Document Title: **System Design Specification for Network Banking End-to-End Service**

Document Type: System Design Specification (SDS)

Release BI1-3

Abstract: This Document is the System Design Specification for the End-to-End Network Banking Service (NBS) to be implemented at BI3

Document Status: Approved

Originator & Department: Peter Wiles and Gareth Jenkins (Tel: 7302 6688) - ASD

Contributors:

Simon Fawkes
Phil Hemingway
Richard Hicks
Allan Hodgkinson
Mark Jarosz
Gareth Jenkins
Steve Newman
Peter J Robinson
Glenn Stephens
James Stinchcombe
David Tanner
Geoffrey Vane

Internal Distribution

Liam Foley
Jan Holmes
Richard Laking
Pathway Library

External Distribution None

Approval Authorities

Name	Position	Signature	Date
Tony Drahota	Pathway ASD Manager		

Chapter 0 - Document Control

0.1 Document History

Version	Date	Reason for Issue	Associated CP/ PinICL Nos.
0.1	15/06/2001	First draft	None
0.2	29/06/2001	Second draft	None
0.3	12/07/2001	Third draft	None
0.4	17/07/2001	Fourth draft	None
0.5	07/09/2001	Fifth draft (sent to contributors only)	None
0.6	09/10/2001	Sixth draft	None
0.7	25/10/2001	Seventh draft	None
0.8	06/11/2001	Eighth draft	None
1.0	03/12/2001	For Approval and baselining	None
1.1	15/02/2002	Revised for NB CR026 and CR027	CP3175 CP3176
1.2	15/03/2002	Further revisions following comments and modifications to [SRS]	None
1.3	14/01/2003	Updated following the completion of development ready for final approval.	None
2.0	24/01/2003	For Approval and baselining	None

0.2 Review Details

Review Comments by:	
Review Comments to:	Gareth.Jenkins GRO

Mandatory Review Authority	Name
Customer Requirements	Dave Hollingsworth
Customer Services	Martin Riddell
Quality & Audit	Jan Holmes
PTU	Alan D'Alvarez
Optional Review/Issued for Information	
Programme Director	Peter Jeram
Development	Gill Jackson
ASD	Allan Hodgkinson
	Mark Jarosz
	Gareth Jenkins
	Glenn Stephens
	Geoffrey Vane
APDU	Richard Hicks*
	Dave Johns
	Steve Newman
	Alex Robinson
	Peter J Robinson
IPDU	Ian Morrison
	Simon Fawkes
	James Stinchcombe
	Dave Tanner
Customer Requirements	Tony Hayward
	Ramesh Kallidai*
Business Development	Alan Paterson
Customer Services	Pat Lywood*

Programmes	Bill Reynolds

(*) = Reviewers that returned comments

0.3 ASSOCIATED DOCUMENTS

Ref.	Doc.	Vers.	Title	Source
ACP	RS/POL/003		Access Control Policy	PVCS
ANSI X9.24	ANSI X9.24		Financial Services – Retail Management	ANSI
AUDM	IA/MAN/005		Horizon System Audit Manual	PVCS
BS7799	BS7799			
CA	BP/CON/180-253		PO Ltd/Pathway Codified Agreement	
CAN01		0.1k	New Codified Agreement Schedule N01 – Network Banking Service Definition	
CAN05		0.1o	New Codified Agreement Schedule N05 – NBS Service Management	
CAN08		0.13	New Codified Agreement Schedule N08 – NBS Service Levels and Remedies	
CCDLIST	BP/SPE/026		Contract Controlled and Referenced Document List	PVCS
CHD	BP/DES/003		Counter Hardware Design Specification	PVCS
CNTRDLG	NB/SPE/003		Network Banking Counter Dialogue – Activity & Screen Flows	PVCS
CNTRRD	NB/IFS/003		Network Banking Counter Reference Data Interface	PVCS
CTRBM	CS/PRP/001		Counter Transaction Performance Measurement and Benchmarking	PVCS
DPA			Data Protection Act 1998	HMG
DRSIFS	NB/IFS/011		TPS to DRS AIS	PVCS
DRSRDAIS			RDDS/DRS Interface Specification	PVCS
DRSREP	CS/SPE/011		Network Banking End to End Reconciliation Reporting	PVCS
DRSWS	NB/SPE/002		Network Banking DRS On-line Workstation Specification	PVCS
DSSSEC	RS/CSD/001		Social Security IT Security Standards	PVCS
DWRDAIS	DW/IFS/005		Data Warehouse To Reference Data System Interface	PVCS
DWTPSAIS	DW/IFS/001		Data Warehouse to TPS Interface Specification	
EFTPoS	NB/SRS/002		Network Banking: EFTPoS System Requirements Specification [sic]	PVCS
EFTSDS	EF/SDS/001		System Design Specification for EFTPoS	PVCS
GENAPI	TD/STD/004		Generalised API for OPS/TMS	PVCS
HADDIS	TD/STD/001		Host Applications Database Design and Interface Standards	PVCS
HSHDIFS	CS/IFS/007		ICL Pathway/POCL Interface Agreement for NBCS and HSH Interface	PVCS
ISO 7810	ISO 7810		Identification Cards – Physical Characteristics	
ISO 7811	ISO 7811		Identification Cards – Recording Technique	
ISO 7812	ISO 7812		Identification Cards – Recording Technique	
ISO 7813	ISO 7813		Identification cards – Financial Transaction Cards	
ISO 8732	ISO 8732	1988	Banking -- Key management (wholesale)	
ISO 9001	ISO 9001	2000	Quality management systems - Requirements	
ISO 9003	ISO 9003			
ISO 9564	ISO 9564		Banking – Personal Identification Number management and security	
ISO 9564-1	ISO 9564-1		Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques	
ISO 10646	ISO 10646		Information technology – Universal Multiple-Octet Coded Character Set (UCS)	

ISO 11568	ISO 11568/1-6	1994-1998	Banking - Key management (retail)	
ISO 17799	ISO 17799		Code Of Practice for Information Security Management (formerly BS 7799)	
LINKTS		2.6	LINK Test Strategy	PO Ltd
NBEAIS	NB/IFS/008		Post Office Limited - Network Banking Engine - NBE – Horizon Application Interface Specification	PVCS
NBEIFS	NB/IFS/004		Network Banking Message Flows and Interfaces	PVCS
NBETIS			NBE – Horizon Technical Interface Specification	IBM
NBRDBRV	NB/SPE/009		Network Banking Reference Data Business Rules and Values	PVCS
NBSCSRS			NBS Community Security Policy	
NBSMIS	NB/SDS/008	2.0	Network Banking MIS Reports Design	PVCS
NSBV	PA/PER/031		Horizon New Service Business Volumes	PVCS
OBC	CS/PRD/058		ICL Pathway/ PON Interface Agreement for Operational Business Change	PVCS
OPSARCH	TD/ARC/030		OPS Architecture Specification	PVCS
OPSMENU	SD/SPE/016		Horizon OPS Menu Hierarchy	PVCS
OPSMESS	SD/DOC/009		Horizon OPS messages and Desktop Help	PVCS
PACE			Police & Criminal Evidence Act 1984	HMSO
PDHOST	SD/DES/011		Physical Design for Host Central Server [CSR]	PVCS
PERFSTRAT	PA/PER/015		CSR Performance and Scalability Strategy	PVCS
PMIFS	CS/IFS/008		ICL Pathway / POCL Interface Agreement for the Problem Management Interface	PVCS
PPREQ	NB/REQ/002	1.0	Network Banking Automation – Release 1 – PIN Pad Service Definition and Change to NB Requirements Reflecting the use of PIN verification	PVCS
PPSPEC	NB/SPE/008	0.3	Purchase Specification for Hypercom HFT117 PIN pad used on Network Banking	PVCS
POLISSP	BP/POL/002		Post Office Counter Information Systems Security Policy	PVCS
RAC	CR/SPE/028	0.6	Network Banking – Transaction States & Data Flows	PVCS
RDAIS	BP/IFS/010		Application Interface Specification - Reference Data to Pathway for CSR+	PVCS
RDMCDM	RD/DAT/001		RDMC Data Model	PVCS
RDSAIS	NB/IFS/001		Consignia RDS to Pathway RDMC Interface – Network Banking Logical Data Changes	PVCS
RDTAIS			RDT AIS	
RECIM	NB/PRO/002		Network Banking Reconciliation and Incident Management	PO Ltd
REPREC	SD/DES/005		Horizon OPS Reports and Receipts – Pathway Horizon Office Platform Service	PVCS
RIPA			Regulation of Investigatory Powers Act 2000	HMSO
RIPCONF	AD/DES/029		Riposte Configuration Guide [Withdrawn]	PVCS
RIPENH			Riposte Enhancement Register	
SADD	CR/FSP/004		Service Architecture Design Document	PVCS
SDSAPP	NB/SDS/001	0.8	SDS for Network Banking Application	PVCS
SDSINF	TD/SDS/001		System Design Specification for 2001/02 Horizon Infrastructure Enhancements	PVCS
SDSREC	NB/SDS/004	~~1.0~~	SDS for Network Banking Reconciliation	PVCS
SDSRD	NB/SDS/002	0.5	SDS for Network Banking Reference Data	PVCS
SDSSEC	NB/SDS/005	1.0	Network Banking Security System Design Specification	PVCS
SECCOP	BP/ION/002		A Code of Practice for Post Office Information Systems Security	PO Ltd
SECPOL	RS/POL/002		ICL Pathway Security Policy	PVCS
SFS	RS/FSP/001		Security Functional Specification	PVCS
SOR	NB/REQ/001	1.2	Network Banking Automation – Requirements Catalogue	PO Ltd
SRS	NB/SPE/001	1.3	Network Banking Statement of Requirements	PVCS

SRSVOLS	NB/SRS/001		System Requirements Specification for Business Volumes	PVCS
STYLE	SD/DOC/001		ICL Pathway Horizon Office Platform Service Style Guide	PVCS
TED	TD/ARC/001		Technical Environment Description	PVCS
TEM	PA/TEM/084		System Design Specification template	PVCS
TESTSTRAT	VI/STR/010		Revisions to the testing & Integration Approach for ICL Pathway Release CSR+	PVCS
TIPAIS	TI/IFS/001		Pathway to Post Office Application Interface Specification	PVCS
TPSREC	CS/PRO/111		TPS Reconciliation and Incident Management	PVCS

Where explicit versions are specified, these are the versions that have been consulted in the preparation of the current version of this document.

Chapter 17 lists a number of other existing documents that will require updating as part of the NBS design process. These are, in general, not listed above.

0.4 Abbreviations & Definitions

0.4.1 Abbreviations

[A]	Authorisation request returned from the NBE to the Horizon Counter
[C]	Confirmation message
[C0]	Message sent from the Counter indicating that a previously Authorised transaction did not complete, or that no Authorisation was received within the timeout period
[C2]	Transformation of a [C0] as sent to the NBE
[D]	Message returned by the NBE to Horizon to indicate a discrepancy or error condition
[E]	Message generated by the NBE to an FI to Reverse the effect of a previous [R]
[F]	Financial Advice Note; not used in NBS
[R]	Request message
[S]	Message returned to the DRS to indicate a temporary settlement position. Not used in NBS
ACDB	Auto Configuration Database; Horizon application that configures newly installed Counters
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
ACRR	Agent and Correspondence Server - Resilience & Recovery
AIS	Application Interface Specification; standard document type required for each external interface to the Horizon system
APACS	Automated Payment And Clearing System

API	Application Programming Interface
APS	Automated Payment Service; Horizon service that supports automated bill payments
ATE	Automated Targeting Engine; part of the Systems Management suite that handles the scheduling of software distribution to Outlets
ATM (1)	Asynchronous Transfer Mode; protocol used on 155 Mbps links between Campuses
ATM (2)	Automated Teller Machine
BES	Benefit Encashment Service [obs]
BI1, BI2, BI3	Banking Infrastructure Release n (e.g. BI1, BI3)
BLOB	Binary Large OBject
BO	Business Objects
BT	British Telecom
CAP	Cash Account Period
CAPO	Card Account for Post Office Was know as Post Office Card Account (POCA) and is referred to as such in this document.
CAPU	CA Public Key
CCD	Contract Controlled Document
CCS	Counter Call Scheduler (aka Riposte Call Scheduler)
CD	Compact Disk
CHAP	Challenge Handshake Authentication Protocol
CMS	Capacity Management Service
CNIM	Counter Network Information Monitor; Counter-based ISDN monitoring service introduced at S06 and enhanced at BI3
COM	Microsoft Common Object Module architecture
CS	[Pathway's] Customer Services organisation
CSR+	Core Service Release plus
CSS	Content Services Switch
CUG	Closed User Group
DES	Digital Encryption Service
DLE	Digital Local Exchange
DLL	Dynamic Linked Library
DLT	Digital Linear Tape
DMZ	De-Militarised Zone
DRS	Data Reconciliation Service

DSA	Digital Signature Algorithm
DUKPT	Derived Unique Key Per Transaction; key management scheme described in [ANSI X9.24]
DW	Data Warehouse
DWP	Department of Work and Pensions
E2E	End to End
E3	34 Mbps Asynchronous Transfer Mode (ATM) link
EFTPoS	Electronic Funds Transfer at Point of Sale; new Horizon service likely to be introduced during the same development timescale as NBS
EMV	Europay, Mastercard, Visa
EoD	End of Day
EPOSS	Electronic Point of Sale Service; Horizon service that supports retail functions in Outlets
ERA	Error Reconciliation and Accounting; PO Ltd programme to rework the “back end” processes supporting its business processes. This is now expected to have an impact on the Horizon Counter environment
FAD	Finance Accounts Division; part of PO Ltd
FI	Financial Institution
FRIACO	Fixed Rate Internet Access Call Origination
FSM	Field Service Manager
FTMS	File Transfer Management Service; Horizon process that provides configurable file transfer services between Horizon and PO Ltd’s Clients. Services available include data compression and encryption
FTP	File Transfer Protocol
GGP	Government General Practitioner; previous name for Your Guide, a PO Ltd programme that is likely to require Internet access within Post Office Outlets
HCI	Human-Computer Interface
HMG	Her Majesty’s Government
HORN	Head Of Retail Network
HSHD	Horizon Systems Help Desk
HSM	Hardware Security Module
HSRP	Hot Standby Routing Protocol
HTTP	Hyper Text Transport Protocol
ID	Identity
IDS	Intrusion Detection System
IE	Internet Explorer

IETF	Internet Engineering Task Force
IIN	Issuer Identification Number; represents the first few digits of a magnetic swipe card's PAN. Typically six, but may vary between four and eight.
IP	Internet Protocol
ISA	Integrated Service Adapter
ISDN	Integrated Services Digital Network; telecommunications service providing digital 64 Kbps access via standard telephone lines
ISP	Internet Service Provider
KEK	Key Encryption Key
KMA	Key Management Application
KMS	Key Management Service
L2TP	Level 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LFS	Logistics Feeder Service
LNS	L2TP Network Server
LRC	Longitudinal Redundancy Check
LREC	LINK Reconciliation file
LUC	Look Up Cluster; utility that is called by an Agent and tells it which Correspondence Server to connect according to the Cluster that it is to service.
MAC	Message Authentication Code
MIS	Management Information System; Horizon application set that provides access to and analysis of the information held in the Data Warehouse
MoP	Method of Payment
MSU	Management Support Unit (within Pathway Customer Services)
MSWP	Maximum System Wait Period
MTBF	Mean Time Between Failures
NAS	Network Access Server
NAT	Network Address Translation (carried out in a Firewall)
NB	Network Banking
NBA	Network Banking Application
NBCA	Network Banking Counter Application
NBE	Network Banking Engine; system that handles the interface between the Horizon system and the Financial Institutions (FIs) that have reached agreement to provide automated banking services in Post Office Outlets

NBS	Network Banking Service[1]; the acronym used in this Document for the application that supports banking functionality within the Horizon architecture
NFS	Network File System
OBC	Operational Business Change (procedures for change to PO Ltd Reference Data)
OBCS	Order Book Control Service
OC-3	Optical Carrier-3, where 1 = 51.84Mbps, thus 3 = 155.52Mbps
OCMS	Outlet Change Management Service
OLA	Operational Level Agreement
OMDB	Operational Management Database
OPS	Office Platform Service
OSPF	Open Shortest Path First (Routing protocol)
P&A	Pension and Allowances
PADS	Pre-determined Administrative Data System. Standard time based system used by POCL for Counter transaction activities including the integration of both manual & system time components (commonly embraced by "Benchmarking" activities)
PAN	Primary Account Number
PIN	Personal Identification Number
POCA	Post Office Card Account
	NB. This is now known as Card Account for Post Office (CAPO), however this document has not been updated for the new terminology.
PO Ltd	Post Office Ltd (formerly POCL – Post Office Counters Ltd)
PON	Post Office Network business unit
PPD	Processes and Procedures Description
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunnelling Protocol
PRI	Primary Rate Interface (E1 2 Mbps circuit presenting 30 ISDN lines)
PSTN	Public Switched Telephone Network
PTU	Pathway Testing Unit
PVC	Permanent Virtual Circuit
PVCS	Project Version Control System; software suite used for development and documentation control within Pathway
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service

[1] *cf EPOSS, APS, LFS, OBCS…*

RDDS	Reference Data Distribution System; overall service for handling Reference Data within Horizon
RDMC	Reference Data Management Centre, comprising RDDS and RDMS
RDMS	Reference Data Management Service
RDS	Reference Data System; PO LTD system that provides a Reference Data feed to Horizon and other systems
RDT	Reference Data Team [within Pathway]
RLM	Retail Line Managers
RMS	Riposte Message Service
RNM	Retail Network Managers
RPC	Remote Procedure Call
RTL	Run-Time Library
S10	Release S10 of the Horizon system. It is a Release that precedes the BI2 and BI3 developments described in this SDS.
SAM	Secure Access Module
SDS	System Design Specification (e.g. this document)
SIP	Service Improvement Package
SLA	Service Level Agreement
SMC	System Management Centre
SMDB	Service Management DataBase
SOAP	Simple Object Access Protocol (Version 1.1, World Wide Web Consortium)
SoR	Statement of Requirements; produced by PO LTD
SP	Service Pack
SPAN	Switch Port Analyser
SQL	System Query Language
SRDF	Symmetrix Remote Data Facility
SRS	System Requirements Specification; produced by Pathway in response to an SoR
SYSMAN	Pathway's systems management application, based on Tivoli
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
TIP	(PO LTD's) Transaction Information Processing system
TIS	Technical Interface Specification; standard document required to specify and agree the technical details of each external interface
TMS	Transaction Management System
TPS	Transaction Processing Service; Horizon service that formats data for

	transmission to PO Ltd's Transaction Information Processing (TIP) service
UB	Universal Bank
UK	United Kingdom
URL	Uniform Resource Locator [see RFC 1738]
UTC	Stands for Co-ordinated Universal Time (ISO 8601); equivalent to Greenwich Mean Time (GMT), but a term that doesn't upset some of our continental neighbours
VB	Visual Basic
VPN	Virtual Private Network; security service that provides encryption over the ISDN links between Outlets and Campuses, and over the Outlet LAN
VSAT	Very Small Aperture Terminal; covers satellite communication with Outlets
WAN	Wide Area Network
WRMS	WebRiposte Message Service
XML	eXtended Mark-up Language
YG	Your Guide; Internet Kiosk service currently in pilot in some Outlets, with arms-length links to the Horizon network
ZMK	Zone Master Key

0.4.2 Definitions

The following terms, when Capitalised as here, have specific meanings as indicated.

Abandon

A transaction that is terminated before a Request message is generated at the Counter is Abandoned. Abandon includes:

- Transactions that cannot proceed i.e. require no action from the Clerk
- Transactions that require the Clerk to abandon them by using a function on the screen
- Transactions that the Customer has elected to abandon at the PIN Pad before verification entry

In all cases, no record of the transaction is maintained by the Counter.

Agent

Component of the Horizon Application Architecture that conventionally sits between the Correspondence Servers and Host layers.

Agent Layer

Architectural layer containing the services running on the Agent Servers

Agent Server	Hardware platform that supports Agent processes. It includes the (newly renamed) *Generic Agent Server*, as well as application-specific servers such as the *NBS Agent Servers* that are introduced at BI3.
Approval	The FI verdict contained in an *Authorisation* [A] that permits an NBS transaction to complete according to the Request [R]. The Clerk or Customer may still prevent the transaction from completing e.g. bad signature or change of mind
Asset Manager	Product of Escher Group
Attribute	An item of information associated with a data item (typically used for Reference Data object)
Audit Server	Platform that is responsible for the gathering and archiving audit data, and for retrieving and extracting it for subsequent analysis. Note: This server is used in a subsidiary role for performing various other backup activities
Audit Trail	One or more Audit Tracks, which between them, enable an auditor to follow the treatment of related data transfers, movements or accesses by named individuals
Authorisation Agent	Agent that processes [R] messages from Counters, and passes them to the NBE, then taking [A] messages from the NBE and passing them to the Counter
Auto Configuration Database Service	Service that is invoked by newly installed Counters. It "personalises" them with information set up within the Campus prior to their installation
Bronze Service Outlet	An Outlet that continues the current network strategy, of making an ISDN call to the Outlet in response to any real-time transaction
Bubble Help	Help text displayed as a cartoon style 'bubble' linked to the text being explained
Bulk Agent	Agent that reads and/or loads a potentially large amount of information to or from Riposte (or, from BI3, the DRE) in bulk Now no longer just to / from Riposte (NBE to DRS agents could be described as Bulk).
Business Rules	Rules governing the conduct of a Transaction which are contained within Reference Data or processes
Button	Icon on the Riposte Desktop that can be "pressed" by the user to invoke a particular action
Campus	One of two data centres installed by Pathway in Bootle and Wigan. Each can handle the entire Horizon workload
Cash Account	The method by which the Transactions performed and the cash and Stock on hand at the end of a PO LTD Outlet Accounting Period are declared to PO LTD main accounting offices

Cash Account Period — Period (one or more weeks) over which a Cash Account is calculated

Client — The Client Financial Institution on behalf of which PO LTD provides a service to Customers at Outlets

Cluster — Group of Correspondence Servers, all handling the same set of Outlets and replicating data between each other for resilience purposes

Collection — [Reference Data] A specific type of Reference Data identifiable in a Riposte Message Store. Analogous with an Entity or Table.

Confirmation Agent — NBS Confirmation Harvester Agent takes [C] messages from Counters and feeds them to the Data Reconciliation Service (DRS). NBS Confirmation Loader Agent takes the stored [C]s from the DRS and feeds them to the NBE.

Connection Handler — On the NBE, a particular IP address and port number that can be connected to by a particular Agent. It represents the interface to a particular Process Interface on the NBE

Contra Entry — A Transaction that negates a preceding Transaction to which it refers

Contract Controlled Document — A document which: (a) is listed as a CCD in [CCDLIST] and (b) may only be amended through the Change Control Procedure

Correspondence Server — Hardware platform that supports the Campus-based Riposte Message Service, and handles message replication to and from a group of Outlets

Counter — Counter PC installed in a Post Office Outlet

Counter Application — An application resident within the Counter that contains the business logic controlling the dialogue with the Clerk, or other business specific functions on the Counter (such as End of Day processing)

Counter Call Scheduler — Process running within the Gateway PC that schedules the opening of the ISDN link to the Campus, depending on the number of waiting messages and the time since the last call. It is influenced by Priority Messages that causes an immediate call to the Campus

Counter Clerk — Person working in an Outlet and operating a Counter

Customer — A member of the public transacting, or seeking to transact, business with PO LTD through any of the Services

Customer Session — A set of contiguous Transactions recording business transacted by a single Customer. These are all committed at the same time when the Customer and Clerk have exchanged goods and monies

Data Reconciliation Service — Service provided by Pathway to PO LTD which matches transaction flows from Counter and NBE, and reports on these to PO Ltd

Data Warehouse
Computer system holding information about past Transactions executed at Outlets, and used to calculate Service Level Agreement (SLA) adherence

Day 'B'
First working day after the date on which a transaction took place at a Counter

Day 'D'
Third working day after the date on which a transaction took place at a Counter

Decline
A transaction is declined when it does not proceed as per the initial customer request. Decline includes:

- Transactions that cannot proceed because a decline response has been received at the counter from the NBE/FI.
- Transactions that are terminated by the Clerk because of e.g. signature comparison failure or card check failure
- Decline by Customer, e.g. does not sign the office receipt
- Decline by Counter due to timeout, i.e. no response received to the request

In all cases, a record of the transaction is maintained by the Counter.

Digital Signature
Process of 'signing' Reference Data which has been sourced outside of Pathway with a digital key, before it is delivered onto the Counter, so that its authenticity may be verified before use

EPOSS Settlement
Settlement of a Customer Session at the Counter

Extended Verification Process
Authentication of the Customer through a defined process consisting of a number of questions, the answers to which establish the identity of the Customer

Fallback
Where a system has attempted to go On-line but failed and has the ability to proceed with the transaction in an Off-line manner – typically with limits on the transaction value

Financial Advice Note
Financial Advice Note [F] is a movement that exists within the enhanced RAC model where a transaction may be locally authorised as a result of Fallback or Off-line work.

Framework
Financial Transaction Framework; an adjunct to WebRiposte that provides a constrained environment for Counter Applications written to work with WebRiposte. It is not used in NBS Release 1

Gateway PC
Counter that has an attached ISDN line or other communications channel that enables it to pass data to and from the Campus

Generic Agent Server
Hardware platform that support the Agent processes for most applications (i.e. all those for which there are no application-specific requirements such as onboard crypto support). See also Agent Server and NBS Agent Server.

