 6.2 (WebRiposte) on both Counter and Correspondence Servers.

Riposte applications include in each message an indication of the Release level of the software.

Escher's latest enhancement to the Counter software is called *WebRiposte Essentials.* Escher expect that this can form a complete replacement for the existing desktop software, and use Asset Manager in a way that simplifies the Counter processing and activities such as the Cash Account. Pathway is working with Escher to validate this approach and to ensure that the WebRiposte Essentials software is fully capable of forming the basis for future enhancements to the Counter software.

17.3.2.5 Counter Hardware

The Counter PC platform is built around a 300 MHz Pentium III processor with 128 Mb of memory and a 13 Gb disk. It is intended that this platform will continue throughout any new Horizon Contract, and any enhancements to the Counter application suite or infrastructure must be able to run within this hardware platform with the minimum possible performance degradation.

17.3.2.6 Central Hardware Capacity

Chapter 15 "Performance" assesses the scaleability potential of each class of server within the Campuses. However, there are other potential changes to the central hardware that are not covered in that Chapter.

17.3.2.6.1 Windows NT Servers

Pathway's strategy towards the purchase of Windows NT servers is to buy the most cost-effective Compaq Intel servers available at the time. Additional disk and memory are purchased in line with the calculations or estimations given in Chapter 15 "Performance".

Scaleability is provided in the first instance by the potential to add more memory, disks, network connections and (in some cases) processor cards to the basic system. Where this proves inadequate, the second option is to replace the entire server by a more powerful one. And if this, too, is inadequate, all Horizon servers and the applications that run on them are designed such that their capacity can be expanded by "sideways expansion" – by adding more identical servers, and sharing the workload between them.

To enable this to be done with the minimum disruption, all Windows NT servers are built from standard scripts using information stored in PVCS. While these scripts may need to change as a result of using new hardware, the major functionality will be unchanged. Thorough rehearsals will ensure that the services running on the hardware can be transferred to the new hardware with the minimum of disruption.

In each case, as described in Chapter 13 "Availability", Windows NT servers are replicated for resilience. The operation of the system as a whole can cope with the outage of any one system. This capability makes it feasible to take any particular server out of service to upgrade it, with only a limited and predictable impact on the overall system SLAs.

17.3.2.7 Oracle

Oracle V8i is now widely available and stable, and Oracle V9 is available. There will be increasing pressure from Oracle consultants involved in Horizon to move to a later version for the Host applications. The DRS application, introduced at BI3, runs on Oracle V8i and has shown that it is possible for applications using different Oracle versions to co-exist on the same platform. At any early point in the future it will be sensible to upgrade the remaining Oracle applications to V8i.

17.3.2.8 Communications Link Capacity

The sizing of the communications links is also covered in Chapter 15 "Performance". Links between the Campuses provide high bandwidth. This can be increased relatively easily, in the first instance by reconfiguring the circuits from 4 Mbps to 34 Mbps, and subsequently by "lighting" additional cores in the 12-way cables coming into each Campus.

The links between Pathway and its suppliers, PO Ltd, and the AP Clients can also be upgraded relatively easily should capacity planning studies show that this is necessary. This will have no impact on the nature of the services run over those links.

The links to the Outlets are more difficult to enhance, because of the inordinate cost of replacing the copper circuits that run from the DLE to each Outlet. However, the range of services, and available bandwidth, that can be carried over these copper circuits has expanded significantly over the past few years.

The principal load on the Outlet network is not the bandwidth but the connection rate. BI3 has introduced FRIACO services at many Outlets. This enables the use of permanent connections for all or part of the day, and hence removes the need for constant call establishment. There is significant scope for expansion in the BI3 network, by increasing the number of Outlets that are permanently connected.

These permanent connections still provide ISDN connectivity, at a standard speed of 64 Kbps. Sizing studies show that this is sufficient for the anticipated daily workload, but this takes no account of new applications that may lead to additional data transmission needs. Should there come a time when a higher bandwidth is required, then we will need to look at the use of new ADSL type services, which privide significantly higher bandwidth over the same copper circuit. Pathway investigated the use of ADSL early in the development of NBS, but at the time the technology was in its infancy and the availability across the UK was distinctly patchy. This situation can be expected to improve in the future.