Horizon
Name that encompasses the totality of the systems provided by Pathway to support the automation requirements of Post Office Outlets

Horizon System Helpdesk	A single point of contact providing fault management for the Horizon applications (including NBS). It also provides overall operational service management, information and administration.
Host Central Server	Hardware platform (Sequent NUMA-Q server running under Dynix) that supports the principal Campus based applications
Host Layer	Architectural layer containing the services running on the Host Central Servers
Interactive Agent	Agent that handles on-line messages from Counters as they arrive at the Campus. An example is the NBS Confirmation Harvester Agent that takes [C] messages from Counters and feeds them to the Data Reconciliation Service (DRS).
Key Management	Covers the tasks involved in the generation, distribution and revocation of keys used for encryption and signing. There are both symmetric and asymmetric keys, the latter has both public and private key part
KMA Server	Hardware platform that supports the KMS
LINK	LINK is a branded and shared network of cash machines and self-service terminals of certain member Financial Institutions in the UK, enabling services from one FI to be provided at cash machines of all other member FIs
LUHN	An established check digit formula which is part of the Automated Payment And Clearing System (APACS) standard
Maestro	A proprietary scheduling system, produced by IBM (previously Unison Software). Used to schedule the Pathway Campuses. Now renamed Tivoli Workload Scheduler (or TWS); batch job scheduling and monitoring subsystem used to provide automated scheduling facilities within the Horizon system
Method of Payment (MoP)	The form of payment recorded against a Transaction involving a Customer
NBS Agent Server	Hardware platform on which the NBS Agents run. It includes a Hardware Security Module (HSM) that is used to handle Personal Identification Number (PIN) translation actions and other crypto functions such as generating and validating MACs and encrypting sensitive data
Network Banking Engine	A central system being supplied by a third party in support of NBS
Object	[Reference Data] A specific instance of one type of Reference Data. Analogous with a key or row
Off-line	Where a system elects not to communicate with another system – typically the Counter having the rules held locally to enable it to complete the transaction. Not supported in NBS
Off-line Indicator	A visible indicator that displays an Icon on the Counter screen when the On-line service is not available at that Counter. It obtains its information from the On-line service Persistent Object

On-line	Where a system attempts to communicate with another system – typically the Counter seeking immediate authorisation from a FI
Outlet	Post Office location with one or more Counter PCs installed as part of the Horizon programme
Outlet Centric Failure	Failure that affects an individual Outlet, i.e. failure at an Outlet or in the Outlet-to-Campus network. This type of failure is the only one for which the Postmaster should raise a Help Desk call
Pathway	Short name for Fujitsu Services (Pathway) Limited; rebranding takes effect on 1 April 2002 and is anticipated here
Persistent Object	Item of Reference Data that is used for long-term configuration or parameterisation of Counter applications. (Most message store messages "expire" after a certain period of time and are removed.)
PIN Block	Block of data containing an encrypted PIN value
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. The model used is the Hypercom HFT117; see [PPSPEC]
Platform	An instance of a hardware unit (server, workstation, Router etc) that is installed by and configured by Pathway to meet the Horizon security, application and capacity requirements
Priority Message	A Riposte message with a parameter that causes an immediate ISDN call to or from the Outlet, if the line is not currently open
Process Interface	NBE partition that handles the messages transmitted by a limited set of Agent instances
Product	Any products to be supplied under [CA].
RAC Model	Basic model for banking transactions where initial On-line Request [R] from Counter elicits On-line Authorisation [A] from FI. Confirmation [C] of outcome of transaction is sent in near time from Counter to NBE, unless it differs from the [R] in which case a [C0] is sent to the NBE in real-time (see NB CR0027 and [RAC]).
Receipt	A printed record of the Transaction at the Outlet
Reconciliation	Ensuring the financial integrity of transactions across service boundaries
Reconciliation Date	The date attributed to a transaction to allow PO Ltd to reconcile. It will be set to the first available Settlement Date from the transaction elements ([C112], [C12], [C4], [D]) that make up that transaction. If no Settlement Date is available, the Reconciliation Date will be set to the processing date that the DRS first recorded any element of the transaction. If a Settlement Date subsequently becomes available, the first available Settlement Date will replace the processing date. However, once a transaction has been accounted for on a reconciliation report, the Reconciliation Date will never change.

Reference Data — This is used in three different ways:

- The end to end service for the receipt, manipulation and delivery of configuration data and parameters for use by the rest of the system, within the Horizon Programme
- Read Only Data defined in the Riposte Message Store providing sets of Collections and Objects used to configure the Outlet and define the business parameters to be used and followed in providing a Counter service
- The entirety of read only objects within the system, whether in the Riposte Message Store or not, that configure the system in some way or provide soft parameters to system definition and use

Release — A documented and co-ordinated collection of software and/or data provided by Pathway to deliver PO Ltd Services, or to extend the infrastructure used to deliver these services

Request — Request message [R] sent On-line from Counter to FI initiating an NBS dialogue

Reversal — A Transaction that nullifies a specific previous Transaction that has been completed (committed) in a previous Customer Session, subject to Business Rules (e.g. time limits, previous receipt). See also Abandon, Void

Riposte — Proprietary product from Escher group that is used to (a) support the Counter PC user's desktop, and (b) to provide a speedy and reliable message replication process between the Counters in an Outlet and the Correspondence Servers at the Campuses

Serve Customer Mode — Desktop environment for conducting a Customer Transaction

Service Boundary — Intersection between operational domains

Service Level Agreement — Agreement to provide a quantified and measurable standard, required for a specified PO Ltd Service

Settlement — This is used in two different ways:

- Settling a Customer Session where the balance of the session is reduced to zero and the appropriate cash (and other items such as cheques, tokens, stamps etc) is exchanged between the Customer and the Clerk
- Settlement between PO Ltd and an FI (either direct or, initially, via LINK) where an agreement is made as to the aggregate value of transactions for a given period (probably a day)

Settlement Date

The date on which the Client settled the transaction (in some instances a default is set by the NBE). The Settlement Date will be allocated by the Client (or failing that the NBE) and included in both authorisations and confirmations. The [C4] will also contain a Settlement Date.

Silver Service Outlet

An Outlet that is provided with a permanent network connection to the Campus, thus avoiding the need to establish an ISDN call in response to an NBS transaction

Stock Unit

An individual unit of accountability, mandatory within a main (branch) post office and optional within a sub post office, for which an individual (or a group of individuals) is accountable. It may contain: (i) Transaction Vouchers for a designated period, (ii) Value Stock, and/or (iii) cash

Temporal

Of Reference Data, defines an item that has an associated start date and time, and optionally an expiry date & time

Token

A magnetic stripe card, smart card, smart key, or other physical device, bearing information about a customer. This is restricted to magnetic stripe cards only for NBS for the initial Release (BI3).

Track 1

First track of data held on the magnetic stripe on a magnetic swipe card

Track 2

Second track of data held on the magnetic stripe on a magnetic swipe card

Training Mode

A service that allows a Clerk to be trained on a Counter without affecting the accounting of the overall Outlet. Any such transactions are not recorded and no money or goods are expected to change hands. Some transactions are specifically excluded for security reasons (e.g. Automated Payment Service (APS) Smart card Transactions)

Transaction

A recorded and auditable instance of business activity, involving service provision or Stock movement across organisational or service boundaries

Transaction Element

Part of a transaction i.e. [C112], [C12], [C2], [C4] or [D]

Transaction Type

The Txn_Type as defined in [RAC]

Universal Bank

A client FI that supports Post Office Card Accounts

Void

Cancellation of a Counter Transaction before it is committed (but after Request has been sent). An NBS transaction will have its Confirmation status set to a Decline after the Request has been issued and before the transaction is committed at the end of the Customer Session. See Abandon

VPN Server

Hardware platforms that support the VPN service used to secure communications between the Campuses and Outlets

Working Document	Any document designated as a Working Document and any document other than [CA], Change Control Notes executed by both parties, Contract Controlled Documents and Contract Referenced Documents. Working Documents are without prejudice to any of the parties and nothing contained therein shall be deemed or construed as affecting existing contractual obligations or creating new contractual obligations between any of the parties. This is a Working Document

0.5 CHANGES IN THIS VERSION

0.5.1 Changes in Version 2.0

Minor corrections from Review cycle – mainly to Chapter 9.

Changes from version 1.3 use a red font, like this (~~with deletions in red strikeout like this~~).

0.5.2 Changes in Version 1.3

The purpose of this version is to enable a final review before a baselined version is produced. Changes have been kept to a minimum, but an effort has been made to ensure that the document does reflect what was actually implemented.

Changes from version 1.2 use a red font, like this (~~with deletions in red strikeout like this~~).

0.5.3 Changes in Version 1.2

"ICL Pathway" replaced by "Pathway" (short for "Fujitsu Services (Pathway) Limited") as part of the rebranding exercise that comes into effect on 1st April, 2002.

Changes have been made to bring this Version of the SDS in line with [SRS], prior to the formal baselining of that document. Other changes reflect the Counter dialogues documented in the CCD [CNTRDLG], and in recent versions of the underlying SDSs. These changes (and others made in response to comments received on Version 1.1) use a red font, like this.

0.5.4 Changes in Version 1.1

This Version responds to NB CR026 and CR027

- CR026 replaces the MQSeries interface to the NBE with an interface based upon TCP/IP connections direct to a set of NBE partitions.
- CR027 removes the [C2] flow to the NBE, apart from zero-value [C2]s. These are "expedited". In addition, the [S] and [EoD] flows from the NBE to the DRS are removed, and the residual [C4] and [D] flows are carried in batch files rather than via MQSeries.

In addition, it has been agreed with PO Ltd that the NBS Counter application will not make use of Escher's Financial Transaction Framework. Chapter 5 has been modified accordingly. There are number of further changes arising from this, such as removal of the need to handle Type X Reference Data. These changes are covered in this Version.

Recent discussions and agreements on the NBE-to-Horizon AIS are also reflected in Chapter 7.

0.5.5 Changes in Version 1.0

The network type for Bronze Service Outlets will now be metered dial-in, rather than FRIACO dial-in.

Other minor changes in response to comments on V0.8

Addition of "Changes Expected" indicating that it is expected that the Financial Transaction Framework will not be used at BI3

0.5.6 Changes in Version 0.8

0.5.6.1 General

Chapter 14 (Application Development) has been moved to Part E.

Minor changes in response to comments received.

The term POL has universally been changed to PO Ltd

0.5.7 Changes in Version 0.7

0.5.1.1 General

Chapter 5 (Functional Decomposition) has been renamed "Conformance to Requirements" and moved to the end of the document.

Chapter 19 (Potential for Change) has been removed.

Changes have been made to keep this Document in line with the latest versions of [SDSSEC], [SDSRD] and [SDSREC] as recorded in Section 0.2.

0.6 CHANGES EXPECTED

None.

0.7 CONTENTS

0.7.1 Table of Contents

0.7.2 Table of Figures

0.7.3 Table of Tables

Chapter 1 - Introduction

1.1 PURPOSE

This Document forms the top level *System Design Specification* (SDS) for the proposed Horizon *Network Banking Service* (NBS) developments. It outlines the developments to be undertaken, and the enhancements to the Horizon infrastructure, required to support NBS. It is a Working Document, as defined in [CA], and defines the starting point for the High Level Design of the NBS service and associated infrastructure upgrades. It will not be maintained once it is baselined against the [SRS] and design begins, other than for major changes of requirement agreed between Pathway and PO Ltd. However, it will be updated once the implementation of NBS is complete, to reflect any changes made during the design process.

It should be noted that if this document conflicts with statements in HLDs or CCDs, then those other documents should be considered to be definitive rather than this SDS.

It does not discuss the developments to be undertaken by other parties, or the operation of the service once it is in place.

The full set of PO Ltd requirements for NBS are given in [SOR]. Pathway's response to these, indicating which of the requirements will be met, is given in [SRS]. This Document reflects the Version of [SRS] listed in Section 0.3.

NBS provides an End-to-End On-line service that supports card-based banking transactions. It must have qualities of data integrity, support reconciliation and settlement, and provide interworking between different domains of responsibility. The Counter-based components of the service must be provided through the Horizon Counter infrastructure but use the new WebRiposte technology where appropriate.

NBS will be provided by a number of enhancements to the Horizon system, and by components provided by or operated by a number of suppliers as well as Pathway. The aspects that affect Pathway involve the application itself, which introduces a number of new architectural principles, and the Horizon infrastructure including the applications developed and used by Pathway to manage the Horizon system, and new methods of connection to systems running on external sites.

This document provides an overview for all of these developments. It introduces and defines the scope for a number of lower level SDSs that cover particular aspects of the service and its infrastructure.

1.2 SCOPE

This Document describes the developments that are needed to meet the NBS requirements. In general, it does not discuss (except in passing) the processes or procedures that will be necessary to operate the NBS service, or the impact on existing processes caused by the introduction of NBS, or the monitoring of SLAs that do not require the automated collection of new classes of data within the Horizon system. [SRS] identifies many such new or enhanced processes.

A series of lower level documents are being produced to describe the developments necessary in various areas of the Horizon system. These are as follows.

- Application architecture and Interfaces ([SDSAPP], largely summarised in Chapter 5)
- *Data Reconciliation Service* (DRS) ([SDSREC], see Chapter 9)
- Reference Data ([SDSRD], see Chapter 8)

Note that [SDSRD] is significantly out of date and so has been withdrawn.

- Infrastructure, including network and platform changes and systems management, and describing the performance, scalability, resilience and availability features of the development [SDSINF]
- Security ([SDSSEC], see Chapter 13)

The current document provides a full end-to-end description of NBS, and summarises the enhancements described in each of these lower level SDSs. It thus serves as an introduction to the developments found necessary by Pathway to provide NBS.

1.3 Relationship to Other Documents

The design for NBS will generate a structure of documents, as shown in the figure below.

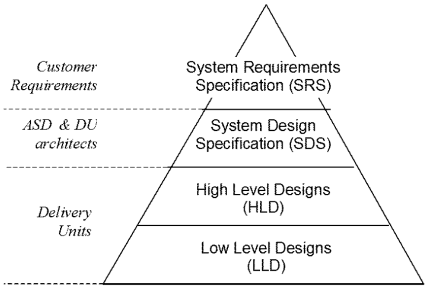


Figure 1 – Structure of Design Documentation

This document is thus linked to others as follows.

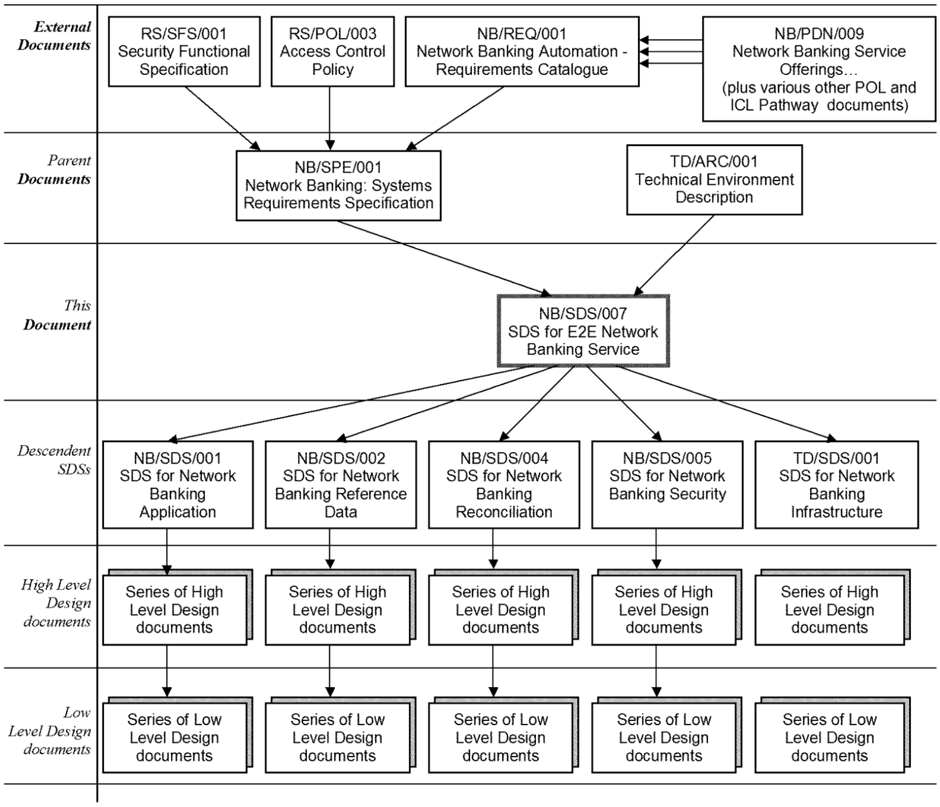

External Documents
RS/SFS/001 Security Functional Specification
RS/POL/003 Access Control Policy
NB/REQ/001 Network Banking Automation - Requirements Catalogue
NB/PDN/009 Network Banking Service Offerings… (plus various other POL and ICL Pathway documents)
Parent Documents
NB/SPE/001 Network Banking: Systems Requirements Specification
TD/ARC/001 Technical Environment Description
This Document
NB/SDS/007 SDS for E2E Network Banking Service
Descendent SDSs
NB/SDS/001 SDS for Network Banking Application
NB/SDS/002 SDS for Network Banking Reference Data
NB/SDS/004 SDS for Network Banking Reconciliation
NB/SDS/005 SDS for Network Banking Security
TD/SDS/001 SDS for Network Banking Infrastructure
High Level Design documents
Series of High Level Design documents
Low Level Design documents
Series of Low Level Design documents

Figure 2 – Relationship to Other Documents

1.4 STRUCTURE

This Document is split into six logical parts, each comprising a number of Chapters.

1.4.1 Part A– Introduction

- Chapter 1 – Introduction
- Chapter 2 – Summary of Requirements, including the [SRS], existing *Service Level Agreements* (SLAs) that will continue to impact on the Horizon service, and requirements originating within Pathway that have a bearing on the overall solution
- Chapter 3 – System Functionality: a description of the service to be provided, including the RAC model, transaction types supported and features of the Reconciliation service
- Chapter 4 – Design and Development Principles and Assumptions, including the use of mandated products and other major extensions to the existing Horizon architecture, and broad timing constraints on the implementation of the service

1.4.2 Part B – Application

- Chapter 5 – Application Architecture, covering extensions of the current Horizon architecture to handle the use of WebRiposte, and all major system components affected by or introduced by the development of NBS
- Chapter 6 – User Interface, summarising the way in which the NBS application is delivered to the Counter Clerk
- Chapter 7 – Information Management, including data flows and the use of database products
- Chapter 8 – Reference Data enhancements
- Chapter 9 – Data Reconciliation services

1.4.3 Part C – Infrastructure

- Chapter 10 – Network Infrastructure, focusing on the need to radically enhance the ISDN service that currently connects Outlets to the Campuses
- Chapter 11 – Platforms Infrastructure, including new hardware platforms necessitated by the introduction of NBS, and changes to existing platforms including upgrades to commodity software products
- Chapter 12 – Systems Management Infrastructure, including enhancements to the major third party enablers (Tivoli, BMC Patrol, Maestro) and to the infrastructure products developed by Pathway including *Auto-Configuration Database* (ACDB) and *Outlet Change Management Service* (OCMS).
- Chapter 13 – Security Infrastructure, covering the particular security issues involved with access to banking services and the implications of interacting security domains within the end-to-end solution, and the developments proposed to meet the security requirements

1.4.4 Part D – Strategies

- Chapter 14 – Resilience & Availability Strategy, describing the approach taken by Pathway to meet the resilience requirements for NBS
- Chapter 15 – Performance & Scalability Strategy, including an analysis of the volumetric information supplied by Consignia and its implication for the sizing and scalability of the Horizon system

1.4.5 Part E – Service Introduction & Service Management

- Chapter 16 – Application Development, indicating all the system components introduced or modified by the development of NBS
- Chapter 17 – Documentation, listing the set of documents that will need to be produced or enhanced to develop and support NBS
- Chapter 18 – Acceptance & Integration Testing, covering the approach taken and particular areas where specialised testing is required
- Chapter 19 – Service Introduction, covering the Release strategy, migration issues and other service introduction areas such as training and Help Desk reskilling

- Chapter 20 – Service Operation & Management, covering the operation of the enhanced Horizon service including service level measurement and management

1.1.6 Part F – Conformance to Requirements

- Chapter 21 – Conformance to Requirements, including a list of all the Requirements listed in [SOR] as qualified by [SRS], with an indication of the point within this SDS at which compliance is indicated. (The text at these points is cross-referred back to Chapter 21 with an indication, in blue text, such as [NBR001]).

Chapter 2 - Summary of Requirements

2.1 General

This Chapter identifies the sources of the requirements that influence the NBS outline design described in this Document.

2.2 Explicit Business Requirements

[SOR] is the PO Ltd Requirements Catalogue for NBS. It includes requirements relating to all the suppliers of components of the end-to-end NBS solution, and is not specific to Pathway. The requirements listed there define the business parameters of a service that provides the ability for Customers in Post Office Outlets to carry out a defined set of supported banking transactions. These services are provided for Customers of FIs with which PO Ltd has reached a service agreement.

In addition, the service provides some mechanisms to administer some aspects of the introduction of *Post Office Card Accounts* (POCAs) for people who do not currently have a bank account, or do not choose to use an existing bank account to receive monies that are currently paid by Benefit Order Book.

Major requirements in [SOR] that have a significant impact on the design of NBS include the following.

- The Counter application will be implemented using Escher's WebRiposte product
- The application will use an RAC model in which Request [R]s are passed back to the Customer's *Financial Institution* (FI) in real time, and the Authorisation [A] messages are returned in real time. Confirmation [C] messages are returned in "near real time" if the outcome differs from the amount Authorised
- Verification of the transaction should be supported by PIN Pad as well as by signature
- The interface to the FIs is provided by a *Network Banking Engine* (NBE), which provides the sole FI interface to the Horizon domain, and hence avoids the need for the Horizon system to understand the different interfaces to the supported FIs
- *Service Level Agreements* (SLAs) will be implemented at appropriate and measurable points on the service boundaries between Pathway and the NBE, subject to the workload remaining within the parameters defined in [SRSVOLS]
- A *Data Reconciliation Service* (DRS) will be provided by the Horizon system, taking information from the Pathway and NBE domains and presenting settlement and reconciliation information to PO Ltd.

[SRS] is Pathway's response to the requirements that, in whole or in part, are relevant to Pathway. It identifies the proposed conformance to the requirements in [SOR]. It is being prepared in parallel with the preparation of this document, and will be baselined before this document is completed. The Version identified in Section 0.3 provides the context for the developments identified by the present document.

[SRS] is more than just a requirements catalogue. It contains many details of the service to be provided. Some of these are more suited to this SDS, and are repeated here, either as a requirements item or as part of the description of each subject area. Note that Chapter 21 of the present document provides a complete list of the Requirements in [SOR], and cross-refers each to the SDS Section where compliance with that requirement is identified (or otherwise) in accordance with [SRS].

2.3 CONTRACTUAL REQUIREMENTS

Although there is at this point no contractual obligation covering the development of and facilities of NBS, contractual discussions are continuing in parallel both with the development of this Document and of the facilities described therein. It is expected that the contractual service definition for NBS ([CAN01]) will replace [SRS] as the definitive specification of the requirements that must be met by NBS. In support of that objective, [SRS] will be brought into line with the then current status of the contractual negotiations, and moved to a status of "Version Complete" at V2.0. Any subsequent changes will be handled by Pathway Change Proposals (CPs).

2.4 VOLUMETRICS

[SRSVOLS] defines the message volumes that the NBS is expected to support over the first few years of its introduction. It includes the volumes expected to arise from the introduction of *Electronic Funds Transfer at Point of Service* (EFTPoS), as well as NBS, as it is expected that the Horizon infrastructure will be enhanced in one stage to support both of these applications. [NBR057]

2.5 INFRASTRUCTURE REQUIREMENTS

[SOR] accepts, and [SRS] confirms, that the infrastructure developed to support current Horizon business applications will be inadequate to support the additional load generated by NBS and EFTPoS. A number of additional requirements arise from this. They are summarised here and expanded in the body of the Document.

2.5.1 Network Capacity

The business requirements for NBS will force a major redevelopment of the Horizon Outlet network. The current network is designed to support a largely batch ISDN load, directed by the Counter Call Scheduler. Within this, some 2% of messages require a real-time response, and these are handled by Riposte Priority messages. However, the take-on of NBS will rapidly move to a situation in which, at peak times, most calls to the Campus would be initiated by NBS transactions that require a real-time response. This would have a significant impact on the peak workload (number of messages per second) that the network will have to handle, the peak connection rate, and on the resilience needed (i.e. chance of a call succeeding). The existing ISDN voice network will not be able to cope with the peak load and an alternative technology is required.

Any such change to the network topology needs to be done in such a way that it has:

- Minimal disruption on existing network usage
- Minimal impact on Outlet operation (ideally without requiring a Counter reboot, as such upgrades are more complex than those that do not require a reboot)
- A "bypass" regression capability at the Outlet (e.g. the ability to use an alternative, possibly more costly, network) in case of unacceptable congestion on the modified network
- Minimal impact on the space required for equipment in the Campuses

The proposed Network enhancements are discussed in Chapter 10.

2.1.2 Infrastructure Software Versions

The use of WebRiposte at the Counters will require that the Counter estate (38,000 Counters in 18,000 Outlets) is upgraded from Internet Explorer V4.1 to V5.01 or later[2]. This is a dependency of WebRiposte itself.

The availability and performance requirements for NBS will increase the demand for a stable and reliable Counter platform. At present, the Counter systems run on Windows NT 4.0 with Service Pack 3. This contains a number of memory leakage problems that are fixed in later *Service Packs* (SPs). To enable WebRiposte based applications to co-exist on the existing Counter hardware, it is necessary to upgrade the Counter estate to a later Service Pack (SP6a).

Because of the upgrade to SP6a, a number of other third party products used on the Counters or within the Campus systems will also need to be upgraded. Others will need to be upgraded because the versions used are no longer supported, and Pathway is unable to meet the Service Level requirements of NBS with unsupported versions of these products. The full implications of this requirement are discussed in Chapter 11.

[2] *In fact the target version is IE 5.5 SP1*

Chapter 3 - System Functionality

3.1 GENERAL

This Chapter contains a description of the NBS service to be provided by Pathway, and its relationship with bodies outside Horizon.

PO Ltd's objective for the Network Banking Automation Project is to deliver a Network Banking Service, via the existing Horizon Network, that is operational and able to support the introduction of Universal Banking, by April 2003. The qualities required of the NBS include:

- Establishing an infrastructure to enable additional financial transactions to be implemented through agreed *Operational Business Change* (OBC) procedures
- The NBS is to appear as another Service on the Horizon desktop, alongside and integrated with existing Services such as APS
- The NBS is to be "data driven" in that it will use PO Ltd Reference Data to define many aspects of the service provided
- Service management and support appropriate to an On-line service

3.2 NBS COMPONENTS AND CONTEXT

The NBS system enables Counter Clerks in Outlets to carry out On-line banking transactions on behalf of Customers, using the Customer's magnetic swipe bankcard[3], 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. [NBR001, NBR002, NBR003, NBR004]

The End-to-End systems supporting the operational NBS are shown below.[4]

[3] *Smart cards are not supported.*

[4] *Source: [SRS]*

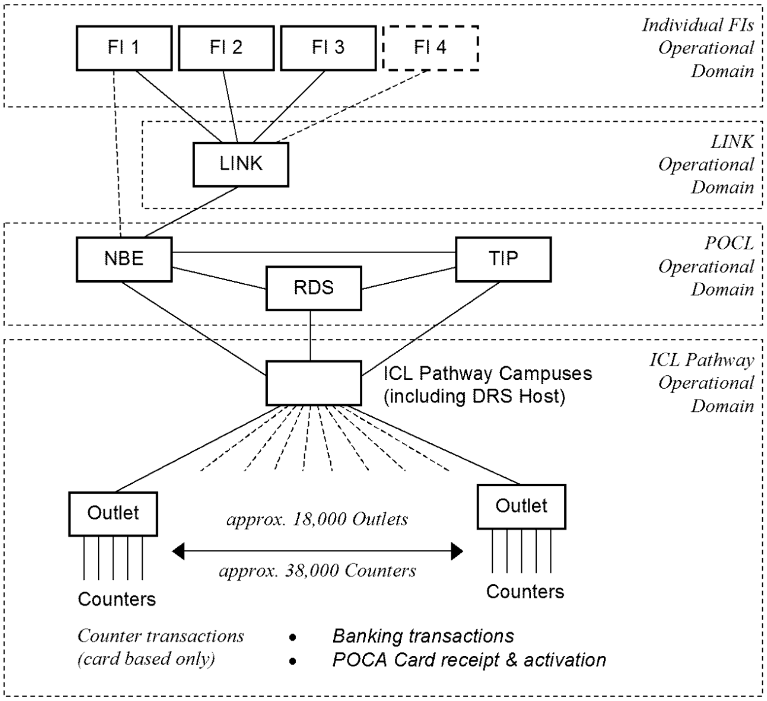

FI 1
FI 2
FI 3
FI 4
Individual FIs Operational Domain
LINK
LINK Operational Domain
NBE
RDS
TIP
POCL Operational Domain
ICL Pathway Campuses (including DRS Host)
ICL Pathway Operational Domain
Outlet
Outlet
approx. 18,000 Outlets
approx. 38,000 Counters
Counters
Counters
Counter transactions (card based only)
• Banking transactions
• POCA Card receipt & activation

Figure 3 – Operational Domains and their Relationships[5]

The principal purpose of the NBE is to convert 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[6]. It interfaces in a generic manner with the Horizon Campus systems. There will be a hot-standby system in case the operational system fails, and a disaster recovery system available at a separate site. The systems and infrastructure in the PO Ltd operational domain will be configured to support at least[7] the same peak load as those in the Pathway operational domain.

NBS will support a set of defined 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. [NBR023]

- New cards (i.e. new *Issuer Identification Number* (IIN) ranges) may be introduced via PO Ltd Reference Data from time to time according to OBC procedures. [NBR416]
- New FIs may be added or removed from time to time, according to OBC procedures, by being treated as extensions to the range of IINs supported at the Counter

3.3 NBS Data Flow Model

The full implementation of NBS depends on a number of data flows between various components of the end-to-end system shown above. The following diagram[8] shows the

[5] *Source: [SRS]*

[6] *Initially, only via LINK*

[7] *PO Ltd originally expected the NBE to support other channels than just Horizon*

[8] *Source: [RAC]*

major data flows[9], and the relationship of NBS to four external entities: the FIs, the NBE, the Post Office and the retail Customer. A subsequent Section illustrates how each of the NBS transactions is invoked by the Counter Clerk in an Outlet.

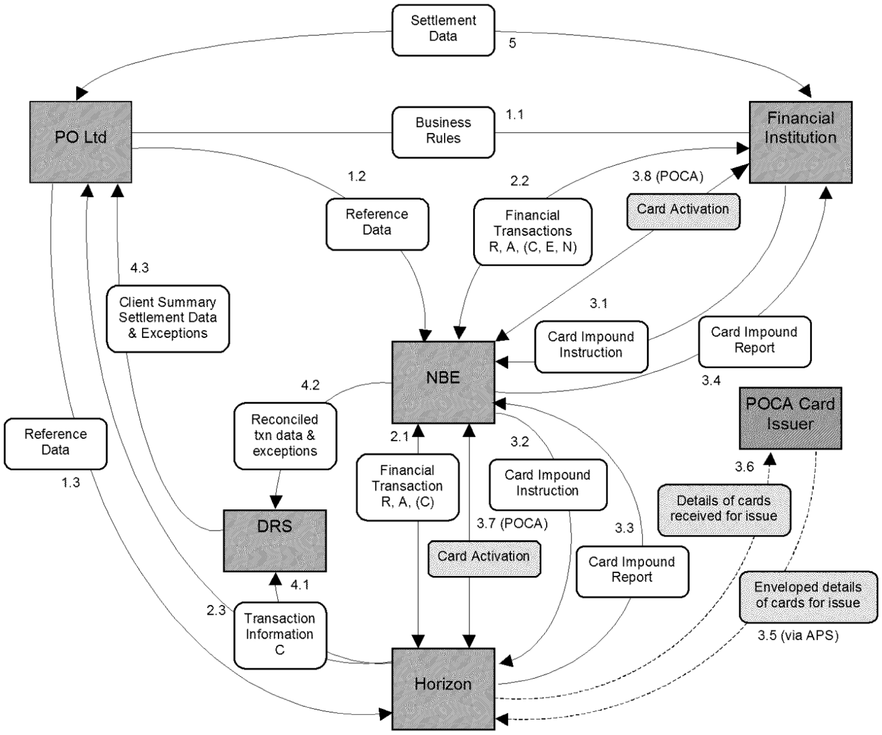


Figure 4 – NBS Context Diagram

3.3.1 NBS Entities

The following entities are defined in the above diagram.

- *Financial Institution* represents all the organisations that are served by the NBE (including those accessed only via LINK)
- *NBE* supports the interface between the Horizon system and all the FIs that are served by NBS. It is the only interface to the FIs for Horizon. It normalises all the different FIs' interfaces so that they appear the same throughout the rest of the Horizon system.
- *PO Ltd* represents the operational part of the PO Ltd organisation
- *Horizon* represents the computer systems operated by Pathway, including those located at the Campuses and the Counter PCs installed in Outlets
- *DRS* represents the application that reconciles the various data flows, and provides settlement data to PO Ltd based upon the transactions executed
- *POCA Card Issuer* represents the organisation that issues Post Office Card Account (POCA) cards for collection and validation in Outlets

3.3.2 Data Flows

There are five principal groupings of data flow types, represented on the diagram by numbering conventions according to the following primary digit.

[9] *Those omitted are concerned mostly with handling of Key material used for encryption*

1 Business Rules and associated Reference Data
2 Financial transactions relating to operations on bank accounts
3 Operations on account cards
4 Reconciliation related data
5 Settlement related data

The data flows shown are described in the following Sections

Data flow	Nature	Section
1.1	Business Rules from FI to PO Ltd	3.3.2.1.1
1.2	Reference Data from PO Ltd to NBE	3.3.2.1.2
1.3	Reference Data from PO Ltd to Horizon	3.3.2.1.3
2.1	Financial Transactions Horizon to or from NBE	3.3.2.2.2
2.2	Financial Transactions NBE to or from FI	3.3.2.2.3 and 3.3.4.3
2.3	Financial Transaction Reporting Horizon to PO Ltd	3.3.2.2.4
3.1	Card Impound Instruction FI to NBE	3.3.2.3.3
3.2	Card Impound Instruction NBE to Horizon	3.3.2.3.3
3.3	Card Impound Report	3.3.2.3.3
3.5	Card Distribution	3.3.2.3.3
3.7	Card Activation	3.3.2.3.2
4.1	Reconciliation Reporting Outlets to DRS	3.3.2.4.3
4.2	Reconciliation Reporting NBE to DRS	3.3.2.4.4
5	Settlement	3.3.2.5

Table 1 – Data Flows

3.3.2.1 Business Rules and Reference Data

3.3.2.1.1 Business Rules from FI to PO Ltd

All Business Rules used by Horizon or the NBE originate from discussions between the FI and PO Ltd, and identify the agreed basis on which PO Ltd undertakes business transactions on behalf of the FI. The definition of the operational flow is outside the scope of this document. Neither the NBE nor Horizon has a direct interface to the FIs for such rules. PO Ltd is responsible for ensuring their consistency through PO Ltd Reference Data used by both Horizon and NBE

3.3.2.1.2 Reference Data from PO Ltd to NBE

Responsibility for defining this interface rests with PO Ltd, in consultation with the NBE supplier.

3.3.2.1.3 Reference Data from PO Ltd to Horizon

The existing Reference Data interface and distribution mechanisms will be employed, and will be extended to incorporate NBS specific Reference Data (FI, token and product).

Any dynamic Business Rules incorporated within the transactional data flows are covered within Interfaces 2.1 (Section 3.3.2.2.2) and 2.2 (Section 3.3.2.2.3)

[10] *Source: [RAC], modified to show the position of each Platform*

3.3.2.2 Financial Transaction Data Flows

The key transaction flows within the NBS application are defined by the "RAC" model shown below[10]. (This diagram specifies the platforms on which various processes and data stores are located.) [NBR020]

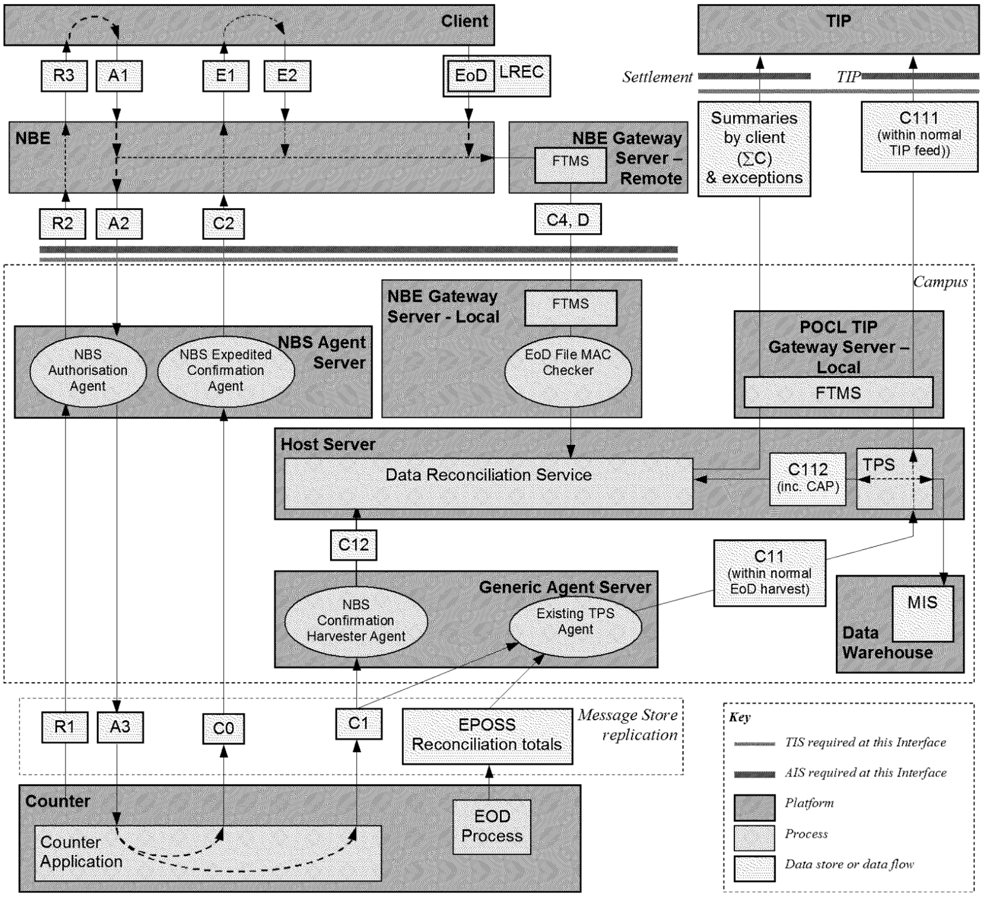

Client
R3
A1
E1
E2
EoD
LREC
TIP
Settlement
TIP
NBE
NBE Gateway Server – Remote
FTMS
Summaries by client (ΣC) & exceptions
C111 (within normal TIP feed))
R2
A2
C2
C4, D
Campus
NBE Gateway Server - Local
FTMS
NBS Agent Server
NBS Authorisation Agent
NBS Expedited Confirmation Agent
EoD File MAC Checker
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 – RAC Model and Data Flows[11]

The main data flows are shown on the left. Each small light blue box represents a message. It is identified by a Letter indicating the type of message and a number representing its form at that point. The number represents the fact that the format of the message may be transformed at various stages, but the overall purpose is the same.

Each transaction has three steps, each generating a separate message:[12]

- 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*

[10] *Source: [RAC], modified to show the position of each Platform*

[11] *Source: [RAC], repeated in [SRS], and modified to show position of NBS Agent processes and the platforms that they run on*

[12] *An additional message type, Financial Advice Notification [F], is identified within the RAC Model for any Counter transaction that is authorised locally or which does not require authorisation. This is not required for NBS*

(see Section 5.7.2) will process the Request, reformatting it into the [R2] message and send 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*. 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. The [C] message will contain timing data to show how long was spent in the Pathway domain, and how long in other domains. This data is used subsequently at the Data Warehouse to calculate data relating to SLAs
- 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)

3.3.2.2.1 NBS Transaction Types

The following NBS transactions are specified in [SOR], with verification provided by Signature or PIN as defined.

Banking Transactions	Verification by Signature (S) or PIN (P)
Cash Deposit [NBR002]	-
Cash Withdrawal [NBR003]	S, P
Balance Enquiry [NBR004]	S, P
Cash Withdrawal With Balance	S, P
Withdrawal of Entire Balance With Balance Report (“Withdraw limit”)	P
Change of PIN at PIN Pad	P
Recovery Transactions	
Recovery of NBS transactions following premature logout or system failure	---
Card Management Transactions (POCA cards)	
Receipt of Card at Outlet (handled by APS)	---
Activation of a POCA Bank Card (Counter procedure only)	---

Table 2 – NBS Transaction Types Supported

Voiding of any transaction is permitted, in accordance with defined Business Rules, and must occur prior to transaction commitment to the *Electronic Point Of Sale*

Service (EPOSS) stack. Once a transaction has been entered onto the EPOSS stack, it shall become non-voidable. [NBR458, NBR480]

The On-line "Change PIN" transaction allows the Customer to change the PIN associated with a card. This follows the RAC model, although the transaction is non-voidable and non-reversible once the [A3] is received at the Counter[13].

Other transaction types (e.g. opening or closing an account, or Customer complaints), are outside the scope of this SDS.

3.3.2.2.2 Financial Transactions – Horizon to or from NBE

[R] and [C0] messages flow from Horizon to NBE and [A] messages from NBE to Horizon. [R], [A] and [C0] messages are sent from the Outlet to the Campus by immediate messaging, [C1] messages by normal messaging (i.e. on the next replication payload triggered by the next immediate message or at the next subsequent replication interval). [NBR021, NBR038]

[C4] and [D] messages can also flow from the NBE to Horizon. These are described in Section 3.3.2.4 below.

3.3.2.2.3 Financial Transactions – NBE to or from FI

[R]s flow from the NBE to FI and [A]s from the FI to the NBE. Several variants of confirmation and exception reporting exist which affect the NBE treatment of [C] messages.

3.3.2.2.4 Financial Transaction Reporting Horizon to PO Ltd

The existing TPS data interface and file mechanisms will be employed to transfer details of NBS transactions to PO Ltd. This is an end-of-day file based flow for Outlets that report an *End of Day* (EoD) position, following harvesting at the Campus. No changes are planned to this interface, and so the only information about NBS transactions passed to PO Ltd are those attributes of the transaction common to other EPOSS products.

3.3.2.3 Card Operation Data Flows

3.3.2.3.1 Card Distribution

POCA account cards will be physically transferred to Outlets for issue to Customers. The card envelope will be read at the Outlet and recorded as an APS card receipt transaction to confirm delivery of the card to the Outlet. The details are outside the scope of the Pathway NBS developments.

3.3.2.3.2 Card Activation

An On-line card activation transaction is required for POCA cards during the Counter process of issuing the card to the Customer. This is outside the scope of this SDS, but by convention, this will be generated as a "balance enquiry" on the account. This will be recognised by the FI as the first transaction using the card, and must be transacted at the Outlet associated with the card issue (i.e. as previously notified via message flow 3.6). The transaction will follow the RAC model. It will be non-voidable and non-reversible once the [A3] is received at the Counter.

[13] *The exact end-end logic depends upon whether banking host functionality is available to confirm and/or undo a PIN change transaction. The working assumption is as stated.*

Card Activation messages are not written to the DRS.

3.3.2.3.3 Card Impounds

NBS supports Card Impound actions initiated by the relevant FI in response to an [R] from the Counter. The impound instruction will be included within the [A], carried as a response from the NBE that is interpreted by the Counter Application as an Impound directive. [NBR014]

The results of the Clerk instruction – normally a confirm, but exceptionally a failure outcome might need to be returned – will be recorded in the message store for audit purposes.

It is expected that the Counter procedures will provide the Clerk with autonomy to instigate a card impound in response to physical card characteristics observed during Counter processing, for example defaced card or signature mismatch between card and receipt. It is noted that existing PO Ltd procedures provide for such impound situations and that such Counter initiated impounds will not be reported electronically to the FI via the NBE. This functionality lies outside the scope of NBS and it is assumed that existing procedures will be used to support any such capability.

3.3.2.4 Reconciliation Data Flows [NBR040]

3.3.2.4.1 Reconciliation Principles

Reconciliation information is exchanged between Horizon and PO Ltd (including the NBE) to facilitate reconciliation of transactional data flows and to provide PO Ltd with financial summary data to support the FI settlement process. Comprehensive facilities are already provided within Horizon to support reconciliation across existing interfaces, based on end of day control flows and reporting. These will be retained for NBS. [NBR159]

Reconciliation processing will be applied to all financial NBS transactions. It will not apply to non-financial transactions such as card activation, and these transactions will not be recorded in the DRS.

There are three views of the transaction data which are to be reconciled. Essentially, they should be the same but separated by time.

a. The Outlet view as recorded in the [C1]

b. The NBE view (derived from the [A2] authorisation, possibly modified by a subsequent [C2]), and consequent upon this, the FI view

c. The PO Ltd central systems view, as reported from Horizon via the PO Ltd *Transaction Information Processing* (TIP) interface

Settlement between PO Ltd and the FI is based upon (b), which must be reconcilable with (c) and the aggregated Outlet view (consolidation of (a)).

The Outlet view is the definitive outcome of the transaction, based upon the single [C1] message generated by the Counter application and written as part of the EPOSS session data. This forms the (single) basis for transaction reporting to PO Ltd as part of the EPOSS transaction stream for reporting to TIP.

The principal issues to be addressed are the timing differences between the various interfaces and the mechanisms by which a consistent view can be obtained.

Transactions reported from the Outlets to NBE (i.e. [C111] messages), and transactions reported from Outlets to TIP (i.e. [C1] messages), can be different at any point in time as a result of incidents such as the following.

- Outlet EoD processing may be deferred
- TIP may reject files, following Pathway EoD processing

3.3.2.4.2 The Data Reconciliation Service

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:
  - [C12] – as derived from the *NBS Confirmation Harvester Agent*
  - [C11] – as reported to TIP
  - [C4] – as reported from the NBE across the FI interface

  This position is maintained for each combination of IIN (range) and service. Since there is no single PO Ltd EoD cut off, settlement and reconciliation will both be based upon the FI settlement day[14] boundary as a synchronisation point. This is notified to Horizon within the [A2] message and via trailer records within the [C4] file, such that each [C4] file can be recorded as associated with a FI settlement day.

  Where a zero-value [C0] is created following timeout of the [A], this value will be blank and the Settlement Date will be provided in the [C4] message. Normally such transactions will have no net settlement significance, although the original [A] may generate a FI settled transaction posted on the day of authorisation, which is reversed on a later posting day, following receipt of the [C2][15]. The DRS will apply separate reporting category rules for dealing with exceptions reported by the NBE e.g. [D] which will require investigation and manual corrective adjustment.

  The immediate status of any specific transaction will be reflected in one of the internal transaction states within the DRS.

[14] *The day at which the transaction is brought to account by the Bank. Theoretically, this could be generalised to other specified time intervals subject to review of, and agreement on, the processing implications.*

[15] *In these situations, two settlement transactions on different days may be generated from one Counter transaction.*

3.3.2.4.3 Reconciliation Reporting – Horizon Outlets to DRS

There are two types of message flow between Horizon Outlets and the DRS.

- *Individual [C12] transactions*. These are transferred throughout the day by the *NBS Confirmation Harvester Agent*. Harvesting is done on a continuous basis, with the [C12]s loaded into the DRS in recoverable commitment units, following normal replication of the [C1] messages within the EPOSS transactions
- *EoD transaction processing of [C11] transactions*. As part of the normal EoD Campus processing, TPS transaction harvesting will occur following receipt of the EoD marker from Outlets. This provides a delineated set of completed transactions up to the Outlet declared EoD, which forms the basis for transaction reporting to TIP. (Subsequently such transactions also provide the basis for calculating the Cash Account report for TIP.)

  NBS transactions included within the TPS harvesting will be forwarded to the DRS to provide an aggregated Outlet position to support reconciliation. Such transactions will be consistent with the Outlet reported transactions sent to TIP (other reconciliation measures detect inconsistencies within the TIP reporting stream), and will include the intended *Cash Account Period* (CAP) in which they will accounted by PO Ltd (as part of the TIP processing).

3.3.2.4.4 Reconciliation Reporting – NBE to Pathway (DRS)

The NBE will send a [C4] message for each [R] or [C2] received indicating that the transaction has been reconciled within the NBE and across the FI interface, permitting settlement to be initiated by the FI. Errors will be reported from NBE to DRS using a [D] message. The only transaction condition reported in this way is where the NBE has received a [C2] too late to Reverse the original authorisation.

The NBE will include the settlement day on each [A] returned to the Counter and it will be copied by the Counter application into the [C1] message. The settlement day will also be included in [C4] messages.

These [C4] and [D] messages will be sent in a set of batch files at end of day.

3.3.2.4.5 Reconciliation Reporting – Pathway DRS to PO Ltd

This is Interface 4.3 in Figure 4. A number of reports are generated, some daily and some weekly, as defined in [DRSREP].

3.3.2.5 Settlement

The actual settlement flow is outside the scope of this document.

For NBS, it is understood that PO Ltd will settle with each FI on a rolling basis against the FI consolidated position based upon its view of actual and projected transactions, as reflected in the NBE to FI interface. This is consistent with the reconciled [C4] position.

It should be noted that the FI position will be based upon its view across the FI–NBE interface, whereas the PO Ltd position will be based upon its view from the settlement summary supporting data from the DRS.

3.3.3 Transaction Modes – Online, Fallback and Offline processing

Three generic modes of transaction authorisation are identified. Only the first of these (On-line) is permitted in NBS. The authorisation is undertaken by On-line reference to a central authoriser. Within Horizon, On-line authorisations are routed via the NBE, which supports the interface to the Financial Institution. This is the model described in 3.3.2 above. [NBR011, NBR012]

3.3.4 Interfaces within the End-to-End R, A, C Message Structure

Four generic message handling layers are defined within the RAC model.

- Horizon Outlet
- Horizon Campus
- NBE
- Financial Institution, either direct or via a proxy such as LINK

In addition, the existing Horizon-to-PO Ltd TIP and Reference Data interfaces remain and are enhanced for NBS. [NBR511]

The detailed Service Boundary points for each of these interfaces will be established by the *Application Interface Specification* (AIS) and *Technical Interface Specification* (TIS) (or equivalent) document sets. These are required for each of the points identified in Figure 5. [NBR285]

The significant interface for Pathway is that between the Horizon Campus and the NBE. This interface is defined as an XML-based data flow. Each of the supported transaction types will utilise a specific XML definition.

3.3.4.1 Horizon Outlet to Campus

This is an internal Horizon interface that is carried by the Riposte messaging middleware.

[R1], [C0] and [C1] messages are submitted to the messaging system at the Outlet and are read by Agent processes at the Campus.

[A3] messages destined for a specific Outlet are also entered into the message system at the Campus by the Agent process, and are read at the Outlet by the Counter application.

Standard bi-directional Riposte message replication is used between Outlets and Campus. Where an ISDN call is required to the Campus:

- Immediate message replication (using Priority messages) is used for the On-line message flow [R1]/[A3]. The ISDN line is opened for the [R1] message[16], and then is held open (until the defined timeout period and for a short period thereafter) to facilitate the immediate transfer of the returned [A3]
- Immediate replication is used for [C0] messages. These are written immediately the outcome of the [A] is known, in effect while the ISDN line is still open

[16] *If not permanently connected*

- Normal replication is used for [C1] messages. These messages are written at the end of the customer session and are transferred on the next replication payload (likely to be the next NBS transaction executed in the Outlet)

3.3.4.2 Horizon to NBE

The NBE interfaces to the Horizon Campuses, and all communication with the Outlets is carried through the Campus. The logical interface between Horizon and the NBE is, again, a set of XML documents.