17.4 CHANGE MANAGEMENT

A number of mechanisms are used to control and manage change. The most important are as follows.

- The use of Reference Data to handle routine changes to application configuration and standing data
- The use of architectural principles which simplify the task of adding a new application on top of the infrastructure of a particular Release
- The use of open networking standards wherever possible
- The use of the Release strategy described in Chapter 11 "Application Development" to group together consistent changes into a system of *Builds* to simplify the development, integration and rollout strategy

17.4.1 Use of Reference Data

Reference Data has a major role within the architecture. It is the enabler for routine changes to the operational applications. It is designed to make it possible to implement many changes to the nature and operation of the Counter applications without the need to make changes to the application code. It enables the development of "soft centred" applications that are largely driven by the values held in their Reference Data. This makes it easy to apply routine changes, including those to the prices of standard items such as stamps or vehicle excise licences.

The types and treatment of Reference Data are discussed in Chapter 7 "Information Management", and its importance to the application architecture are discussed in Chapter 5 "Application Architectures".

Chapter 5 also contains a description of the RDMC. This is the standard mechanism for PO Ltd and its Clients to pass Reference Data to Pathway. It enables this data to be received, verified, transformed and tested, and merged with Reference Data generated within Pathway itself. Finally, it allows a consistent set of Reference Data changes to be brought into use in a controlled way and across the entire Horizon estate.

The attribute grammar used by Riposte makes it relatively easy to migrate applications to a new Release, or to introduce new applications. New classes of message or attribute type can be introduced with no impact on existing applications.

17.4.2 Architecture for New Applications

Where business changes cannot be implemented by Reference Data, it will be necessary to develop a new application or adapt an existing one. The principal purpose of this document (and in particular of Chapter 5 "Application Architecture") is to define the ways in which applications fit into the Horizon architecture. Most of the constraints and guidelines described are specifically there to make it as easy as possible to introduce a new application. When a new application paradigm has to be introduced, such as the use of real-time authorisations in NBS and DCS, it is sensible to exploit the same technology in other new business applications such as electronic mobile phone tip-ups (E-TopUps) or MOT certificate validation.

However, any such architectural re-use needs to be carried out in the light of Chapter 15 “Performance”. This ensures that the impact on the performance or capacity of the existing system and network is fully considered as part of the application introduction process. This impact needs to be assessed in good time for any likely capacity problems to be alleviated by the purchase of new kit or upgrade of existing Platforms.

17.4.3 Open Networking Standards

Using open networking standards such as TCP/IP has the benefit that it enables access to the widest possible set of application and interworking principles. For example, the link between the Counter is TCP/IP over ISDN, and this enables the introduction of “secure tunnelling” through the IP layer to provide an encrypted data stream in line with CESG requirements.

17.4.4 System Release Strategy

Other changes may affect the infrastructure used to support the business applications. Again, this document describes that infrastructure and no such change should be made without the current document first being updated to reflect it.

The architecture described is mostly that of BI3. It is clear that components of the solution will become out of date and need to be replaced during the lifetime of the Pathway contract. New business agreements will require further enhancements to the applications supported and in some cases to the overall architecture.

Horizon has a complex infrastructure and it is not practical to introduce changes on an “ad hoc” basis. The solution is based, where possible, on “commercial off the shelf” (COTS) products. A major impact of basing a complex solution on products of this type is that it is necessary to carry out a detailed and prolonged validation exercise before the solution is brought into general use.

There are inevitably knock-on effects on other components from changing one infrastructure component. A fundamental aspect of the Release strategy is that it must be architecture-led. A new Release must involve a change from one architecturally consistent infrastructure to another, taking into account the needs of the moment and the migration difficulties that will undoubtedly arise.