An AIS and TIS are both required at this interface. Both are expected to be generated by IBM.

- The [R1] from the Outlet is mapped to an [R2] for transfer from the Campus to the NBE. [R1] messages that have failed to transfer to the Campus using immediate replication (i.e. "stale" [R]s) will not be forwarded as [R2] messages, since the Counter system will have already timed out the transaction and forced a zero-value outcome [C1]
- The [A2] from the NBE to the Campus is mapped to an [A3] for the Outlet and sent via immediate messaging (as the link will have been kept open until the [A3] arrives)
- A [C0] from the Outlet is mapped to a [C2] at the Campus by the *NBS Expedited Confirmation Agent* and is transferred to the NBE partition that processed the original [R]

The underlying network transport mechanism between the Campus and the NBE is an appropriate TCP/IP based infrastructure.

Note that the operation of this interface may occasionally result in multiple copies of the same [R] or [C0] being sent to the NBE[17]. The NBE requires the capability to detect and discard such duplicates. It can recognise them by the use of repeated Transaction ID. Note that this is at variance with a strict interpretation of [NBR180], but is presaged by [SRS].

3.3.4.3 NBE to FI

At a detailed level, this is expected to be dependent upon bilateral agreements with each FI, although wherever possible a common approach will be used. A common logical level interface is assumed, in line with the above transaction types.

- Request (NBE to FI) – dataflow [R3] (immediate messaging)
- Authorisation (FI to NBE) – dataflow [A1] (immediate messaging)
- Confirm (NBE to FI) – dataflow [E1]/[E2] (as needed – FI specific)

The nature of this interface will be agreed between PO Ltd, each FI and the NBE supplier.

3.3.4.4 TPS to TIP

This interface provides details of transactions harvested from Counters to TIP. It remains essentially unchanged. The data content is unchanged. The volumes are

[17] *Typically during recovery from certain classes of failure condition*

expected to decline as *Order Book Control Service* (OBCS) transactions are replaced by NBS ones or claimants go elsewhere (e.g. a bank ATM) to obtain their benefit.

3.3.4.5 DRS to TIP

A new interface is required to support the flow of Settlement data from the DRS to PO Ltd. This will use the existing communications link from Horizon to TIP.

3.4 The NBS Desktop Service

Chapter 6 provides full details of the transaction dialogues and the interactions with the RAC model. Each dialogue consists of the following stages:

- *Data Capture* of the data held on the card
- *Identification and authentication of the token,* including validation against Business Rules held in Reference Data
- *Identification and verification of the Customer,* by signature or by PIN
- *Transaction request and authorisation,* using the RAC model to obtain an authorisation or decline from the NBE
- *Printing receipts,* one for the Customer and, in some cases, one to be retained in the Outlet

3.4.1 Application Principles

3.4.1.1 Audit Data

The architecture for the Horizon platform ensures that audit data is generated automatically for all messages handled by the Riposte Message Store. Messages received by the Correspondence Servers are automatically harvested and written to an Audit Server for long term storage. [NBR453]

3.4.1.2 Information Retrieval

The existing Horizon audit infrastructure provides facilities to enable audit information to be retrieved, on request, and made available to PO Ltd Auditors. These facilities will be enhanced as described in Section 13.5 to support:

- Increased data volumes, caused by the requirement to hold NBS audit information for up to seven years
- An increased number of requests for audit retrievals as envisaged by [SOR]

In addition, limited facilities will be provided by Pathway's *Management Support Unit* (MSU), via the DRS, to retrieve transaction information for a period of up to three months from the date of the transaction. These may be used to resolve disputes. [NBR260]

Further requirements may be identified in a proposed information retrieval study, and could be implemented beyond the NBS Release 1 timescale.

3.4.1.3 Interpretation of Response Codes

Ideally, it would be the responsibility of the NBE to interpret the FIs' response codes and generate the appropriate responses and text for printing on receipts. However, the NBE will not do so and the transformation to error messages will be made at the Counter. The relevant error codes are documented in [CNTRDLG]. Note that this contravenes [NBR423]

3.4.1.4 Presence of Token

It is a requirement that the Customer must be present with his token to carry out an NBS transaction, and it is PO Ltd's responsibility to enforce this procedurally.

3.4.1.5 Completion of NBS Transactions

Once an NBS transaction has been initiated, and an [R] generated, then that transaction must complete before another transaction can commence at that Counter. In particular, the Counter will not register further token swipes until the first transaction is confirmed and added to the transaction stack (or timed out). [NBR468]

3.4.1.6 Introduction of New FIs and Cards

New cards or card ranges may be introduced by OBC where the FI and the interface to it already exist.

Additional PO Ltd Reference Data and trials will be required when a new interface is required (data mapping the IIN to the Routing Gateway) [NBR024]

The addition of a new Client FI or a new interface to an existing Client will be subject to Change Control, because this may impact Pathway applications (e.g. DRS). [NBR412]

3.4.1.7 Currencies

Counter transactions are recorded in Pounds Sterling (GBP) only. EPOSS does not have the capability for recording transactions in Euros.

Pathway notes that PO Ltd are planning for Euro capability from 21/02/2004, but this is not being delivered in this release of NBS. NBS will be designed so as not to preclude future developments to transact business in Euros (for example it will record the currency (GBP) used as part of the transaction data) [NBR399, NBR153].

3.4.1.8 Transaction Identification

Transactions will be uniquely identified by the Counter application such that it is possible to follow them through for subsequent enquiries.

- The Riposte *Application Programming Interface* (API) *RiposteUniqueID* is used to generate a Request Id (in the form *44-gggggg-cc-nnnnnn-uu*, where "gggggg" is the Outlet's *Finance Accounting Division* (FAD[18]) code, "cc" is the Counter position and "nnnnn" is a monotonically increasing number for that Counter.
- The receipt will contain sufficient of this to enable the rest to be reconstructed

[18] *The FAD Code is the supposedly unique number used by the Horizon system to identify Outlets*

- The Transaction Time will be included in the [R] and printed on the receipt. This will be in Local Time in the format *hh:mm:ss*. [NBR158]

3.4.1.9 Service Boundaries

The interface between the Pathway Domain and the PO Ltd operational domain will be detailed in both an AIS and a TIS, which will ensure that service boundaries and responsibilities are clearly marked between the domains. [NBR050, NBR285]

3.4.1.10 Impact on Cash Account

The Confirmation [C] will form part of the associated EPOSS Transaction, i.e. a single message will be recorded at the Outlet at the completion of the Transaction. This will ensure that value of Withdrawals, Deposits and Balance enquiries will be reflected in the Cash Account, [NBR017, NBR182, NBR464].

NBS transactions are mapped to a product, dependent upon the IIN and the transaction type (e.g. Withdrawal). These are mapped to the appropriate Cash Account line as defined by PO Ltd Reference Data [NBR018, NBR261].

The Cash Account records all [C] transactions, including zero value transactions. [NBR263]

3.4.1.11 Help Functions

“Bubble Help” functionality is supported in WebRiposte as in “conventional” Riposte. These will be verified and approved by PO Ltd *Business Service Management* (BSM) Development team prior to authorisation for distribute to Outlets.

Processes and Procedure documents (PPDs) are to be produced which will provide assistance to staff by describing the procedures to be used when exercising NBS Service functionality at the Counter, including exception conditions

3.4.1.12 Forced Session End

Forced session end will not compromise the integrity of the RAC model. In the event of there having been a Request [R] generated, but no matching Confirmation [C], a forced session end at the Counter must not breach integrity by orphaning the [R] with no corresponding [C]. At the next logon, a “recovery” [C] will be generated to complete the transaction history. [NBR072]

3.4.1.13 NBS Integration with Existing Applications

NBS transactions are integrated with the Counter system such that the Clerk can carry out any of the transaction types supported (e.g. OBCS, EPOSS, APS and NBS) as required. Initiation of NBS transactions at the Counter will be supported by the touch screen and the keyboard as well as the magnetic swipe card reader. [NBR438, NBR450]

As with existing applications, the Counter Clerk will be is led through the steps of the NBS transactions, with prompts as necessary to minimise reliance on the skill and knowledge of the Clerk. [NBR451]

3.1.1.14 Message Logging

The message logging function ensures that a unique Session Identifier is generated for every session transacted. The Session Identifier is used to associate a group of transaction(s) with a particular session. The Session Identifier will include the Outlet's FAD Code, which is unique across the estate.

3.1.2 Session Settlement

After one or more sale items have been selected and placed on the Product Stack, the user can initiate the payment phase via the Finish Button. Settlement is part of the current EPOSS Transaction Service and is concerned with the final settlement, validation and committal of the transaction stack.

The Settlement function checks the outstanding balance (including NBS transactions) to determine whether a transaction session can be committed, and displays the Settlement menu for manual payments. The outstanding balance must reach zero for the current transaction session. When this is the case, all transactions on the Product Stack can be committed into the message store and the Product Stack is cleared for the next session.

There is no check that only cash is accepted for the cash deposit transaction.

3.1.3 Outlet Reports

A number of new reports can be printed on the Counter printer. See Section 5.4.4.1.7 and [CNTRDLG]. [NBR256]

3.1.4 Message Recovery

An NBS transaction requires On-line Authorisation before it can positively progress. Copies of the [R] and [A] are recorded in the message store from whence they can be replicated to restore lost data at the Counter (e.g. following a Counter failure). System failures at the Counter can result in failure to write a [C], or loss of the message before it is replicated. Thus, on Clerk log-on, the Counter will carry out a health check to ensure that there are no missing [C] messages. If there are, it enters the *Recovery of Banking Transactions* process, which determines the outcome of each transaction and generates the appropriate [C]. [NBR013, NBR505, NBR037]

This is the case irrespective of whether the failure is catastrophic, requiring replacement of the Counter system, or a temporary problem cured by re-booting the Counter system; whether the failure is at a single or multiple Counter office. This process will apply at Clerk log-on.

- For an [R] with no [A], or the [A] is a Decline with no request to retain the card, then the process generates a zero-value [C0] (decline) with an appropriate error code
- A [C] is generated automatically for Balance Enquiries
- For an [R] with an [A] that is an Approve or a Decline (retain card), the process prompts the Clerk for the outcome as recorded on the Outlet copy of the receipt. An appropriate [C] is generated. [NBR035, NBR176]

Chapter 4 - Design Principles and Assumptions

4.1 GENERAL

The previous Chapter describes the service to be provided, both in terms of its implementation on the Counter desktop, and the data flows within Horizon and to other entities that are involved in the End-to-End NBS Service.

A fundamental requirement is that the NBS service is to be provided via the existing Horizon system. This imposes a number of constraints on the way in which it can be developed and implemented. In addition, there are a number of significant features of the Horizon system, many of them included in the *Codified Agreement* [CA] and supported by SLAs, which must not be impacted by the introduction of NBS.

This Chapter discusses the design, development and timescale principles that arise from the need to integrate NBS with the existing Horizon system.

It also identifies a number of outstanding issues that have not been clarified during or since the extensive series of Workshops that preceded the development of this SDS. Pathway has made assumptions about the outcome of these issues, to enable it to complete the process of developing this specification and estimating the costs involved in the development of NBS. These assumptions are listed here.

It excludes functionality that is specifically excluded in Chapter 3.

4.2 ISSUES AND ASSUMPTIONS

This Section lists the principal assumptions and issues that affect the service provided to PO Ltd. Each of the following Chapters also contains a list of more technical issues that will be resolved during the High Level Design process.

4.2.1 NBS Application Functionality

4.2.1.1 Undo

"Undo" is where a transaction may be cancelled after the transaction is complete, but before the Customer session is settled. This is normally done using the *Bin* button on the Desktop.

[SRS] makes it clear that Undo is not to be supported. The Network Banking Counter Application must therefore ensure that no action is taken when the Desktop's *bin* button is used to attempt to undo a Network Banking Transaction.

4.2.1.2 Lost or Stolen cards

Neither the NBS nor the *Horizon System Help Desk* (HSHD) provides a service for Customers who have lost their cards or had them stolen. The NBE provides a service to instruct the Counter Clerk to impound a lost or stolen card. If a lost or stolen card is used and the transaction is rejected, this is counted as a successful transaction in the Pathway domain SLAs.

4.2.1.3 Damaged Cards

Service for Customers with damaged cards is by manual entry of the card details (if they can be read). No facilities are provided for cards where the embossed details are unreadable.

4.2.1.4 Incorrect PINs

Transactions where the PIN verification fails are counted as successful transactions in the Pathway domain.

No attempt is made by the system to limit the number of PIN retries. Each will be considered a separate transaction.

The HSHD does not provide a service to resolve PIN issues.

4.2.1.5 No Funds

Transactions where monies are incorrectly delivered or delivered late to the FI, and thus a cash withdrawal transaction is declined, are counted as successful transactions in the Pathway domain.

The HSHD does not provide a service to resolve such issues.

4.2.1.6 Transmission of [C] Messages

The only [C] messages that are to be written to the NBE are those where the Outcome may differ from that Authorised by the NBE in the [A2] message. The circumstances in which this can occur are:

- The Clerk has Declined a Transaction that the NBE has Authorised
- A Failure has occurred (such as a Counter timeout), and so the Counter has Declined the Transaction and the status of the [A] is unclear

In the second case, it is likely that the [R] was never passed to the NBE.

In either case, the Counter will generate a [C0] message for immediate transmission to the Campus. It is handled by the *NBS Expedited Confirmation Agent*. Each Agent instance is bound to a particular NBE Connection Handler (effectively a particular IP address and port), and uses the same message selection filter as the original NBS Authorisation Agent. This ensures that the message is handled by the same *Process Interface* (effectively the same NBE partition) as handled the original [R]. This is important because the NBE Process Interface keeps a cache of recently handled messages. Messages are cleared from this cache after a time, expected to be around ten minutes. If a [C2] is received by the Process Interface within this time window, the NBE can generate a Reversal ([E1]) to the FI. This Reversal will subsequently be communicated to Horizon in the [C4] batch files transmitted at end of day.

If the [C2] is not received by the Process Interface within the time window, then the NBE will process the [C2] at the end of day and generate a [C4] or a [D] as defined in Figure 6.

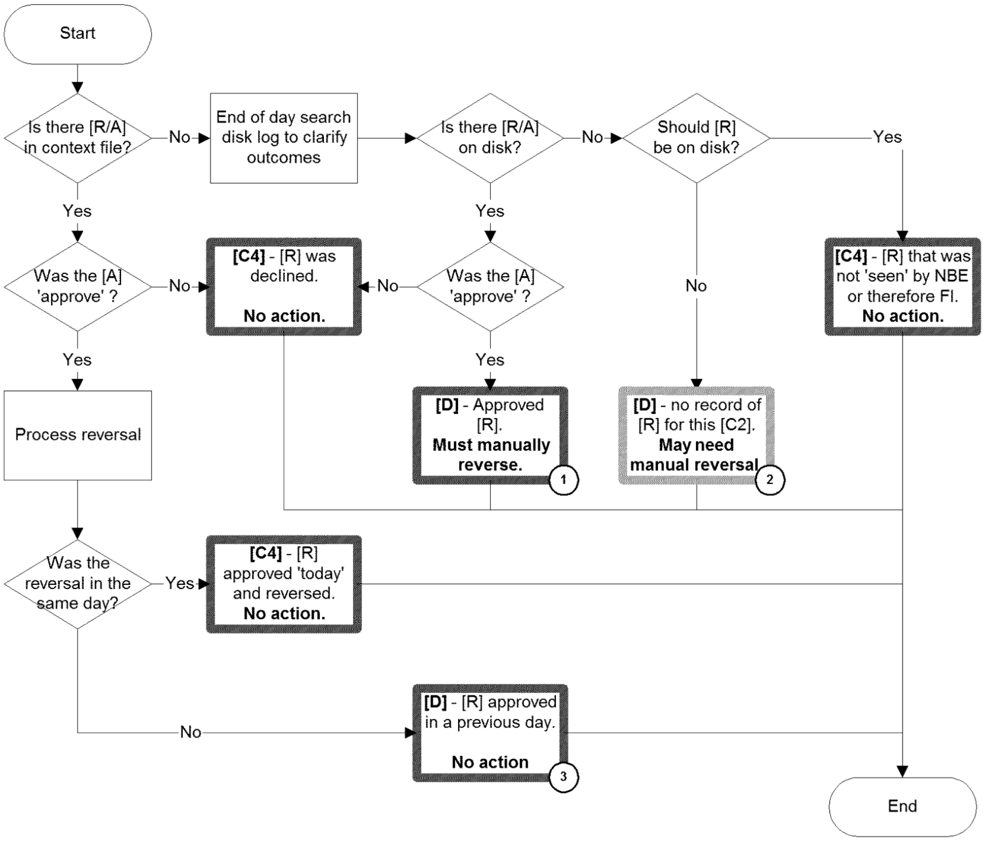

Start
Is there [R/A] in context file?
No
End of day search disk log to clarify outcomes
Is there [R/A] on disk?
No
Should [R] be on disk?
Yes
Yes
Yes
Was the [A] 'approve' ?
No
[C4] - [R] was declined.
No action.
No
Was the [A] 'approve' ?
No
[C4] - [R] that was not 'seen' by NBE or therefore FI.
No action.
Yes
Yes
Process reversal
[D] - Approved [R].
Must manually reverse.
1
[D] - no record of [R] for this [C2].
May need manual reversal
2
Was the reversal in the same day?
Yes
[C4] - [R] approved 'today' and reversed.
No action.
No
[D] - [R] approved in a previous day.
No action
3
End

Figure 6 – NBE EoD Processing

Pathway cannot guarantee that a [C2] will arrive at the NBE within the cache time window, and cannot accept any SLAs in this respect.

4.2.1.7 Forced Logout

Section 5.4.3.3 describes the session timeout mechanisms and the fact that if Session Mobility is inhibited, then the Session timeout mechanism is also inactive. The consequence of this is that if a Clerk leaves a Counter unattended in the middle of an NBS Transaction, then the terminal will not be locked or logged out.

This is no different from existing Desktop Applications.

4.2.2 Use of WebRiposte

[NBR022] requires Pathway to use WebRiposte.

Originally it was also required that Pathway should use Escher's WebRiposte Financial Transaction Framework. However in order to meet the NBS Timescales, this requirement has been dropped and the Network Banking Counter Application is now being developed as a VB application, though using the overall architecture of the WebRiposte FT Framework, thus providing the opportunity to consider utilising the Framework in the future.

4.2.2.1 Scalability of WebRiposte

The scalability of WebRiposte (i.e. the ability to support large numbers of concurrent connections) is unknown and will be evaluated by Technical Testing. Such testing will not be possible in the SDS timescales. Thus, if WebRiposte does not scale adequately, and the shortfall cannot be rectified by additional or upgraded hardware, it is assumed that Escher will resolve the problems in time for the NBS release.

Section 11.5.4 proposes an upgrade of the Correspondence Server platforms to the most powerful NT platforms available, plus additional memory to support known and agreed volumes. Adding additional Clusters, and reconfiguring the Correspondence Server layer accordingly, is a highly complex step that would disrupt both the existing service and the plans for the NBS service. It is therefore ruled out and, as indicated above, it is assumed that any scalability problems will be resolved by Escher.

A number of Riposte enhancements have already been identified (see [RIPENH]) and have been delivered but not yet tested.

- Sending multiple priority messages to the Campus when the Gateway PC is in a "connected" state. This is to improve availability
- Minimising the number of messages queued in the network between the Gateway PC and the Correspondence Servers to minimise response times (and timeouts). The current assumption is that Esher will provide an implementation that allows Satellite and ISDN latencies to be differentiated by a neighbour type (e.g. remote and local)
- Improved APIs at the Correspondence Server, to allow Agent Servers to know when a Correspondence Server is building indexes or archiving. This is to avoid performance critical Agent activity on a Correspondence Server that is heavily loaded

4.2.3 Legal Responsibilities

4.2.3.1 Legal Responsibilities for Universal Bank

It is assumed that there are no additional legal or regulatory requirements arising from providing NBS access to the Universal bank beyond those for other FI.

4.2.3.2 Data Processors

It is assumed that Pathway are Data Processors within the terms of [DPA] with regard to NBS.

4.2.3.3 Transaction Verification

Where the Counter Clerk accepts Authorised NBS transactions based on the verification of the Customer signature, then it is assumed that Pathway and the Horizon system are not responsible for any further verification of that transaction.

4.2.4 Impact of EFTPoS

EFTPoS volumetrics are included in the network capacity sizing but Pathway will not commit to supporting EFTPoS within the NBS configuration until [EFTSDS] and subsequent plans are approved. These will require enhancements to the NBS system and infrastructure defined in this SDS (for example to support an interface to a Merchant Acquirer). [NBR057]

4.2.5 Impact of YG and ERA

The infrastructure enhancements for NBS and EFTPoS are not designed to include any requirements for *Your Guide* (YG; formerly known as GGP) and/or ERA. The measures described in this SDS to free up space in Wigan and Bootle will not guarantee that any space is available to meet YG or ERA infrastructure requirements. Indeed, this space is likely to be required for EFTPoS.

4.2.6 Outlet Resilience Model

The general resilience within an Outlet will be as in S10. This SDS defines two levels of resilience as follows:

- Bronze Service Outlets will have a metered dial-up network connection
- Silver Service Outlets will have a permanent network connection and this will not usually incur the delay, and risk of non-connection, inherent in a dial-up link

4.2.7 Counter Hardware Configuration

It is expected that the current Counter applications plus NBS and the WebRiposte infrastructure, running under NT4 SP6a, will run in the existing Counter hardware configuration with no degradation of service and no requirement for a hardware upgrade[19]. This will be confirmed by testing before the NBS service is rolled out.

The NBS Counter Applications[20] must:

- Co-exist with the Horizon Counter applications on the Counter hardware platform as defined in [CHD]
- Operate on the existing Counter hardware platform without impacting the response times[21] of Horizon Counter applications e.g. when switching from a NBS transaction to a Horizon transaction
- Deliver response times similar to those delivered by the Horizon Counter applications. The Counter Clerk should experience similar response times for similar functions (e.g. changing menus) on both the NBS and the Horizon Counter applications

4.2.8 Service Boundaries

SLAs that apply to Service Boundaries must be measurable, in the sense that the time of transit, the volumes of data and possibly the data content, should be logged for all data crossing the boundary.

[19] *Other than the introduction of a PIN Pad*

[20] *Pathway cannot predict the additional Counter resources required by applications other than N\BS. Future requirements e.g. EFTPoS will be evaluated separately when more is known about the Counter application and how it will be implemented*

[21] *The NBS* **and** *Horizon applications will be benchmarked as part of the NBS testing strategy*

There are SLAs associated with service delivery, and an important part of this set of infrastructure enhancements is to ensure that sufficient information is collected at or near each boundary to establish the following.

- Ownership of any problems that arise
- Liability for SLA conformance

The information to be gathered must include the following.

- Timestamps near to the point where service responsibility changes
- Data volumes
- Responses (e.g. success/failure) from other parties

4.2.8.1 Data delivery SLAs

4.2.8.1.1 Reconciliation File Delivery

A new SLA is required to cover the delivery of reconciliation data. The working assumption is that Reconciliation data is available to PO Ltd by 08:00 on day ‘B’.

4.2.8.1.2 TIP File Delivery – With Additional NBS Data

TIP file delivery SLAs will be as in the current [CA].

4.2.8.2 Response Times

4.2.8.2.1 Limitations on Response Time Responsibilities

Pathway will be responsible for response times only within the Pathway domain including the Counter applications.

4.2.8.2.2 Response time SLA measurement

Response times at the Pathway to NBE service boundary will be at the last measurable point within the Pathway domain. Components in the Pathway Campus beyond the measurement point in the *NBS Authorisation Agents* (for example Firewalls or network components) will not form part of the Pathway domain when calculating response time SLAs.

Note that timestamps, where used for SLA purposes, should be collected on the same platform, for example by the outgoing and incoming messages that relate to the same transaction being handled by the same server. This is because there may be differences between the clock settings on different platforms that, though minor, could have a significant impact on SLA calculations. Pathway will not be in a position to accept any new SLAs where this provision cannot be met.

4.3 DESIGN PRINCIPLES

4.3.1 Performance & Scalability

4.3.1.1 Message sizes

Normal messages between the Outlets and the Campuses should be designed such that they are smaller than the TCP/IP packet size (approximately 1,400 bytes). They must not exceed the Riposte size of 2 Kb.

If there is a need to support mini-statements, these should be provided by a different (and less common) transaction type from Balance Enquiry, as the size of the [A] is likely to exceed these limits and may require a *Binary Large Object* (BLOB). [NBR324]

4.1.2 Changes Required to Existing Applications

Changes will be required to existing services (for example EPOSS, APS, Reference Data) to support NBS.

Changes will also be required to certain Pathway Infrastructure Applications (for example OCMS, ACDB, SYSMAN) to support NBS. All such changes are summarised in Chapter 12 of this SDS and described in the appropriate lower level SDS.

No changes or enhancements will be made to existing applications solely to improve performance, especially in respect to their memory footprints.

Chapter 5 Application Architecture

5.1 GENERAL

This Chapter describes the enhancements to the Horizon application architecture to support NBS. These enhancements include the introduction of WebRiposte. NBS and EFTPoS also both require connections from the Agent or Host layers to third party applications outside the Pathway Campuses.

5.2 REQUIREMENTS SUMMARY

There are two major requirements for enhancements to the existing Horizon system architecture.

- The mandated requirement to use WebRiposte within the Counter [NBR022]
- The mandated requirement that [R]s are handled, in real time, by an NBE, with [A] responses being returned to the Counter from the NBE. Performance and other considerations require the connection to the NBE to operate at the Agent layer.

5.3 OUTLINE OF NBS ARCHITECTURE

5.3.1 Overview

NBS is mandated to use WebRiposte and to anticipate the implications of any future introduction of the Financial Application Framework. These are new components within the Horizon architecture, and have a significant impact on the Counter structure. The need for access to a third party application (the NBE) has an impact on the components at the Agent layer. Both of these are described below.

In addition, NBS has ramifications for a number of existing Horizon components, including the following.

- It generates messages that affect the EPOSS reconciliation totals
- Card receipt is handled by new APS transactions (see Section 5.4.4.2)
- New message types, and the introduction of the DRS, have an impact on the TPS
Host Application
- New SLA types, and the data required to enable these to be calculated, has an impact on the Data Warehouse and *Management Information Service* (MIS) applications.

5.3.2 Horizon Vertical Application Structure

The Horizon application architecture uses a four-tier model. Each application is implemented as a vertical "stripe" across a number of Horizontal system layers, as shown below. This model defines a standard structure for all Horizon applications, and is supported by the infrastructure in a great many ways.

Each vertical stripe is ideally independent of the others, and should have no inherent knowledge of the other's implementation. New applications are added to the existing system by providing the relevant vertical components. Where some form of integration is required with another application, the mechanisms used vary between the layers.

NBS introduces some new components and new interfaces.

- There is a direct connection from the Agent layer to the NBE, acting as an application Client
- The introduction of WebRiposte provides some significant extensions to the functionality of the Counter architecture

The following diagram shows this four-layer architecture, as modified for NBS. It also shows the ways in which the architecture is intended to scale to support more applications or a higher workload, both of which are factors in the introduction of NBS.

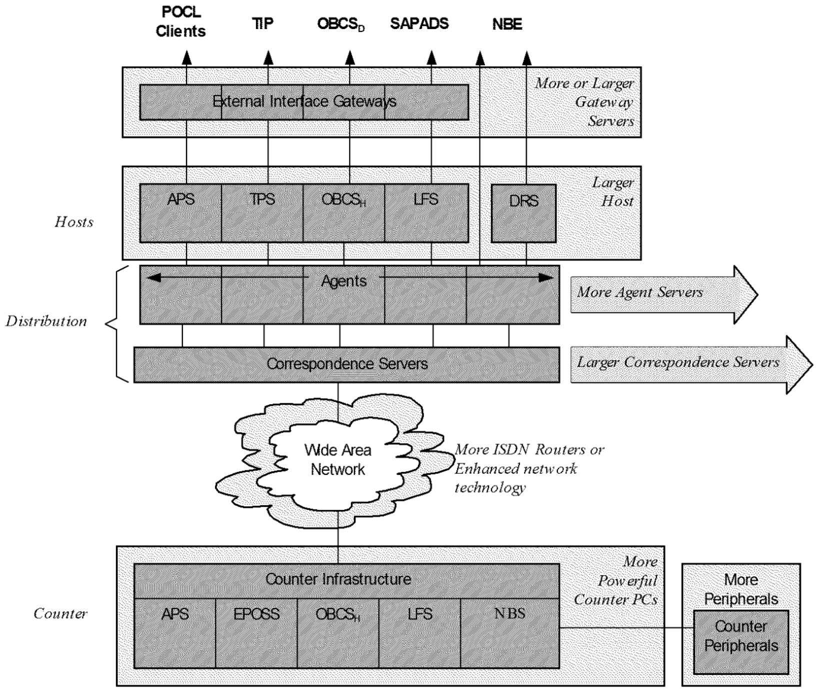


Figure 7 – Horizontal Scalability

5.3.3 Application Breakdown Structure

Conventionally, each Horizon application provides an elaboration of this model that involves a number of components at each layer. Some of these components are unique to the application, while others are modifications to components provided as generic functions or as parts of other applications. Every application needs to consider whether (and if so, how) to provide each of the boxes shown on the following diagram[22].

[22] *Source: [TED], and modified to include the influence of the WebRiposte Application Framework*

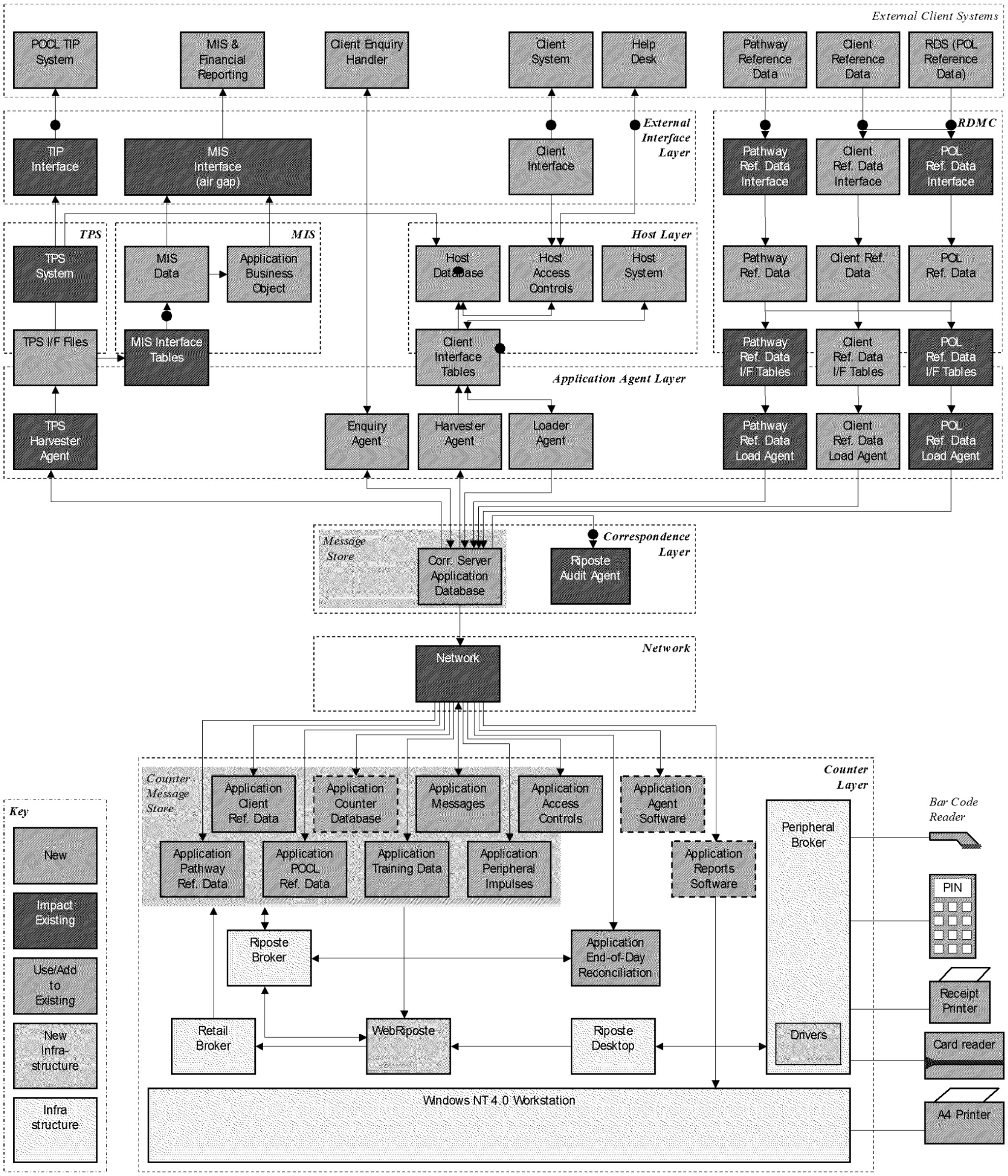


Figure 8 – Application Component Checklist

The following Sections discuss the changes introduced by WebRiposte in the context of this diagram. Each of the dotted groupings (Counter Layer, Correspondence Layer, etc.) identifies in the diagram maps onto a Section in the remainder of this Chapter.

5.4 COUNTER LAYER

This Section describes the structure of WebRiposte, its functionality, and the work required to integrate it within the Horizon Counter architecture to support the NBS Counter Application. [NBR022]

5.4.1 WebRiposte

WebRiposte provides a set of extensions to the Riposte desktop and message server. The new components are shown here.[23]

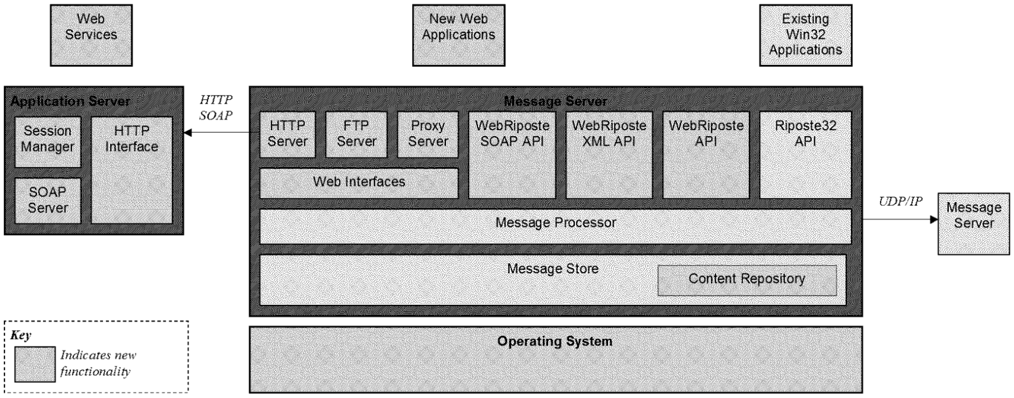


Figure 9 – Components of WebRiposte

The existing Riposte32 APIs, the Message Processor and Message Store continue, as does message replication to a remote Correspondence Server. These components continue to support existing 32-bit Riposte desktop application, such as APS, EPOSS, OBCS and *Logistics Feeder Service* (LFS).

In addition, new APIs are provided for use by Web based applications, and new Web Services are provided to support web applications (for example by providing access to Reference Data).

5.4.1.1 WebRiposte Components

5.4.1.1.1 WebRiposte API

This provides support for Web applications.

5.4.1.1.2 WebRiposte XML API

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

5.4.1.1.3 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.

5.4.1.1.4 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 existing 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

[23] *Source: Escher*

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. There is no requirement for this facility within NBS[24] and it will be disabled in line with the Horizon security policy.

5.4.1.1.5 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. This facility is not required for NBS, and will be disabled.

5.4.1.1.6 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. It is not needed by NBS and will be disabled.

5.4.1.1.7 Web Interfaces

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

5.4.1.1.8 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, they 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.

WebRiposte Objects are not used for NBS Release 1.

5.4.1.2 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. They are not used for NBS, but are listed here for completeness.

5.4.1.2.1 HTTP Interface

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

[24] *It would be useful to support YG access to web content that was too rarely used to be held on the Counter*

5.4.1.1.2 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.

5.4.1.1.3 SOAP Server

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

5.4.2 NBS Counter Application Structure and Components

This Section describes the structure of the Counter application and describes the functionality that it supports. It is summarised in the following diagram[25].

Although the NBS Counter Application will not be developed using the Escher Financial Transaction Framework, its structure will follow that of the Framework where feasible within the Release 1 timescales, as shown here.

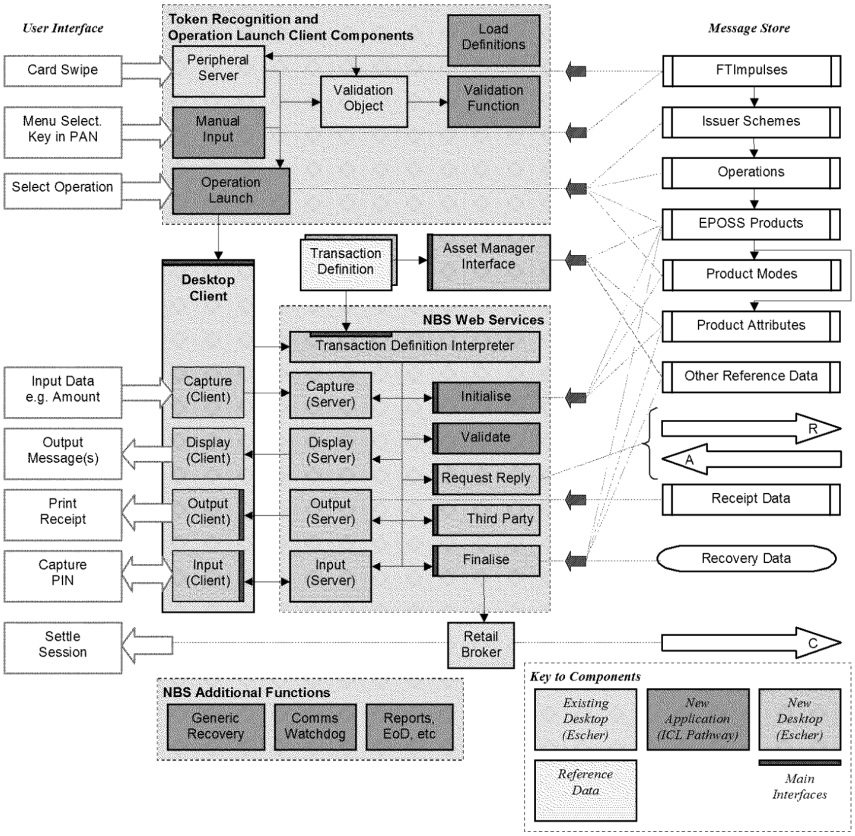


Figure 10 – Web Services Framework – Software components

The following sub-sections describe each component in turn.

> *The latest Framework definition from Escher has changed this substantially. However we have not attempted to change the design to match that.*

[25] *Source: Escher, modified by D.L.Johns*

Note that the term "Local Devices", used in earlier versions of this Document, has now been replaced by "Input".

5.4.2.1 Token Recognition and Operation Launch

This stage of the application is responsible for capturing data about a magnetic token that is used to initiate an NBS transaction. The data can be captured either via a card swipe or manually. It establishes the IIN of the token, 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. [NBR023]

5.4.2.1.1 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 a given Collection[26]. Such Temporal Persistent Objects should be accessible in a Subscription Group[27].[28]

5.4.2.1.2 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.[29]

The Impulse definitions will be held as Temporal Persistent Objects (as opposed to Web Objects) in a given Collection[30]. Such Temporal Persistent Objects will be accessible in a Subscription Group[31].[32]

[26] *Peripheral server is unable to do this directly, however an application can read temporal Reference Data and pass details of each Impulse separately to Peripheral server (as APS currently does).*

[27] *Initially it is likely that such data may not be provided in a subscription group*

[28] *This isn't a specific to NBS, but it is a requirement of the current Horizon system that all Reference Data is held as Temporal Persistent Objects accessed through the Retail Broker temporal interfaces*

[29] *This is existing standard functionality of the Peripheral Server*

[30] *Peripheral server is unable to do this directly, however the application can read temporal Reference Data and pass details of each impulse separately to Peripheral server (as APS currently does.*

[31] *Though initially it is likely that such data may not be provided in a subscription group*

5.4.2.1.3 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 NBS Counter Application would use the basic validation matching criteria, and will also provide an NBS card specific *Validation Functions* to be invoked as part of the analysis of each token.

Note that there are around 2,000 APS cards, 2,000 debit and 20,000 credit card types in circulation. There are potential performance implications in parsing the IIN if each is held individually. Therefore, it will be necessary to specify ranges of IINs, or use wild cards, to speed up the parsing process. [NBR413]

5.4.2.1.4 Validation Function

This validation function will handle ranges of IINs. It also handles the issue of distinguishing between the NBS and EFTPoS environments.

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.

5.4.2.1.5 Manual Input

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

This component represents the dialogue required to capture the *Primary Account Number* (PAN) from the card, and from this to identify the other items that need to be captured.

This will be done by displaying a dialogue to capture the PAN, and then passing the PAN 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, the Reference Data associated with the FT Impulse or Issuer Scheme Persistent Objects can be used to identify whether or not manual entry is supported for this token, and if so, which additional fields are 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.

There are likely to be a number of variations in the data to be captured, depending on the Issuer Scheme. These are:

- Need for Expiry Date[33]
- Need for Issue Number

[32] *This isn't a specific to Network Banking, but it is a requirement of the current Horizon system that all Reference Data is held as Temporal Persistent Objects accessed through the Retail Broker temporal interfaces*

[33] *Though it is likely that Expiry Date will always be required.*

- Need for Start Date

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").

This functionality is Platform specific and will be provided by Pathway as a *Manual Card Token Manual Input* component.

5.4.2.1.6 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 (see Section 5.4.5.3.). 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.

This component will be implemented as a traditional *Visual Basic* (VB) application by Pathway.

5.4.2.2 Desktop Client

This is the Desktop Client component of the Framework, and is a VB application provided by Pathway. It is responsible for all communication with the Counter Clerk, as defined by the Reference Data associated with the Operation selected by the Clerk. The application is invoked by passing it an impulse.

It invokes appropriate functions to interpret the transaction definition (held in Reference Data), and will execute requests along the lines of "what do I do next". It is responsible for driving the screen dialogues for the *Capture* and *Display* functions (invoking the appropriate functions to carry out any validation). It will also control printing, through the *Output* function, and the PIN Pad through the *Input* function.

5.4.2.2.1 Capture (Client)

This handles the dialogue with the Clerk for the Capture function as a normal Desktop Script.

5.4.2.2.2 Display (Client)

This handles the display dialogue and identifies which Button the Clerk has selected following the Display.

5.4.2.2.3 Output (Client)

This handles the output of data (for example receipts) to the printer. Variable Data is passed to the function for merging with a "Skeleton Report". The function is also responsible for the presentation of progress and error messages. In particular, it handles Print Preview and manual receipt printing. Pathway will develop this component based on the existing EPOSS Report Broker, thereby ensuring the Receipt can be reprinted later (i.e. after completion of the NBS transaction. [NBR155, NBR219]

5.4.2.2.4 Input (Client)

This handles the dialogue with the PIN Pad as specified by the transaction's Reference Data definition. It displays messages to the Counter Clerk allowing him to abandon the PIN input (for example if the Customer leaves without inputting a valid PIN value). It will return data captured from the PIN Pad (for example the value of the encrypted PIN). Pathway will develop this component.

5.4.2.3 Application Framework

The NBS application is implemented as a VB program that uses Reference Data to determine the underlying components to invoke for particular actions. It includes calls to a number of "hooks" which are invoked as .COM calls.

The Transaction Definition defines the Business Logic of the Transaction, in terms of a number of discrete steps. These are:

- The first call is always to the *Initialise* component
- Obtain data from the Clerk (*Capture*)
- Specify Validation routines for validating the data that is captured (*Validate*)
- Present information to the Clerk and seek confirmation (*Display*)
- Communicate with a PIN Pad Driver (*Input*)
- Invoke functions for local processing (*Third Party Component Invoke*)
- Request Authorisation for a Transaction (*Request Reply*). The transaction is not automatically suspended pending the outcome of the request, but may decide to wait
- Print a receipt (*Output*)
- Commit the result of a Transaction to the Transaction Stack (*Finalise*). After this, the transaction is irrevocably committed

Chapter 6 describes the operation of the Counter dialogues

5.4.2.3.1 Asset Manager Interface

This component was introduced as part of the WebRiposte FT Framework to enable Temporal Reference Data to be accessed by applications. However, the NBCA will not utilise this interface, but will access Temporal Reference Data in the normal way.

5.4.2.3.2 Initialise

This function is invoked as part of the initialisation of the operation and is passed the impulse used to invoke the application.

5.4.2.3.3 Capture

The purpose of the Capture function is to execute a script that prompts the Clerk to provide the values for a set of Variables and ensure that the validation specified for those variables is successful.

5.4.2.3.4 Validate

The application can define validation functions to carry out specific validation on data that is being captured.

This will have a single input parameter, the Variable to be validated, and an output parameter indicating Success or Failure. In the case of failure, a Text string can be supplied describing the failure in terms meaningful to the Clerk.

5.4.2.3.5 Display

The *Display* function displays the current values of a set of variables together with some Buttons allowing the Clerk to control the logical flow of the transaction (i.e. whether it should continue or not).

5.4.2.3.6 Request Reply

This component is responsible for communicating with the Campus. It uses standard Riposte Priority Message functionality to ensure that the link to the Campus is opened.

Once a call has been made, the Counter application can continue to execute until it reaches a point where it is dependent upon the outcome of the *Request Reply* statement. The application then waits for the *Request Reply* statement to complete (or timeout) before continuing.

5.4.2.3.7 Output

The *Output* function outputs a document to a printer. The structure of the document is specified in Reference Data. The function assembles the document and substitutes the values of any variables defined in it, and then passes it through to the standard EPOSS Report processor for printing and communications with the Counter Clerk (to handle reprints etc).

5.4.2.3.8 Input

The *Input* function communicates with an input device (e.g. a PIN Pad or a future Customer operated Smart Card Reader). Details of information to be passed to the device and the variables into which returned data is to be stored are specified in the call.

5.4.2.3.9 Third Party

This component can be used for any additional processing required by the application logic.

5.4.2.3.10 Finalise

The Finalise component is responsible for writing the outcome of each Financial Transaction to the normal Retail Broker "transaction stack" as for any other Transaction, and is settled by EPOSS in the normal way. The final Transaction is not written to the Message Store until the Customer session is settled. [NBR182]

5.4.2.4 Retail Broker

This is the standard Retail Broker. It will be accessed using the normal COM interface.

5.4.2.5 NBS Additional Functions

These will all be written by Pathway and include:

- NBS Counter Recovery Application (see Section 5.4.3.4)
- Counter Call Scheduler (see Section 5.4.5.3)
- Reports, EoD etc. (see Section 5.4.4.1.7)

5.4.3 Application Components

The NBS Counter Application will coexist with the existing Counter applications and appear as part of another Counter service, alongside EPOSS, OBCS and APS. It will use the existing application user interface and conform to the Horizon Style Guide. It will take note of the evolving structure of the Escher Financial Transaction Framework, up to a point beyond which significant design changes can no longer be made within the Release 1 timescales, but will be implemented as VB applications rather than XML scripts.

Many aspects of the application will be driven by Reference Data. This provides a "soft" method for configuring the system, for example, where new account types and FIs can be added with minimal impact.

This Section also discusses other topics relevant to the use of NBCA, namely:

- Session Mobility
- Session Timeout
- Session Recovery

5.4.3.1 Host Components

The primary function of the Host Components is to define the integration of the NBS Transactions with EPOSS. This is provided by a number of COM Objects, developed by Pathway, to support the Host functions.

5.4.3.1.1 The Initialise Host Function

This function is invoked as a first step within the NBCA. It is passed details of the Impulse used to invoke the NBCA. This enables it to store information associated with the transaction obtained from the Impulse for use in other Host functions. It also needs to ensure that any data from previous invocations is cleared out.

Another function that the *Initialise* function needs to perform is to call the Retail Broker's *StartTransaction* method to ensure that transaction times are correctly recorded.

5.4.3.1.2 The RequestReply Host Function

This function implements the logic of the *RequestReply* call in the NBCA. It generates the appropriate [R1] message, based on data passed from the NBCA, sends it as a priority message to the Campus and waits for the corresponding [A3] to be returned.

Processing carried out in this function will include:

- Generating timestamps to enable measurement of SLAs
- Encryption of relevant parts of the message
- Message Signing
- Timeout handling
- Verification of the Signature on the [A3] received

5.4.3.1.3 The Output Host Function

This function implements the logic of the *Output* call in the NBCA.

It will be passed details of the receipt to be printed, together with a flag indicating if a bilingual receipt is required (this will be the case if the Outlet is considered to be in Wales). It will take the receipt and use the information within it to invoke the standard EPOSS Report process to handle the output to the printer. The EPOSS Report process will handle any printer failures and print preview that may be required. On completion, control will then be returned to the Framework. [NBR155]

5.4.3.1.4 The Input Host Function

This function implements the logic of the *Input* call in the NBCA.

It will be passed details of the data to be sent to the PIN Pad and a message to be displayed to the Counter Clerk. It will handle the communication with both the screen (to communicate with the clerk) and the PIN Pad. This includes ensuring that any message displayed to the clerk will be cancelled when the PIN Pad completes its operation, and the clerk has the ability to cancel the operation (for example should the customer leave without entering a PIN).

On completion, a return parameter is constructed passing data back to the NBCA as requested by the input parameter.

5.4.3.1.5 The Finalise Host Function

This function implements the logic of the *Finalise* call in the NBCA and causing the transaction to be written to the RetailBroker transaction stack.

Processing carried out in this hook will include:

- Message Signing
- Generation of timestamps for SLA purposes

5.4.3.2 Session Mobility

Session Mobility is a feature of the standard Riposte Desktop that allows a User (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.

It is clearly necessary to inhibit Session Mobility 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. Thus, session mobility is inhibited at the start of the NBS transaction and re-enabled at the end. [NBR070]

The end of the transaction is easy to define, in that this is the point in the logic of the *Finalise* Host function immediately after committing the Transaction to the Retail Broker stack.

Defining the start is less easy. To comply with the requirement as stated, it needs to be done as early as possible within the *Operation Launch* component. However, if there is a need to inhibit session mobility and re-enable it in the same Desktop application, then the *Initialise* Host function can be used to do so.

5.4.3.3 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 during the NBS transaction (as described above), then this has the side effect of inhibiting Session Timeout. The consequence of this is that an NBS Transaction cannot be timed out, however it is possible for a Customer Session with an NBS Transaction on the Transaction stack to be timed out. In this case, the Banking Transaction will already be complete. [NBR072]

5.4.3.4 NBS Counter Recovery Application

As discussed above, during normal operation every Transaction will have both an [R1] and a [C1] message in the Counter Message Store. Most will also have an [A], and some will have a [C0]. The only circumstances under which there can be an [R1] without a matching [C1] are as follows:

- The Counter was switched off (or failed) between the [R1] (or later [C0]) being written and the Customer session completing
- The Counter failed after the [C1] was written and before the [C1] was successfully replicated to another Message Store
- The Counter failed after the [C1] was written and the Message Store was recovered incorrectly, resulting in the [C1] being lost. Note that in this case it is also possible that an [R1] message is lost; however, such a situation is unlikely to be easily detected. Other actions are being put in place to minimise the likelihood of incorrect recovery, so this will not be discussed further
- Following a forced terminal logout (as described in Section 5.4.3.3)

In all cases apart from the last, 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.