In addition, any solution or change to the solution, which is to be made available at 38,000 Counters, in 17,500 Outlets, cannot be rolled out overnight. This is particularly the case where there is a need to visit each Outlet as part of the rollout or upgrade process. It is unlikely that any change requiring a manual upgrade at the Outlets will satisfy any Pathway Business case.

It would take six months or more for any such manual upgrade, even working on the basis of a Counter swap-out. Upgrades that can be implemented purely using Software Distribution mechanisms can be introduced faster, but even for these it is necessary to plan for any retraining necessary for Outlet staff, and this may take some months to complete.

The upshot of all of this is that it is probably infeasible to introduce major system upgrades more frequently than once every nine months. Any changes to the underlying infrastructure should be limited to these major Releases. Application changes that can be introduced via Software Distribution may be introduced as minor Releases in between these major Releases. Urgent infrastructure fixes (for example a new Windows NT service pack) need to be assessed on a one-off basis.

17.4.5 Release Migration

There will be a number of issues involved in a migration from one Release to the next. They are outlined here. These were derived initially in [NR2+MIG]. However, the principles developed for the CSR+ migration apply equally to any future Release introductions.

17.4.5.1 Riposte Attribute Grammar

Riposte Counter applications use Attribute Grammar in a way that ensures that they are forwards compatible. New applications can define and use new attribute types, while co-existing older applications (including earlier versions of the same application) will not see these attributes because they will not know that they exist. Where a new version of an application replaces a previous version, it must also support the attribute grammar of the previous version. This includes its Reference Data.

However, if an application were to *change* the type of an attribute at a new Release, a previous version of the application may become seriously confused if it retrieves a message containing the changed attribute. Hence, if it is necessary to change the semantics of an attribute, then a new name must be used. A changed application must be aware of both attribute names, and infer the correct semantics for each.

Once the new Release is live at all Outlets, and all old data has been archived, then the support for old versions of the attribute grammar should be removed at the next Release of the application. This avoids the need to carry forward history for more than one previous Release.

17.4.5.2 Installation of Counter Applications

It must be possible to upgrade the Counter PCs using Tivoli. If a site visit is necessary to upgrade the Outlet systems, this will have major implications for the business case for that application.

This involves four stages.

- Deliver the Reference Data required by the new or changed applications. This should be set to become effective immediately, but will be ignored until the new application version is activated. Existing Reference Data must not be changed.
- Deliver the new applications to the Counters in the selected Outlets
- Install and activate the new versions of the existing applications.
- The activation process should execute a procedure that updates the persistent objects in the Counter to indicate the menu hierarchy for the new or modified application. This ensures that the appropriate Impulses and Buttons can be delivered beforehand, but not brought into play until the application is activated.

- The actual activation of the upgrade is made by Tivoli. However, this does not know (and should not know) the impact of any particular upgrade that it delivers and activates. Each Counter application maintains a Persistent Object that identifies which version of it is active at which Outlet. Any application that needs to know whether a particular application is active in a particular Outlet, or which version of it is active, should do interrogate the relevant Persistent Object.

17.4.5.3 Reference Data

The implication of the foregoing is that Outlets will need to use different Reference Data depending on whether their Counters are at the previous Release or the new one.

(It is considered impractical to have some of the Counters in an Outlet at one Release and some at a later one.)

There are the following implications.

- The Reference Data AIS for the New Release must be used from before Day 1 (to enable testing of the new Reference Data, and to enable the RDMC to be populated with new data prior to its introduction). "Before Day 1" the Campus applications are at the previous Release.
- The new Release's Reference Data must thus be a true superset of that for the previous Release. This will ensure that, when converted to Riposte messages, the attribute *types* remain unchanged as described above. It also enables the existing applications (including Campus applications) to operate normally even if new Reference Data is present.

17.5 FURTHER READING

Ref	Document	Title	Comments
Previous	Chapter 16	Security	Defines the security architecture used
NR2+MIG	TD/DES/021	Strategy for NR2 to NR2+ Migration	Lists the changes to the architecture which will appear at CSR+, and analyses the migration issues involved in these