Following such circumstances, it is necessary to detect that such a failure has occurred and to ensure that any missing [C1] messages are written to the Message Store to correctly reflect the actual outcome of the transactions. [NBR013, NBR035, NBR505]

In order to simplify the recovery process, information relating to the recovery status of each Counter will be held in a Persistent Object per Counter in the Message Store. This Recovery status is in two parts:

- Does the Counter definitely need recovery?
- Is the Counter currently “clean”?

The Counter status will be set to “unclean” whenever a Clerk logs on, and will be set to “clean” on a tidy logout. If at a Clerk logon the status is found to be “unclean” or recovery is required, then recovery will be carried out.

Additional logic is required to handle the special cases of session transfer and isolated Counters.

When recovery is required, it will usually be possible to carry out the recovery automatically based on a [Recov] message that is written to the message store as soon as the outcome of the transaction is confirmed. This point will be as soon as it is decided that the Transaction has failed or the Clerk has declined the Transaction, or in the case of Approved Transactions as soon as the Customer Receipt has been printed. This point is chosen since it is then easy to define the Counter processes to ensure that in a failure scenario the Clerk will complete the transaction once the Receipt has been successfully printed.

Therefore, the outcome of a transaction can be often be determined by the recovery process by the state of the data. Thus, where the [A] message shows a decline, the transaction must have been declined. If there is no [A] message, the transaction will have timed out. Of course, it may have timed out, even if the [A] is present.

Certain transactions have no financial effect. These will give rise to a zero value transaction, whatever the outcome, and can thus have an arbitrary result recorded. [NBR176]

For transactions with financial effect that were declined at the Counter, the [Recov] or [C0] message will be present, thus allowing a [C1] to be generated.

Thus, the only transactions which need manual intervention are those which were in progress when the system failed, or those where data has been irretrievably lost as a side effect of the failure without being replicated to another surviving Riposte node.

The table below shows whether the clerk is prompted. It also shows the possible results of recovery. It can be seen that the clerk will be prompted only for transactions where an authorisation was returned in the [A]. These will be successful transactions, where the failure occurred during receipt printing, or manual transcription of the receipt, or where the system failed before the clerk had opportunity to decline. They may also occur where the system has been replaced, and the data recovered through replication.

Transaction Effect	[A] Response Code	Prompt Clerk?	Clerk Response	Fields Affected and Transaction Return Code (RC)
Non-financial	Authorised (01)	N		[RC(01)/RC(07)]
Financial	Authorised (01)	Y	Accepted	RC(01)
			Failed	RC(07)
Either	Other (not 01)	N		RC(06)
Either	No [A]	N		RC(07)

Table 3 – Recovery Actions

Any [C] message that is written needs to be clearly identified as a "recovery" [C], however other than that it should be as similar as possible to a "normal" [C]. Part of the work on defining the content of [C] messages needs to take this into account. [NBR176]

Any Recovery messages will be written under the UserID whose logon prompted the recovery, however the original Clerk's UserID also needs to be included in the recovery message for audit purposes. Also, the recovery transaction should be associated with the original Stock Unit to ensure the Cash Account is balanced.

5.4.3.5 PIN Pad Driver

This is a key component of the Counter infrastructure. It will be developed by Pathway.

5.4.3.6 Training

Training Mode will not be supported for NBS, and no specific developments will be made to support NBS training on a classroom training system. However, work is required to ensure that existing training facilities continue to work following the introduction of NBS.

5.4.4 Impact on Existing Applications

There are a number of areas where the requirements for NBS impact on the facilities or behaviour of existing Horizon applications.

5.4.4.1 EPOSS

Changes may be required to EPOSS to meet the requirements of NBS.

5.4.4.1.1 Settlement of NBS Transactions

The *Finalise* of an NBS Transaction will result in an item being added to the Product Stack of the Desktop. The NBS item(s) will be placed on the stack along with other products, if there are other transactions carried out in the same serve Customer session. [NBR182. NBR254, NBR464]

Their values will automatically be reflected in the current Cash Account. [NBR017]

After one or more sale items (including NBS Items) have been selected and placed on the Product Stack, the user can initiate payment via the desktop *Finish* Button. Settlement is part of the current EPOSS Transaction Service and will remain responsible for the settlement of a Customer Session. It is concerned with the final settlement, validation and committal of the transaction stack including NBS Transactions.

The Settlement function checks the outstanding balance to determine whether a transaction session can be committed, and displays the Settlement menu for manual payments. The outstanding balance must reach zero for the current Customer Session.

There will be a significant impact on EPOSS Settlement if preconditions are placed on acceptable method of payments. For example, if only cash deposits for NBS are accepted, other methods of payment such as cheques must be prevented from being used for settlement of an NBS Deposit. EPOSS Settlement would therefore be required to check the preconditions and “bar” access to other methods of payment. This will be addressed by manual processes and will not be policed by EPOSS Settlement.

If this is the case, all transactions on the Product Stack are committed into the Message Store. Once the transactions are committed, the Product Stack is cleared for the next Customer Session.

5.4.4.1.2 Message Logging

A series of transaction messages are written to the Message Store following the settlement of a Customer Session. The message logging function must ensure that a unique Session Identifier is generated for every session transacted. NBS transactions on the stack can thus be committed to the message store with a Session Identifier that is unique across the Horizon estate.

The Transaction Message will be constructed by the *Finalise* function of the NBCA.

New attributes will be added to the structure of the *EPOSSTransaction* Message to accommodate the requirements for NBS Transactions.

Changes to the structure of the EPOSS Transaction Message will be documented as part of the high level design.

5.4.4.1.3 Session Receipt

A distinction needs to be made between two classes of Receipts.

- *Banking receipts*. These are the ones that form part of the actual transaction authorisation and are generated by the NBCA.
- *EPOSS Session receipts*. These contain a summary of all transactions in a session. This receipt needs to include a line detailing the NBS Transaction, which is treated like any other Transaction.

There is no impact on the Session Receipts currently generated by EPOSS and NBS Transactions will be printed using Product Reference Data that is supplied by PO Ltd. The data from the immediate Session is available and the reporting service may be utilised to print a receipt, if required, upon settlement.

The manually requested session receipt printing facility is currently from the end of one session to the start of the next. However, a reprint function for banking receipts is not available until the end of the Customer Session. It is only available as follows:

- The Office Receipt (used for signature verification) is available after the Clerk indicates that Signature Verification has not been possible, until such time as the Banking Transaction is added to the Stack
- The Customer Receipt is only available for reprint after the Transaction is added to the stack until the Customer Session has ended

After the customer Session has ended reprint (of session receipt) is part of the existing Horizon functionality.

Outlets which have the "Welsh Language" indicator set in the Outlet details Reference Data held in the message store, will automatically print Customer receipts in accordance with the Welsh/English Receipt format. Non-customer receipts are always in English. There is customisation of the Counter to cater for Welsh and English Post offices with language settings (in Reference Data). [NBR149]

5.4.4.1.4 The NBS Transaction Model

NBS Transactions will be treated in the same way as a Receipts and Payments Transaction. *Pensions & Allowances* (P&A) or GiroBank Transactions are examples of Receipts and Payments.

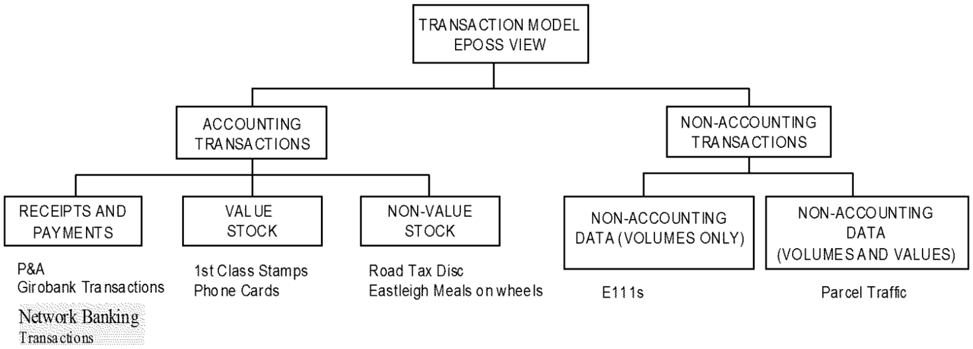

TRANSACTION MODEL EPOSS VIEW
ACCOUNTING TRANSACTIONS
NON-ACCOUNTING TRANSACTIONS
RECEIPTS AND PAYMENTS
VALUE STOCK
NON-VALUE STOCK
NON-ACCOUNTING DATA (VOLUMES ONLY)
NON-ACCOUNTING DATA (VOLUMES AND VALUES)
P&A
Girobank Transactions
Network Banking Transactions
1st Class Stamps
Phone Cards
Road Tax Disc
Eastleigh Meals on wheels
E111s
Parcel Traffic

Figure 11 – An Overview of the Counter Transaction Model

NBS Transactions will be treated as an accounting transaction, because the balance of cash in the Outlet is affected. Transaction values will be accounted for using the standard EPOSS Reporting and Accounting Hierarchy. The receipt of cash through NBS transactions is a credit transaction that increases capital (cash). Payments through NBS Transactions are debit transactions that decrease capital (cash). [NBR018, NBR159, NBR464]

A Balance Enquiry will produce an item on the stack and will be treated by EPOSS as a transaction of zero value. However, in order to support the Cash Account, it will still require a Primary Mapping.

EPOSS balancing will not be affected, as the EPOSS Reporting and Accounting Hierarchy will be used to account for all NBS Transactions involving Cash Deposits and Withdrawals. This will be carried out by the Primary Mappings (*EPOSSNodes*) and it is assumed that additional Reference Data (any new *EPOSSNodes*) will be supplied by PO Ltd through the OBC Process (see [OBC]).

5.4.4.1.5 Reporting Service for NBS

Each Counter is equipped with a combined slip and receipt printer. In addition, each Outlet also has a "Back Office" Printer.

The Reporting Service is part of EPOSS. It is used to print Tokens, Session Receipts, Reports, the Cash Account and Event Logs. The reports include the Counter Daily, Counter Weekly, Office Daily and Office Weekly reports.

Some printed output for NBS is handled by the NBCA and does not impact EPOSS. These include:

- Office Receipts - printed slips with signature "boxes" that are printed for the Customer to sign when making a Cash Withdrawal and are retained in the Outlet
- Signature Receipts – printed slips with signature boxes that are signed by the Customer when making a Balance Enquiry, and are not retained in the Outlet

Receipts relate to a session and provide information on the transactional data relating to each product transacted in the session, along with additional information such as Time and date, Office, Stock Unit. They are generally available through Button(s) on the screen or keyboard or automatically as specified by Reference Data.

5.4.4.1.6 Cash Account

The production of the Cash Account is part of the Office Roll-over process. There is no impact on the current Outlet Roll-over process. The production of the Cash Account is supported within the architecture of EPOSS Counter applications reporting process. No new tables are required and NBS Transactions are mapped to the appropriate Cash Account line as defined by PO Ltd Reference Data. [NBR258, NBR454]

Changes will be required to the layout of the Cash Account through the OBC Process and this will require additional lines to be created in the existing Cash Account.

Any changes to the Cash Account are supplied as PO Ltd Reference Data and are required significantly in advance of March 2002, which is the start of the 2002-2003 financial year.

> *No such changes have been included. However, there are sufficient "blank lines" within the 2002-2003 Cash Account report to allow NBS transactions to be added later through a Reference Data change.*

5.4.4.1.7 NBS Reports

Six new Output reports are required on demand through the Desktop. These will be catered for by the EPOSS application product using the standard Message Store transaction data. Changes to the existing Counter PPD will be required. The new report layouts are to be specified, designed and incorporated into EPOSS. The new reports will require the provision of Reference Data in the form of additional *EPOSSDNodes*, which are currently provided through the OBC Process.

The reports are:

- Cash Deposit Transaction Listing by Bank (Counter Daily Report)
- Cash Withdrawal Transaction Listing by Bank (Counter Daily Report)
- Balance Enquiry Transaction Listing by Bank (Counter Daily Report)
- Office Daily Network Banking Cash Deposits
- Office Daily Network Banking Cash Withdrawals
- Office Daily Network Banking Balance Enquiries

These are formally defined in [CNTRDLG].

5.4.4.1.1.1 Transaction Log

The Transaction Log will not require additional Counter User-specified Report Criteria. Queries for NBS Transactions will be provided through the existing criteria.

5.4.4.2 Impact on APS

One of the Requirements on NBS is the support of POCA “Card Receipt” in the Outlet. This will be handled as an APS Transaction at the Counter, with no changes required to the APS Counter application. This supposes that PO Ltd provide the necessary Reference data to identify the barcode used on the envelope containing the Card and map it to an appropriate EPOSS Product.

Similarly, no changes are required to the APS Harvester.

However, a new APS Client will be required to enable such transactions to be routed through to the POCA Bank. Such a Client can be introduced in the same way as any other APS Client.

The use of APS Emergency Payments may also be affected since they use Riposte Priority messages.

The way in which these call the Riposte APIs to send Priority messages need to be reviewed (and perhaps changed) to ensure that these functions and NBS Transactions don’t interfere with each other.

Lastly, there is a change required to APS to reduce the load on the Correspondence Servers. This is necessary so that Counter message recovery can be supported without the need to upgrade the Correspondence Server hardware.

Currently, whenever APS prints a receipt, it writes two Riposte messages to the Message Store. The first one indicates the start, and the second the completion of printing. APS prints two receipts for each transaction, and hence writes four messages per transaction. However, it calls an EPOSS function to actually print the receipt, and this function generates its own messages for audit purposes. The APS messages are thus redundant and can be removed. They account today for around 25% of the total message load in the peak period.

The EPOSS Reports function needs to be changed to make the logging of these audit messages dependent upon the caller and APS needs to be changed to suppress this audit logging.

5.4.4.3 Impact on OBCS

There is no impact on the functionality of the OBCS Counter application. However, OBCS Foreign enquiries are one of the few existing applications that use Riposte Priority messages. The way in which they call the Riposte interfaces to send Priority messages need to be reviewed.

5.4.4.4 Counter Reconciliation

APS and EPOSS provide reconciliation totals for each day's transactions as part of the end of day processing. EPOSS also provides reconciliation totals to enable the Cash Account to be correlated each week. Insofar as NBS Transactions are "normal" EPOSS transactions, that is all the end of day processing that it is required of them.

5.4.5 Impact on Existing Counter Infrastructure

5.4.5.1 Crypto API Libraries

These will be enhanced to provide new APIs to support PIN Block handling (in particular PIN Pad key management and PIN Block translation in the Agent layer).

5.4.5.2 Smart Card Ping

The way in which Smart Card Ping calls the Riposte interfaces to send Priority messages needs to be reviewed (and perhaps changed), so as to ensure that different Counters in the same Outlet executing this function and NBS Transactions don't interfere with each other.

5.4.5.3 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 continues to force 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. [NBR021]

It will be enhanced for NBS in a number of ways.

- It will register an interest with the *Counter Network Infrastructure Management service* (CNIM; see Section 10.4) to enable it to be notified of changes to the state of the network connection
- It will ensure that the Riposte connection stays open as required
- It will maintain a *Network Status Object* within the Outlet which enables the Counter Applications to check the status of the connection from the Outlet to the Campus
- It will provide interfaces to allow the *Online Status* of the Counter to be returned to Counter applications

Details are given in [SDSAPP]

5.4.1.4 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.

The existing functionality is unchanged. However, this component also needs to maintain the *Off-Line Indicator* on the desktop, which provides a visual indication to the Clerk as to whether or not the Network is currently available. The Off-line 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 *Network Status Object* (described in section 5.4.5.3) indicates that the network is unavailable.

Each time the EPOSS Watchdog is invoked it should check the Status, and if necessary change the visibility, of the Off-line Indicator. [NBR236]

5.5 NETWORK

The principal impact on the Network is the move from a largely asynchronous ISDN connection rate, to largely synchronous connections occurring whenever an NBS transaction takes place in the Outlet. The consequences of this are covered in Chapter 15 (for its sizing implications) and Chapter 10 (for the impact on the nature of the ISDN network).

5.6 CORRESPONDENCE LAYER

This layer provides the message distribution processes. It runs the *Riposte Message Service* (RMS) on a number of high-powered Compaq servers. At BI2, the Message Server is replaced by *WebRiposte Message Service* (WRMS). This is not visible to the application.

All Riposte messages are generated with an expiry period, which determines how long they stay in the Message Store. This can vary depending on the message type. Most messages expire after 35 days. They are kept for that long to permit Cash Account balancing. The expiry period used for new application types can have a profound impact on the amount of data held within the Message Store.

Extending the size of the Message Store is straightforward[34] and has little impact on the performance of Riposte. However, increasing the number of Persistent Objects or WebRiposte Objects has an impact on the size of the Persistent Object index, which could affect performance.

5.7 APPLICATION AGENT LAYER

A number of new Agents are required for NBS. Changes are required to some of the existing Agents.

[34] *Though not cheap*

The new Agents are as follows.

- Real-time *NBS Authorisation Agent* to handle [R]s and [A]s
- Real-time *NBS Expedited Confirmation Agent* to handle [C0]s
- *NBS Confirmation Harvester Agent* to load [C12]s into the DRS

Processing of the bulk file returned by the NBE is covered in Section 5.8.

Existing Agents that require changes include the following.

- TPS Bulk Harvester (this is covered in Section 5.10.3)

A new Agent resilience model is also required, to enable Agent processes to be restarted (or brought into use) very quickly following the loss of an Agent.

5.7.1 Interface to the NBE

5.7.1.1 Real-Time Interfaces

A real-time interface is required between an Agent in the Horizon architecture, and the NBE. This is used by the Agent to:

- Transmit [R]s and [C2]s to the NBE
- Read [A]s from the NBE and return them to the counter by writing them to the WebRiposte Message Store.

Initial versions of this document described the use of IBM's MQSeries messaging software to support this interface. Following acceptance of NB CR026, this interface paradigm has been replaced by the use of a direct TCP/IP connection accessed (at the Horizon end) via a WinSock interface. See [NBETIS].

The NBE will run a series of partitions, each supporting the same IP address and a different TCP/IP port number. Each Horizon Agent instance that communicates with the NBE will connect to this IP address using a specific set of port numbers. Thus, all messages related to a given NBS transaction can be routed by the Agents to the required NBE partition.

Having a single partition per Riposte Cluster doesn't enable the NBE to spread the workload sufficiently, so a value will be generated for each Transaction at the Counter (*AgentHash*) to enable the workload to be split. This value will be generated using a hashing technique based on the FAD code, which is already used to randomise connections across the estate and has proved to be effective. Thus, there will be a separate NBE Partition for each Cluster/AgentHash value combination. Initially there will be four AgentHash values generated at the Counter and four Riposte Clusters, which implies 16 NBE partitions.

This is an important consideration because of the way in which the NBE handles [C2] messages. Each partition maintains a cache of recent [R] messages, with their outcome (i.e. the [A] sent back to Horizon). The cache holds about ten to fifteen minutes worth of transactions (at peak transaction rates, thus significantly more at other times). If a [C2] is received by the same partition while the original message is still in the cache, the NBE can generate a Reversal (an [E1] message) to the customer's FI, and thus release immediately any funds that may have been transferred by the [A]. If the [C2] arrives after the transaction is cleared from the cache, it will require manual reversal.

In consequence, the [C0] message will be generated by the Counter as soon as it is known that the transaction is being abandoned, rather than waiting for the end of the customer session. The ISDN line will be kept open for a few seconds following receipt of the [A], so that if a [C0] is generated it is reasonable to expect that it will be sent to the Campus immediately. There is thus a reasonable expectation that it will reach the NBE while the transaction is still in the cache.

An implication of this approach is that there is a need to co-ordinate the number of NBE partitions with the number of instances of the relevant Horizon Agents.

Other message types ([PS], [PR], [KT] and [KA]) operate in a similar manner to [R2] and [A2] messages.

5.7.1.2 Batch Interfaces

In contrast to the real-time interface used for [R], [A] and [C2] messages, the NBE will transmit [C4] and [D] messages to Horizon in a set of batch files.

The NBE will use FTP to transfer files to a remote FTMS Gateway Server (*NBE Gateway Server – Remote*) located at the NBE site (or its Disaster Recovery standby site). The standard Horizon FTMS service will then be used to transfer files to and from a *NBE Gateway Server – Local* located in the Campuses. Files are then transferred to and from the Host Central Server using conventional NFS techniques. This is covered in Section 5.8.

5.7.2 NBS Authorisation Agent

This Agent runs on the *NBS Agent Server*, a new platform introduced for NBS (see Section 11.4.1). It is responsible for handling all [R1] messages from the Counter and the corresponding [A2] messages returned from the NBE. The same Agent handles both types of message as this enables simple monitoring of the NBE response times and provides the ability to timeout late responses without the need for clock synchronisation.

There will be at least one NBS Authorisation Agent per Correspondence Server Cluster. Its primary function is to take the incoming [R1] and perform the following functions.

- Validate it (including the Digital Signature)
- Reformat it as a [R2] (including any decryption and re-encryption of data)
- Add a *Message Authentication Code* (MAC)
- Pass it through to the NBE

It then needs to pick up any [A2]s returned from the NBE and perform the following functions.

- Validate it (including the MAC)
- Reformat it as an [A3] (including adding SLA and audit data)
- Add a Digital Signature
- Pass it back to the originating Counter

In addition, it will provide a timeout mechanism to ensure that should the NBE not return an Authorisation in time, the *NBS Authorisation Agent* should generate an [A3] indicating that the NBE is unavailable. This is necessary in order to ensure that such delayed NBE messages are not recorded as network failures against Pathway's SLAs.

Similarly, an appropriate [A3] message should be returned for any [R1] message that fails during processing (for example in signature checking).

The Agent will add timing information to the message for later SLA calculation purposes.

5.7.3 NBS Expedited Confirmation Agent

This Agent also runs on the *NBS Agent Server*. It is responsible for handling all [C0] messages from the Counter.

There will be one NBS Expedited Confirmation Agent instance per AgentHash value per Correspondence Server Cluster. Its primary function is to take the incoming [C0] and perform the following functions:

- Validate it (including the Digital Signature)
- Reformat it as a [C2]
- Add a MAC
- Pass it through to the NBE

5.7.4 NBS Confirmation Harvester Agent

The purpose of this Agent is to harvest the [C1] messages as they are received from the Outlets and to pass them to the DRS. It runs on the *Generic Agent Server* platform (see Section 11.5.5).

NBS will use continual interactive harvesting (i.e. using a checkpointed message port). This technique is currently used for the LFS harvester and has the ability for doing bulk inserts into Oracle and co-ordinating checkpoints with Oracle commit units. It would normally be expected that there would be multiple Oracle commit units for a single Riposte checkpoint, which can result in duplicate [C]s being inserted into Oracle in a recovery situation. This situation needs to be allowed for as a normal occurrence. [NBR180]

5.8 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 translate a file-based view of their information into discrete transactions or "messages".

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.

Host systems also implement any Settlement and Reconciliation made necessary by their own Business Rules. Thus, within NBS, the DRS runs at the Host Layer and is implemented on the Host Central Servers. The DRS is described in Chapter 9.

Host Layer systems also communicate at a batch level with any external systems. A particular example of this is the handling of the EoD file passed from the NBE to Horizon each day for reconciliation. This is described below.

5.8.1 Processing the EOD File from the NBE

5.8.1.1 File generation by the NBE

As part of its End of Day Processing, the NBE will generate a number of files containing [C4] and [D] messages. Each file will be converted to XML format, and sealed using the NBE/DRS MAC key. The resultant MAC of each file, together with details of the file name and creation time, will be included in a Control File which will also have a MAC calculated for it.

Once all files have been MACed, a header will be added to the control file detailing the number of records contained in the file. This control record will include a MAC for the record.

5.8.1.2 File Transmission to Horizon

The files will be copied by the NBE, using FTP, to a *NBS Gateway Server* - *Remote* at the same site as the NBE. FTMS software running on that server will detect the arrival of the files, and will copy them to the *NBS Gateway Server – Local* at either Bootle or Wigan. The destination on the local FTMS server will be an NFS mounted disk on the Dynix host. The DRS Host filestore will be located on resilient EMC disk filestore.

5.8.1.3 File Integrity Checking

Once the files are secured on the DRS, the Maestro scheduler will run an *EoD File MAC Checker* process on the local FTMS gateway. This process requires hardware crypto support, and hence the *NBE Gateway Server – Local* platform will be provided with both an HSM card and the standard Crypto libraries and their supporting software, including Key distribution software. (Neither the HSM, nor the Crypto libraries that drive it, are available on the Dynix platform.)

The following checks will be carried out by the *EoD File MAC Checker* process. It will access the files held on the Host Central Server, via the NFS share, rather than any copies still held on the FTMS gateway server itself. This ensures that any corruption introduced between the FTMS gateway and the Host Central Server is detected.

- The MAC for each record of the control file is checked
- Each record in the control file is checked to be within start/end dates in the control file header
- The number of records in the control file matches the number of records stated in the control file header
- For each Data File referenced by the Control File:
    - The MAC for the file matches the value stored within the control file
    - The record/byte count held in the control file matches the number in the file itself

If any file does not pass these checks, an alert will be raised. This alert will cause operations staff to be called in to resolve the problem manually.

5.8.1.4 Database Load

Assuming the file passes the above checks, DRS supplied routines will load the data into the DRS database.

5.9 REFERENCE DATA MANAGEMENT SERVICE (RDMS)

Reference Data is used to configure many aspects of the Counter behaviour. In addition, many of the new Counter components introduced to support NBS are themselves implemented as Reference Data. Changes are required to Pathway's existing Reference Data handling mechanisms to support this. These changes, and the use of the resulting Reference Data, are described in Chapter 8.

5.10 TRANSACTION PROCESSING SYSTEM (TPS)

5.10.1 Overview

The main structure of the TPS Host Application is unchanged by the introduction of NBS. However, a few areas are affected as follows.

- A new interface table from the TPS Harvester containing [C11] NBS messages
- An enhanced data flow to the Data Warehouse, containing details of the NBS transactions to enable the MIS to calculate the necessary SLAs
- A new data flow to the DRS to pass on the [C112] messages and details of closed Cash Accounts

The interface to TIP will not change. [NBR511]

5.10.2 TPS Harvester

If no change were made to the TPS Bulk Harvester, then all [C1]s would be harvested as normal *EPOSSTransaction*s, which is probably sufficient to meet the TIP requirements. However there are additional data fields in the [C1] messages that are required by the Data Warehouse and the DRS. Therefore the TPS Harvester needs to be enhanced to handle the [C1] messages as an additional data stream and harvest the contents into a new interface table within the TPS Host.

5.10.3 TPS Host System

The TPS Host system will need to be enhanced as follows to process the new interface table from the TPS Harvester, containing [C11] NBS messages.

- As far as TIP production and Reconciliation checks are concerned its contents should be treated like standard EPOSS Transactions
- Its contents should be passed to the Data Warehouse as an enhanced data flow, to enable the MIS to calculate the necessary SLAs
- Its contents should be passed to the DRS as a new data flow to pass on the [C112] messages and details of closed Cash Accounts

5.10.4 TPS Host Database

This is an existing Oracle database running on the Sequent Host system. It will need to be enhanced to support the changed functionality described above. The major change is in the workload supported.

5.11 MANAGEMENT INFORMATION SERVICE (MIS)

Pathway's *Data Warehouse* (DW) will be used to provide all Management Information reports required by NBS. These are characterised by the use to which they are put and the timeliness in which they need to be produced. A management information report is used to inform strategic decision making rather than day-to-day operational decisions. Usually the reports are produced some time after the fact and report on events that took place over a period of days, weeks and months, or even years, rather than hours.

5.11.1 Requirements

The set of NBS reports to be produced by the MIS is documented in [NBSMIS].

~~Note that the set of NBS reports to be produced by the MIS is still under contractual discussion. The current position is listed in [CAN05]. [NBSMIS] will be updated in due course from that contract schedule, and this document will in due course reflect the changes to [NBSMIS].~~

~~*[NBSMIS] appears to have a much smaller set of reports. Rather than update this section to reflect the changes, the reader is directed to [NBSMIS].*~~

5.12 EXTERNAL INTERFACE LAYER

5.12.1 General

Standardised facilities are provided to transfer transaction information to and from PO Ltd and its Clients. In most cases, this information is passed as "flat files", and 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. Horizon's usual modus operandi is to install an External Interface Gateway within the Client's premises, and pass data between that and the Campuses using FTMS.

5.12.2 TIP Interface

This is the existing data flow to the TIP database operated by PO Ltd and documented in [TIPAIS]. It should not require any change for NBS as the additional transactions generated will conform to the current EPOSS data model and will use the existing Serve Customer (SC) mode. [NBR455]

There may be an issue if additional events are required by new applications, depending on how they are dealt with by TIP.

5.12.3 PO Ltd Reference Data System

This is the existing data flow from the PO Ltd RDS. There are some enhancements to the data carried over this interface, as discussed in Chapter 8.

5.13 EXTERNAL CLIENT SYSTEMS

These are not part of the Pathway system but are potentially impacted by the introduction of NBS.

5.1.1 NBE

This is discussed extensively elsewhere.

5.1.2 PO Ltd TIP System

This will need updating to handle NBS transactions.

5.1.3 MIS & Financial Reporting

The processes that Pathway has in place to report on transaction volumes, Service Level Agreements and so on, will need to be augmented to include the NBS transactions.

Chapter 6 - User Interface

6.1 General

This Chapter defines the principles that affect the dialogues conducted with users, and shows how these dialogues make use of the styles defined in the Style Guide. The Counter dialogues will be defined in [CNTRDLG], which is being developed in conjunction with PO Ltd and takes precedence over any details listed in this Document.

6.2 Summary of Requirements

The NBS Counter application must use the existing application user interface and shall conform to the Horizon Style Guide ([STYLE]) (which will be enhanced to reflect the use of PIN Pads). [NBR448, NBR493]

The existing Horizon System is compliant with [STYLE], and any extensions to the HCI for NBS should be in accordance with the principles of that style guide. It will be necessary to revise [STYLE] to reflect the use of PIN Pads. [NBR028, NBR159]

The input of NBS transaction data by the Counter Clerk will be supported by use of the touch screen and the keyboard. At appropriate points in the dialogue, the system may provide prompts for the Clerk to instigate activities such as obtaining a signature or input of a PIN via a PIN Pad. [NBR438, NBR439]

The installation of PIN Pads is outside the scope of this SDS, though the development of the software needed to support PIN Pads is included. [NBR066]

6.3 Dialogue Design

The basic functions to be provided by NBS are listed in Section 3.3.4. This Section discusses the principles of the desktop service that will encapsulate the interface by which these transactions are presented to the Counter Clerk.

The Horizon Desktop Service provides the "front end" through which the Counter Clerk accesses the business functions on the Counter. It provides log-on facilities, and enables the user to navigate around the menu hierarchy. NBS is included in the "Serve Customer" part of the Desktop Service, and hence is available without any further need for user authentication. [NBR449]

NBS is invoked when the Clerk swipes a magnetic card for which the IIN falls into the range associated (by Reference Data) with NBS, or chooses the appropriate menu Button on the Desktop.

A Customer session comprises the range of activities that a Counter Clerk dealing with a Customer at the Counter normally carries out from the start of the first Transaction through to completion of the last Transaction and settlement of the session. This is more fully defined in [GENAPI]. Multiple NBS Transactions (using the same or a different token) may be carried out within a Customer session. [NBR329]

However, each NBS Transaction is separate, such that if a Customer wishes to make a deposit and a withdrawal, this would be via two transactions with no system relationship between them. [NBR151]

6.3.1 Desktop Presentation

The Desktop Presentation presents to the Counter Clerk the appropriate Desktop Panels, Menus and Pick Up Lists, and encompasses the Desktop Controls such as *Bin*, *Receipt* and *Quantity*. It displays a hierarchy of menus including those for NBS. It then controls the sequence of menus, dialogs and data capture screens for NBS. It encapsulates the "business process" of the Outlet, i.e. the sequence of activities that the Counter Clerk performs through the Desktop. These facilities will be extended to encompass NBS. [NBR450]

The screen dialogues will follow the standard Horizon style of icons and navigation as set out in [STYLE], with the standard context sensitive help facility. [NBR028, NBR159]

Pathway notes the requirement that existing front-end processes are to be reviewed, modified if required and the PPDs updated, in order to support the NBS functionality. [NBR463]

The NBS Service is invoked under *Serve Customer* mode. During the NBS transaction session, Desktop Presentation encapsulates the rules that govern whether the user can return to the home menu, a previous menu or suspend the current session and start another session. The user can also abandon the transaction and cancel or change the details of one or more transactions on the Product Stack.

The Counter system will support the capability for printing receipts in English and Welsh. This will extend to boilerplate information and to response messages generated from response code supplied by the NBE. In both cases, the text to be printed will be provided as Reference Data by PO Ltd. Free text information provided in responses from the NBE will not be translated by Horizon. [NBR149]

All Counter transactions are conducted under a common Access Control regime. Once the Clerk has logged on to the Horizon system, with their UserID and password, it is not necessary to log on again to use NBS transactions.

6.3.2 Transaction Handling at the Counter

NBS transaction types are listed in Table 2 in Chapter 3.

6.3.2.1 Data Capture

Each transaction is initiated at the Counter by presentation of a magnetic stripe Token (or by manual entry of the same) within *Serve Customer* mode. The Token must conform to the existing standards supported by Horizon ([ISO 7810], [ISO 7811], [ISO 7812] and [ISO 7813]), i.e. must be a standard plastic magnetic stripe debit card. [NBR001, NBR394, NBR395, NBR396, NBR397, NBR501]

Supported cards, and their issuers, will be identified by PO Ltd Reference Data. This will also indicate the transactions permitted on that IIN or IIN range. This allows PO Ltd to map Universal Bank transactions as required. [NBR006, NBR403, NBR429, NBR431]

Where manual entry is required, and is permitted by the card scheme as defined by Reference Data, the Clerk must enter first the PAN, then other card details as determined by PO Ltd Reference Data (normally that embossed on the front of the card e.g. PAN, Date Valid from, and Expiry Date). [NBR164, NBR401, NBR404, NBR486]

Different cards may require different fields to be entered, and it may not be permitted to enter details manually for certain card types. Once the manual entry is complete, the transaction flow is the same as for a successfully swiped card, although the system must record that the entry was manual rather than automatic.

The system now presents a selection of the transactions available. The Clerk selects the transaction type required and enters the appropriate financial amount (cash deposit and cash withdrawals only). [NBR451]

The NBS will only support single account Tokens (including multiple account cards which automatically default to a single account in the absence of any further instruction).

The cash withdrawal options are to be available to all Customers using NBS. Transactions are verified by either Signature or PIN as described below.

PIN based transactions are wholly separate from the corresponding signature-based transactions because of the different dialogue structures, and will be developed separately. If PIN verification is required, and the PIN Pad is unavailable, the Clerk should either move to another Counter position or decline the transaction. [NBR488]

The NBS transactions supported are all On-Line (except for Recovery and Receipt of Card at Outlet).

Note that there are no restrictions on the use of the same card several times within the same Customer session. [NBR019]

The Recovery of NBS Transactions process is described in Section 5.4.3.4.

Note that Smart Card tokens are not supported by the developments described in this Document, though their future support is not constrained. [NBR063]

6.3.2.2 Identification and Authentication of Token

Details of the Token are parsed and validated against rules set out in local Reference Data, identified by IIN and the Token is either rejected or accepted for subsequent processing. This validation will include the following checks. [NBR033, NBR405]

- The IIN is supported
- "From date" is valid (if applicable)
- "Expiry date" is valid (if applicable)
- LUHN on PAN is valid
- "Issue number" provided if required
- *Longitudinal Redundancy Check* (LRC) digit is valid

The System will prompt the Clerk to advise the Customer if the card is rejected. [NBR007, NBR164]

6.3.2.3 Transaction Processing

Details of the required Transaction are checked against Business Rules held in local Reference Data against each product, for minimum, maximum, multiple amounts, (subject to being supported by locally held Reference Data). [NBR240, NBR168]

Note that the multiple and minimum transaction limits will not be enforced for 'Withdrawal of Entire Balance With Balance Report' transactions. If this rule is only to apply to the POCA cards, then this must be enforced via the PO Ltd Reference Data supplied to Pathway defining which transactions can be supported (identified by IIN). [NBR166, NBR430]

Following successful validation of the card, the Clerk will be prompted to perform various APACS 40 standard checks. If any of these checks fail, PPDs will instruct the Clerk as to the steps to be taken. These are likely to include declining the Transaction and retaining the card. A receipt will be generated if a transaction is declined at this point, but will not indicate that the card has been retained. [NBR014, NBR161, NBR337]

6.3.2.4 Identity and Verification Check of Customer

If appropriate, the Clerk will verify the Customer's right to use the card, either by comparing the Customer's signature with that on the card, or by the Customer using a PIN Pad, depending on the transaction type selected by the Clerk, and the IIN. The verification to be undertaken will be indicated by Reference Data for that IIN and transaction type. It may indicate that verification by signature is acceptable if there is not, and has never been[35], a PIN Pad installed and available for use at that Counter. Fallback to signature verification will not be permitted in any other circumstance. [NBR250, NBR406]

There is no support for extended verification procedures, whereby an On-line interaction with the FI brings up additional, Customer specific questions to verify the Customer.

6.3.2.4.1 Magnetic Stripe Card with Signature

In the absence of a PIN Pad, and where permitted by Reference Data, the Clerk obtains a specimen signature from the Customer and compares it with that on the card. The Clerk must acknowledge that this has been successful on the system (e.g. by a check box) before the transaction can proceed.

If the signature does not match, then the system will display a message that could, for example, ask the Counter clerk to do one of the following, depending upon the FI requirements (this is to be set out in PO Ltd Reference Data, identified by IIN). [NBR251]

- Obtain a second signature from the Customer on a second Office Receipt
- Decline the Transaction and retain the card
- Decline the Transaction and return the card to the Customer [NBR008]

[35] *This avoids the risk of fraud by unplugging or otherwise disabling the PIN Pad.*

This signature verification check is carried out at the end of the Transaction, after the [A] has been received from the FI. The result of this signature verification will be recorded in the [C]. [NBR173]

Note that if different logic paths are required for different FI requirements, then these need to be represented as different Transaction logic types – it is not something that can be controlled purely through the text of Reference Data messages.

6.3.2.4.2 Magnetic Swipe Card with PIN

Functionality to support the selected PIN Pad (Hypercom HFT117; see [PPSPEC]) is to be developed, tested and ready for implementation at the Counters, along with the ability to disable this functionality.

PIN Pads will be installed in Outlets in a "phased rollout". The PIN Pad will be situated on the Customer side of the Counter. A different Counter dialogue will be developed to support verification using PIN Pads. Signatures will not be required on PIN Pad Transactions, and thus different receipt formats will be used. Verification takes place at the start of the dialogue, before the [R] is generated, as the PIN Block is contained in this message.

Any decision as to whether the verification process used depends on the physical presence and availability of a PIN Pad must also be taken at the start of the transaction (i.e. affect the Impulse handling), as different dialogue flows will be required.

6.3.2.5 Transaction Request and Authorisation

If validation is successful, and the link to the Campus is available, the Counter application will generate an On-line [R] to the FI as a priority message. (If the link is not available, the "Off-Line Indicator" will be displayed on all Counters in the Outlet. The application displays an appropriate message, the transaction is terminated, and the Clerk informs the Customer that the transaction cannot be processed at this time. No [R] is generated and no record of the attempted transaction is recorded.) [NBR009, NBR038]

Details of the Customer's bankcard are transmitted along with the stipulated amount, and the Counter waits for the result of the request. The Clerk will be asked to undertake the APACS checks while awaiting the response. The resulting [A] may be an authorisation for the transaction, which will result in its completion, or a decline, or an inferred decline initiated by a timeout from the NBE or Horizon Campus. In the latter case, the Clerk will refer to the relevant PPD to determine how to proceed. [NBR020]

For the transaction to proceed, a positive authorisation is required from both the FI and the Clerk. [NBR010]

There is no local override facility for a Decline response on the [A]. The Authorisation must be either for the same amount as requested or zero, except in the case of a Request for a Cash Withdrawal of Entire Balance With Balance Report. [NBR156]

The Counter application will wait for up to a *Maximum System Wait Period* (MSWP) before abandoning the transaction. This global wait period is configurable by local Reference Data, with Pathway's agreement, and prevents the Counter sitting idle if the [A] is not received within an acceptable time. [NBR221]

The outcome is written to the EPOSS stack. Every Transaction will be identifiable to an individual Counter Clerk and stock unit. [NBR182, NBR239]

6.3.2.6 Cash Withdrawal of Entire Balance With Balance Report ("Withdraw Limit")

For these special transactions, the amount of the Withdrawal is returned by the NBE along with the remaining outstanding balance, limiting the amount of the Withdrawal to the maximum permitted amount. This maximum cannot be over-ridden locally. [NBR430]

6.3.2.7 Declined Transactions

The Counter application allows the Clerk to decline the transaction once it has commenced in accordance with standard Counter procedures (e.g. in suspicious circumstances). If this occurs before the [R] is generated, there is no record of the attempted transaction. [NBR008]

In this case, or if the [A] is a Decline, or if the Clerk declines the transaction, then an appropriate message is displayed and a zero-value [C] is written including the reason for the Decline. [NBR010, NBR263]

In all these cases, the system will produce a receipt, which the Clerk gives to the Customer. The reason for the decline is printed on the receipt. In the case of an attempted cash deposit, the Clerk returns the cash along with the receipt. The application will present the Clerk with a message requesting acknowledgement that the monies have been returned.

6.3.2.8 Abandoned, Voided and Contra Transactions

An *Abandoned* transaction is one that is cancelled by the Counter Clerk prior to the issue of the [R1] message. No record of such transactions is kept by the system. [NBR167]

Any NBS transaction may be so abandoned. However, once the [R1] is issued, the transaction must complete or be voided by the Clerk and an appropriate zero-value [C1] generated. The Clerk will be prompted to invalidate any receipts printed. [NBR263]

A *Voided* Transaction is one that is cancelled by the Clerk (for example at the Customer's request) at any point where the Clerk can *Decline* the transaction. Such voided transactions are added to the EPOSS stack as a zero-value item and will contain the appropriate result code. (If the voiding occurs before receipt of the [A3], the [A3] is ignored.) The application will prompt the Clerk to manually invalidate any receipts that may have been printed. [NBR480]

Pathway notes the requirement that the system shall allow transactions to be voided according to rules set within PO Ltd Reference Data, but is unaware of any such rules. [NBR458]

6.3.2.9 Printing of Signature Receipt

Counter receipts are generic across all FIs and are documented in [CNTRDLG]. The layout is governed by Reference Data. Part of the content of the receipt is taken from the [A3]. [NBR029, NBR030, NBR032]

Note that the transaction time is heavily influenced by the amount of data printed on a receipt. [NBR447]

Normally, only a single receipt is produced for an NBS Transaction. This is a Customer Receipt. It is printed on the Counter's Tally Roll printer. It may be printed in English or, for Outlets defined by POL Reference Data as being in Wales, in English and Welsh. FI-provided data may be printed within prescribed formats. [NBR149, NBR238]

For transactions authorised by signature, an additional Office Receipt is required. This is again printed on the Counter's Tally Roll printer. The Counter Clerk will obtain the customer's signature in a "signature box" on the Office Receipt for all transactions authorised by signature. The Clerk must verify that the Customer's signature is correct. The Customer Receipt is printed for the customer only after the transaction is completed. [NBR030, NBR540]

In the case of Balance enquiries authorised by signature, the Office receipt is a slip containing a subset of the card fields, that the Clerk passes to the Customer to sign. This slip is not retained at the Outlet. [NBR237]

The contents of other Outlet and Customer receipts will contain much of the same information, but will differ in detail. In summary, they will contain:

- A main heading (e.g. Post Office Ltd.) followed by the address of the Outlet [NBR539]
- Title (e.g. Cash Withdrawal, Cash Deposit, Refund the Cash Withdrawal, Refund the Cash Deposit) or similar
- FI name (from Reference Data)
- PAN (At least five digits will be masked by an asterisk for security purposes, e.g. 4929 1234 **** *567 8901) [NBR539]
- Expiry Date of card, Issue Number (if applicable)
- Whether swiped or manually keyed
- Value of transaction (GBP)
- FAD code, Stock Unit (Office Receipt only)
- Date and time of Transaction (local time to be printed in hh:mm:ss format). The date-time stamp will be carried through any dialogue with the FI on [R], [A], [C] messages) and the Customer (receipts) to ensure consistency. [NBR157, NBR539]
- Transaction Identifier [NBR539]
- Any authorisation code allocated by the FI
- Free Text space for message from FI within prescribed format (Customer receipt only). [NBR031]
- Outcome message (e.g. reason if declined) [NBR539]
- Whether PO Ltd's copy or the Customer's copy

For Cash Withdrawal With Balance and Withdraw Limit transactions, the balance held on the account after the transaction will be printed on the Customer Receipt only if the Transaction is successful. This will be determined by the NBE. [NBR429]

6.3.2.10 Session Settlement

After one or more sale items have been selected and placed on the Product Stack, the Counter Clerk can initiate the payment phase via the Finish Button. Settlement is part of EPOSS and is primarily responsible for the settlement of a Customer Session.

Specifically it is concerned with the final settlement, validation and committal of the transaction stack.

6.3.2.11 Messages for Clerk and Customer

The [A] received from the NBE may contain error or other messages that are to be displayed to the Clerk (e.g. request to retain card), or to be printed on the Customer receipt (or both). A message requesting a card is to be retained must be unambiguous. This message is held in Reference Data. [NBR252]

Pathway notes that the message codes are the responsibility of the NBE, and that PO Ltd (BSM) will provide matching message texts, in Reference Data, and verify that messages are unambiguous as part of the OBC process. Error codes and the corresponding message texts are documented in [CNTRDLG]. [NBR219, NBR423]

The transaction may display messages to the Customer on the PIN Pad as part of the PIN capture process. These messages are also documented in [CNTRDLG]. [PPR011, PPR021, PPR023]

6.3.2.12 Transaction Fees

The Counter application will be able to display a message to the Clerk to advise the Customer concerning any fees chargeable to the FIs for the transaction. The Customer may then elect to abandon the Transaction without incurring any Customer fees, or accept the Transaction with the fees as advised. [NBR150]

The collection of fees is an FI to Customer issue and is not included in NBS.

6.3.2.13 Change of PIN

On-line change of PIN at the PIN Pad is supported. It enables the Customer to specify a PIN value that they can more easily remember, or to change a value that they believe has been compromised. [NBR431]

6.3.2.14 Card Operation Services

Card Operation services are required for POCA cards. The delivery of cards to an Outlet (or Customer), any pick up notice, and any notification to the Customer of the initial PIN, are outside the Pathway operational domain. Pathway notes there is no requirement for card reporting or redirection, and that the issue of POCA cards has no implications for Reconciliation or Settlement.

6.3.2.14.1 Receipt of Card at Outlet

Card receipt will be acknowledged at the Outlet via an APS bar-code transaction.

POCA cards will be sent to the nominated Outlet, from details supplied by the *Department for Work and Pensions* (DWP), for collection by the account holder. This has no impact on Pathway.

The POCA cards will be issued in envelopes having unique bar codes on the envelope, which the card issuer can relate to the issued card. The envelope contains both the card and other information that may be used to verify the Customer’s identity. This has fraud risks and [DPA] implications that are outside the Pathway operational domain. [NBR061]

The Post Office Manager scans the bar-coded envelopes when it is received, to acknowledge receipt of the cards. The message contains the FAD code of the Outlet. [NBR432]

For the avoidance of doubt, this process is subject to a separate CR and is outside the scope of this SDS.

6.3.1.1.2 Activation of a POCA Card

Card activation will be handled via a normal transaction, typically a Balance Enquiry transaction, with special processing at the Universal Bank to recognise this is the first use of the card.

Mechanisms to inform the Customer that a card is available for collection are outside Pathway's operational domain. Upon receipt of such a notification, the Customer goes to the indicated Outlet and requests his or her card. The Counter Clerk selects the envelope, and takes out the EVP questions and answers. Subject to receiving a correct answer to the EVP questions from the Customer, the Clerk performs a standard Balance Enquiry on the card.

The Universal Bank determines that this is the first use of the card, and checks that the Outlet is the same as that to which the card was issued. [NBR432]

It is assumed that the NBE will support transfer of FAD codes to the Universal Bank.

6.4 PIN PADS

The PIN Pad will be situated on the Customer side of the Counter. The Counter dialogue when using PIN Pads will be sufficiently different to that when using signature verification that completely separate dialogues may need to be developed, although the principles described above will apply. Signatures will not be required on any PIN Pad Transaction thus different receipt formats will be required. [NBR509]

Chapter 7 - Information Management

7.1 GENERAL

This Chapter summarises the handling of information within the NBS. It covers:

- Data flows between and within Components
- Interfaces
- Databases and their properties

7.2 REQUIREMENTS SUMMARY

The principal data flows are identified Figure 5. This Chapter elaborates on the data items that are needed on each flow.

7.3 DATA FLOWS AND INTERFACES

This section considers each of the main data flows listed in Section 3.3, and provides the basis from which the detailed AISs can be produced. The technical interfaces (i.e. details of the physical connections and the protocols used) are covered in Chapter 10.

The following interfaces are considered:

- Counter Data Interfaces into the Network Banking Counter Application (NBCA) from the Operation Launch Application and to and from the Framework functions (see Section 7.3.1)
- Riposte message flows between the Counter and the Agents ([R1], [A3], [C0] and [C1]) (see Section 7.3.2)
- Request and Authorisation Interface between the *NBS Authorisation Agent* and NBE ([R2] and [A2]) (see Section 7.3.3)
- Confirmation Interface between the *NBS Confirmation Harvester Agent* and DRS ([C12]) (see Section 7.3.4)
- Confirmation Interface between *NBS Expedited Confirmation Agent* and NBE ([C0]->[C2]) (see Section 7.3.5)
- Return interface from NBE to DRS ([C4] and [D]) (see Section 7.3.6)
- TPS Harvester interface to TPS Host ([C11]) (see Section 7.3.7)
- TPS Host to Data Warehouse Interface
- TPS Host to DRS Interface ([C112]) (see Section 7.3.8)
- TPS Host to TIP Interface ([C111]) (see Section 7.3.9)
- DRS to TIP Interface (see Section 7.3.10)

These are discussed separately below. The purpose of this Chapter is to define the information that is required across each interface. Detailed design of the data structures is the subject of the HLDs and will be recorded in any relevant AISs.

This Document defines the fields that are included in each message type at each interface. The meaning, nature, content, size and format of each field are as defined in [NBEIFS].

7.3.1 Counter Interfaces to and from NBCA

There are a number of aspects of this interface. They are:

- Definition of the impulse definition information passed to the NBCA from the Operation Launch application
- Data returned from the *Initialise* function to the NBCA
- Data to be passed to and from the *Input* function for communication with the PINPad
- Data to be passed across to the *RequestReply* function for inclusion in the [R1] message
- Data to be returned from the *RequestReply* function from the [A3] message
- Definition of the body of the receipts to be printed using the Output function
- Data stored in the Recovery message to enable automatic recovery to be completed following a terminal failure
- Network Banking specific data to be passed across to the *Finalise* function for inclusion in the [C1] message

Details are given in [NBEIFS].

7.3.1.1 Impulse Definition

This is a definition of the Impulse passed to the NBCA from the Operation Launch application. It identifies the mapping of data from the impulse to NBCA variables.

7.3.1.2 Interface to the Initialise Function from NBCA

The *Initialise* Function is passed the Impulse as received from the Operation Launch application from which it extracts the variables required by the NBCA, which it returns to the NBCA. It also stores the fields required by the other Framework functions for their later use.

Finally, it generates the *Horizon_Txn_Num* and returns that value for use by the *Input* Function.

7.3.1.3 Interface to Input Function from NBCA

This is a definition of the Data passed between the NBCA and the *Input* Function, which communicates with the PIN Pad.

7.3.1.4 NBCA Part of the [R1] Message

This is the data structure passed from the NBCA to the *RequestReply* hook as input.

7.3.1.5 NBCA Part of the [A3] Message

This is the data structure returned to the NBCA from the *RequestReply* hook.

7.3.1.6 Receipt Body Data

This is the definition of the Receipt Data passed from the NBCA to the *Output* function.

There are a number of such receipt layouts, corresponding to the various receipts that are produced.

These will be defined in [CNTRDLG].

7.3.1.7 Recovery Information

Once the Receipt has been successfully printed, Recovery information is written to the message store to enable the Outcome of the Transaction to be automatically recovered should the terminal fail. In the event that this Outcome could differ from what the bank has Authorised, then this information is also used to generate the [C0] message which is sent to the NBE as soon as possible.

7.3.1.8 NBCA Part of the [C1] Message

This is the data structure passed from the NBCA to the *Finalise* hook as input.

7.3.2 Counter Application Interfaces

7.3.2.1 [R1] Message

This is a message generated by the NBS Counter Application. It includes for following fields, provided by the components shown

Message Element	Source
Agent_Hash	*RequestReply* function
Agent_Timeout	*RequestReply* function
Amount_Requested	NBCA
Clerk_Identity	Riposte at Counter [NBR541]
Client_Id	*Initialise* function (from Impulse)
Container	*Initialise* function
Currency	*Initialise* function (from Impulse)
Digital_Signature	*RequestReply* function
Encrypt	*RequestReply* function
Entry_Method	*Initialise* function (from Impulse)
Expiry_Date	*Initialise* function (from Impulse) Included in *Encrypt*
Financial Transaction	Generated by *Initialise* function
Group_Id	Riposte at Counter
Horizon_Txn_Num	Generated by *Initialise* function
Issue_Number	*Initialise* function (from Impulse) Included in *Encrypt*
Issuer_Scheme_Id	*Initialise* function (from Impulse)
Language_Code	*Initialise* function (from Impulse)
Maximum_Withdrawal	NBCA
Message_Type	*RequestReply* function
Node_Id	Riposte at Counter
PAN	*Initialise* function (from Impulse)
PIN_Blob_1	NBCA (from Input function)
PIN_Blob_2	NBCA (from Input function)
Product_Number	*Initialise* function (from Impulse)
Receipt_Transaction_Date	Generated by *Initialise* function
Receipt_Transaction_Time	Generated by *Initialise* function
Routing_Gateway	*Initialise* function (from Impulse)
Signature_Type	*RequestReply* function
Start_Date	*Initialise* function (from Impulse) Included in *Encrypt*

Track_2_Image	*Initialise* function (from Impulse) Included in *Encrypt*
Txn_Type	*Initialise* function (from Impulse)
Version_Number	*RequestReply* function

Table 4 – [R1] Message Contents

7.3.2.2 [A3] Message

This is a message generated by the *NBS Authorisation Agent* when handling an [A2] message from the NBE.

The following table lists all the fields included in the [A3] message:

Message Element	Destination
Agent_Error	If present passed to *Error_Text* field in Transaction XML
Agent_Diagnostic	Ignored (diagnostic use only)
Agent_SLA_Info	Pass through to [C1]
Amount_Authorised	Pass through to [C1]
Auth_Code	Pass through to [C1]
Balance	
Bank_Transaction_Id	Pass through to [C1]
Counter_SLA_Info	This is calculated by the RequestReply function for inclusion in the [C1] for SLA purposes
Currency	For *RequestReply* function to check it is as expected.
Digital_Signature	For *RequestReply* function to check it is correct.
Fee	Pass through to [C1]
Horizon_Txn_Num	For *RequestReply* function to check it is as expected.
Message_Type	For *RequestReply* function to check it is as expected.
Receipt_Text	Pass through to [C1]
Receipt_Transaction_Date	For *RequestReply* function to check it is as expected.
Receipt_Transaction_Time	For *RequestReply* function to check it is as expected.
Response_Code	Pass through to [C1]
Settlement_Date	Pass through to [C1]
Signature_Type	For *RequestReply* function to check it is correct.
Version_Number	For *RequestReply* function to check it is as expected.

7.3.2.3 Recovery / [C0] Message

A single message is written normally as a Recovery message, however if a [C0] is required, then the additional [C0] fields are also included. Note that not all Recovery fields are required in the [C0] message, however they will be included in the message so that it may still be used for recovery purposes should the need arise.

Message Element	Needed for Recovery	Needed in [C0]	Source
Agent_Hash		Yes	Value used in original [R1]
Agent_SLA_Info	Yes		Value returned in [A3]
Amount_Confirmed	Yes	Yes[36]	Amount actually transacted
Amount_Requested	Yes		Value used in original [R1]
Auth_Code	Yes		Value returned in [A3]
Bank_Transaction_Id	Yes	Yes	Value returned in [A3]
Card_Impounded	Maybe		Flag to indicate if the Card was Impounded Probably not required.
Clerk_Identity	Yes	Yes	Riposte at Counter [NBR541]
Client_Id	Yes	Yes	Value used in original [R1]
Counter_SLA_Info	Yes		Calculated by *RequestReply* function
Currency	Yes	Yes	Value used in original [R1]

[36] *Always zero for a [C0]*

Digital_Signature		Yes	Calculated as the message is written
Entry_Method	Yes		Value used in original [R1]
Fee	Yes		Value returned in [A3]
Group_Id	Yes	Yes	Riposte at Counter
Horizon_Txn_Num	Yes	Yes	Value used in original [R1]
Issuer_Scheme_Id	Yes	Yes	Value used in original [R1]
Message_Type	Yes	Yes	
Node_Id	Yes	Yes	Riposte at Counter
PAN	Yes	Yes	Value used in original [R1]
Receipt_Transaction_Date	Yes	Yes	Value used in original [R1]
Receipt_Transaction_Time	Yes	Yes	Value used in original [R1]
Recovery_Flag	Yes		Set to 1
Response_Code	Yes		Value returned in [A3]
Routing_Gateway	Yes	Yes	Value used in original [R1]
Settlement_Date	Yes		Value returned in [A3]
Signature_Type		Yes	Indicates that [C0] is signed as an Attribute Grammar string
Transaction_Result_Code	Yes	Yes	This defines the Clerk's view of the outcome of the transaction
Txn_Type	Yes	Yes	Value used in original [R1]
Version_Number	Yes	Yes	Version of Recovery message structure in use.

Table 5 – Recovery / [C0] Message Contents

7.3.2.4 [C1] Message

This is constructed by the *Finalise* function. It contains the following fields.

Field	Comment
Agent_Hash	Remembered from the [R1]
Agent_SLA_Info	Remembered from the [A3]
Amount_Requested	Remembered from the [R1]
Auth_Code	Remembered from the [A3]
Bank_Transaction_Id	Remembered from the [A3]
Client_Id	Remembered from the *Initialise* function
Counter_SLA_Info	Calculated by *RequestReply* function
Currency	Remembered from the *Initialise* function
Digital_Signature	This will sign that part of the [C1] message that is to be passed to the NBE (in the [C2] message) in Attribute Grammar.
Fee	Remembered from the [A3]
Financial_Transaction	Remembered from the *Initialise* function
Horizon_Txn_Num	Remembered from the *Initialise* function
Issuer_Scheme_Id	Remembered from the *Initialise* function
Message_Type	
Original_Clerk_Identity	Clerk_Identity of the original transaction when a Recovery transaction is written (possibly by a different user)[37] [NBR541]
PAN	Remembered from the *Initialise* function
Receipt_Transaction_Date	Remembered from the [R1]
Receipt_Transaction_Time	Remembered from the [R1]
Recovery_Flag	Only included if generated by the Recovery Application
Response_Code	Remembered from the [A3]
Routing_Gateway	Remembered from the *Initialise* function
Settlement_Date	Remembered from the [A3]
Signature_Type	Indicates that [C1] is signed as an Attribute Grammar string
Txn_Type	Remembered from the *Initialise* function
Version_Number	Version of [C1] message structure in use.

Table 6 – [C1] Message Contents

[37] *This should certainly be recorded for audit purposes. Is there any need to harvest it to TPS or DRS?*

It will also include all the standard *EPOSSTransaction* fields, which will be populated from the *EPOSSProduct* Reference Data as for normal EPOSS Products.

Field	EPOSS Tag	Comment
Amount	SaleValue	
Entry_Method	EntryMethod	Also included in [C12]
Product_Number	ProductNo	Also included in [C12]
Product_Number_Version	PVer	
Quantity	Qty	
Cross_Reference	CrossReference	Is this actually required?
Linked_Transactions	LkdTxns	Is this actually required?
	BlackBoxData	Is anything needed here?
	TxnData	Standard data added by Retail Broker
	TranType	
Primary Mappings	PM	Needed for EPOSS Accounting
Secondary Mappings	SM	Needed for EPOSS Accounting
	Debit / Credit	

Table 7 – [C1] EPOSS Fields

In addition, since the [C1] will be a standard Riposte message, then the following fields will be included:

Field	Comment
Clerk_Identity	I.e. User [NBR541]
Group_Id	FAD Code without check character
Node_Id	Within FAD i.e. Counter Position

Table 8 – [C1] Message Additional Fields

7.3.3 Request and Authorisation Interface to NBE

7.3.3.1 [R2] Message

Information in the [R2] is derived from the [R1] (see Section 7.3.2.1 unless indicated otherwise.

Message Element	In [R2]?	Source
Agent_Date	Yes	Added in by Agent
Agent_Hash	No	
Agent_Time	Yes	Added in by Agent
Agent_Timeout	No	
Amount_Requested	Yes	NBCA
Clerk_Identity	Yes	[NBR541]
Client_Id	Yes	
Container	No	Ignored by Agent
Currency	Yes	
Digital_Signature	No	
Encrypt	Yes	
Entry_Method	Yes	
Expiry_Date	Yes	
Group_Id	Yes	
Horizon_Txn_Num	Yes	
Issue_Number	Yes	
Issuer_Scheme_Id	Yes	
Language_Code	Yes	
Maximum_Withdrawal	Yes	
Message_Authentication_Code	Yes	Added in by Agent
Message_Type	Yes	

Node_Id	Yes	
PAN	Yes	
PIN_Blob_1	Yes	
PIN_Blob_2	Yes	
Product_Number	No	Ignored by Agent
Receipt_Transaction_Date	Yes	
Receipt_Transaction_Time	Yes	
Routing_Gateway	Yes	
Signature_Type	No	
Start_Date	Yes	
Track_2_Image	Yes	
Txn_Type	Yes	
Version_Number	Yes	Added in by Agent. Identifies Protocol Version in use

Table 9 – [R2] Message Contents

7.3.3.2 [A2] Message

Data in the [A3] is derived from the [R1] unless otherwise indicated.

Message Element	In [A2]?	Destination
Agent_Diagnostic	No	
Agent_Error	No	
Agent_SLA_Info	No	
Amount_Authorised	Yes	
Auth_Code	Yes	
Balance	Yes	
Bank_Transaction_Id	Yes	
Currency	Yes	
Digital_Signature	No	Generated by agent
Fee	Yes	
Horizon_Txn_Num	Yes	
Message_Authentication_Code	Yes	Checked by Agent and discarded
Message_Type	Yes	Implicit
Receipt_Text	Yes	
Receipt_Transaction_Date	Yes	
Receipt_Transaction_Time	Yes	
Response_Code	Yes	
Settlement_Date	Yes	
Signature_Type	No	Indicates that [A3] is signed as an Attribute Grammar string
Version_Number	Yes	Identifies Protocol Version in use

Table 10 – [A2] Message Contents

7.3.4 Confirmation Interface to DRS

This interface consists of the Data being harvested for processing within the DRS.

The Data will be harvested into a single logical table.

The following table shows the data fields in the [C1] message that are relevant to the DRS in the [C12] message:

Message Element	Comment
Amount_Confirmed	Included in [C2]
Amount_Requested	May be relevant if the transaction was declined
Auth_Code	
Bank_Transaction_Id	Included in [C2]
Card_Impounded	
Clerk_Identity	[NBR541]

Client_Id	Included in [C2]
Currency	Included in [C2]
Entry_Method	
Fee	
Group_Id	
Horizon_Txn_Num	Included in [C2]
Issuer_Scheme_Id	Included in [C2]
Message_Type	
Node_Id	
Product_Number	
PAN	Included in [C2]
Receipt_Transaction_Date	Included in [C2]
Receipt_Transaction_Time	Included in [C2]
Recovery_Flag	
Response_Code	
Routing_Gateway	Included in [C2]
Settlement_Date	
Transaction_Result_Code	Included in [C2]
Txn_Type	Included in [C2]
Version_Number	
XML	[C2] data for passing through to the NBE

Table 11 – [C12] Message Contents

In addition to the [C12] message, the Agent will pass the following information to the DRS:

Parameter Name	Comment
Agent_Error_Code	
Agent_Error_Message	
Agent_Host_Name	
Agent_Id	
Application_Type	"NBA" or "DCA"
Record_Status	

Table 12 – Additional Data passed to DRS

7.3.5 Confirmation Interface to NBE

Normal [C1] messages are not passed to the NBE. Instead, [C0] messages that signify a different outcome from that in the [A] message *are* passed to the NBE as a [C2] by the *NBS Expedited Confirmation Harvester Agent*. They contain the following fields, derived principally from the [C0].

Message Element	In [C2]?	Source
Amount_Confirmed	Yes	
Bank_Transaction_Id	Yes	
Clerk_Identity	Yes	[NBR541]
Client_Id	Yes	
Currency	Yes	
Digital_Signature	No	
Group_Id	Yes	
Horizon_Txn_Num	Yes	
Issuer_Scheme_Id	Yes	
Message_Authentication_Code	Yes	Added in by Agent
Message_Type	Yes	Added in by Agent
Node_Id	Yes	
PAN	Yes	
Receipt_Transaction_Date	Yes	
Receipt_Transaction_Time	Yes	

Routing_Gateway	Yes	
Signature_Type	No	
Transaction_Result_Code	Yes	
Txn_Type	Yes	
Version_Number	Yes	Identifies Protocol Version in use

Table 13 – [C2] Message Contents

7.3.6 Return interface from NBE

There are two separate data flows from the NBE to the DRS:

- Confirmation Receipt ([C4])
- Discrepancy messages ([D])

Both are transmitted in a set of batch files at the NBE's End of Day.

7.3.6.1 Confirmation Receipt ([C4])

The following table shows the data fields in the [C4] message:

Message Element	Comment
Amount_Confirmed	
Bank_Transaction_Id	
Client_Id	
Currency	
Group_Id	
Horizon_Txn_Num	
Message_Type	
PAN	
Receipt_Transaction_Date	
Receipt_Transaction_Time	
Routing_Gateway	
Settlement_Date	
Txn_Type	
Version_Number	

Table 14 – [C4] Message Contents

7.3.6.2 Discrepancy Messages ([D])

The following table shows the data fields in the [D] message:

Message Element	Comment
Amount_Authorised	
Amount_Confirmed	
Amount_Discrepancy	
Amount_Requested	
Bank_Transaction_Id	
Clerk_Identity	[NBR541]
Client_Id	
Currency	
Discrepancy_Reason_Code	
Group_Id	
Horizon_Txn_Num	
Message_Type	
Node_Id	
PAN	
Receipt_Transaction_Date	
Receipt_Transaction_Time	

Routing_Gateway	
Settlement_Date	
Txn_Type	
Version_Number	

Table 15 – [D] Message Contents

7.3.7 TPS Harvester Interface to TPS Host

This will be a new Interface table into the TPS Host. It will consist of all the normal *EPOSSTransaction* fields (including those associated with Reversals in readiness for implementing reversals in the future) plus the following Banking specific fields:

Field	DRS ?	Data Warehouse?
Agent_SLA_Info	n	y
Amount_Requested	y	n
Auth_Code	y	y
Bank_Transaction_Id	y	y
Card_Impounded	y	y
Client_Id	y	y
Counter_SLA_Info	n	y
Currency	y	y
Fee	y	n
Financial_Transaction	y	n
Horizon_Txn_Num	y	y
Issuer_Scheme_Id	y	y
PAN	y	y
Receipt_Transaction_Date	y	y
Receipt_Transaction_Time	y	y
Recovery_Flag	y	n
Response_Code	n	y
Routing_Gateway	y	y
Settlement_Date	y	y
Transaction_Result_Code	y	y
Txn_Type	y	y

Table 16 – TPS Host Data Fields

Note that the DRS will only utilise the values received by this route if they have not already been received from the [C12] message.

NB: although all items are marked as "y" in the Data Warehouse column, some may not strictly be required, however it is considered to be simpler to pass all data to the Data Warehouse in case it is considered to be useful at a later time.

7.3.8 TPS Host to DRS Interface

This is covered by Section 9.5.1.1 and consists of a View of the TPS Database made available to DRS..

7.3.9 TPS Host to TIP Interface

This is unchanged.

7.3.10 TPS Host to Data Warehouse Interface

TPS Host will send details of all NBS transactions, both successful and unsuccessful, to the Data Warehouse. The existing interface will be expanded to pass data in a set of flat files in the same manner as EPOSS, APS and OBCS transactions are currently. The interface will be fully defined in [DWTPSAIS].

7.3.11 DRS to TIP Interface

This is covered by Chapter 8.

7.4 ORACLE

The DRS will be implemented on the Host Central Server as an additional Oracle application with its own Oracle database.

This application and database will be implemented using Oracle 8i. This is to permit exploitation of new facilities needed to provide the required performance.

The RDMS and *Reference Data Distribution Service* (RDDS) applications will also be upgraded to Oracle 8i. The TPS, APS, LFS and OBCS databases will remain on Oracle 7.

It is not believed that there are any significant issues with running two versions of Oracle on the same platform, though the disk space available on the Host Central Servers will need to be increased to cater for the extra software.

7.5 SQL SERVER

The applications running on SQL Server (*Key Management Application* (KMA), ACDB, OCMS) will be upgraded from SQL Server V6.5 to V2000. This is in line with Pathway's strategy of moving to a later, fully supported release when there is a need for significant development to an existing application.

Each SQL Server application runs on a dedicated platform, so there are no co-existence issues with this upgrade strategy.

The Audit Checksum Database, which is significantly enhanced at BI3, is migrated from Access to SQL Server and appropriate licences will be required. The enhanced service will run on the Audit Server.

Chapter 8 - Reference Data

8.1 GENERAL

Reference Data provides the source of business and system parameters that are used to configure the Horizon System. It is used by System applications or services, and is controlled outside of changes to the application or service to which it pertains.

The Pathway Reference Data Management Service (RDMS) provides the components and processes that receive, control, manage, verify and deliver that data to the system processes that use it. The introduction and change of Reference Data is subject to *Operational Business Change* (OBC) processes within PO Ltd. RDMS is one of the Pathway services that interacts with and implements the outcome of OBC.

NBS introduces some major changes to the requirements for Reference Data.

There are established OBC procedures governing the distribution of PO Ltd Reference Data and these will be extended to handle WebRiposte and web application parameters. [NBR025]

The PO Ltd Reference Data changes are categorised according to risk and complexity and validated accordingly. The time taken for data to be authorised for distribution to Counters depends on the category and complexity of the change, though once data arrives, in most cases it is subject to Temporal control (i.e. it is distributed with a "commencement date" and "expiry date". [NBR407]

8.2 SUMMARY OF REQUIREMENTS

It is a requirement that NBS shall be driven by Reference Data such that new account types and new FIs can be added with minimal impact on the system.

Changes that are outside the OBC procedure will require to be handled via contractual Change Control procedures.

Specific requirements include additional Business Attributes to manage and configure NBS Transactions

It also provides for:

- Service Management control of additional Reference Data
- System Management control of Reference Data delivery to the estate

Requirements for the operation and management of Reference Data include:

- The increased use of Reference Data and the impact on volumes (particularly the number of Persistent Objects held on the Counter), and the control and timely distribution of these to the estate. This will impact on the Maestro schedule for NBS

- The changes to Reference Data and the underlying systems used to handle it must not impact the quality of service for supporting existing systems. The design and release strategy must encompass solutions that eliminate any compromise to quality of service.
- The introduction of NBS will be activated at pilot Outlets first, followed by the rest of the estate. RDMS must be capable of supporting the phased activation of Outlets whilst also allowing the early distribution of NBS Reference Data to all Outlets so as to maximise the speed with which an Outlet can be activated

8.3 SERVICE DESCRIPTION

8.3.1 General

Reference Data is used by System applications or services but is controlled outside of changes to the application or service to which it pertains.

The introduction of NBS significantly extends the use to which Reference Data is put. The specific and principle change is the ability to introduce new services (transactions) that themselves are defined as Reference Data. In consequence, these services are themselves released, controlled and configured from outside the environment in which they are used.

8.3.2 End-to-End Service Boundaries

The following diagram shows the context of Pathway Reference Data and its relationship to four external entities: the Post Office, Pathway (Development), the (Pathway) Host Servers and Correspondence Servers

- The Counter Application development will be carried out by Pathway for NBS
- PO Ltd supply PO Ltd Reference Data including configuration data for NBS

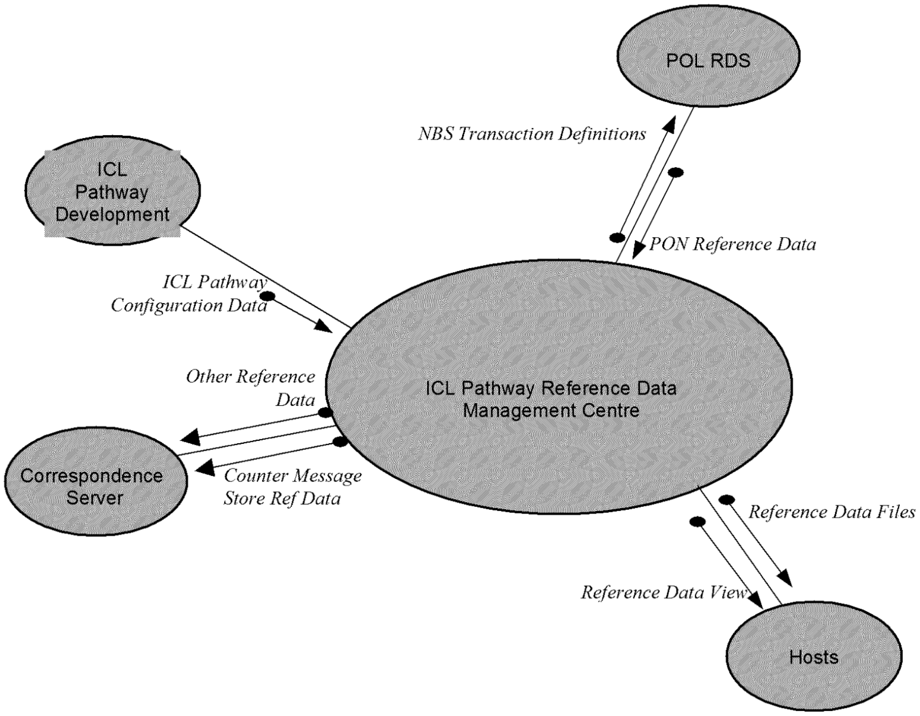


Figure 12 – Reference Data Context Diagram

8.3.3 External entities

The following entities are defined in the above diagram.

- *Post Office* represents the operational part of PO Ltd responsible for Reference Data management. Reference Data under their control will be distributed via PO Ltd's *Reference Data Service* (RDS)
- *Pathway* itself also provides Reference Data. Pathway Data Management (whether Customer Services or Development) is responsible for the provision and enrichment of certain classes of Reference Data prior to delivery to the Counter.
- The *Correspondence Server* represents the primary destination for the delivery of Reference Data. Data held in these is replicated to the Counter messages stores where it can be accessed by Counter applications.
- *Pathway Host Systems* also use Reference Data, for example TPS.

PO Ltd BSM and the Pathway System Management Domain are treated as components of Pathway Reference Data Management for the purpose of this document.

8.3.4 Data Flows

The following logical data flows are shown in the above diagram. They are described in alphabetical order.

- *Counter Message Store Reference Data* – The primary data store for Reference Data is the Counter message store. Data for use by Counter applications and Riposte, including NBS, resides here. Counter Message Store Data includes Business Rules, system parameters and Outlet configuration data. It is delivered to the Correspondence Server for onward replication by WebRiposte to the Counters.
- *NBS Transaction Definitions* – The ability for PO Ltd to take-on new Clients and market the offerings available for Banking Services requires them to be notified of all Banking Transactions supported by the system. The available NBS Transactions are notified to PO Ltd for use in product and Client introduction.
- *Other Reference Data* – not all Reference Data available for use resides in the Counter message store. For example, Icon files are delivered as files that are accessed directly by Riposte Infrastructure to display the appropriate Icon. Similarly, the Global Objects Report Definition file is delivered as part of the EPOSS product set and is accessed by EPOSS. Such data, whilst on the fringes of the definition of Reference Data, nonetheless provides data that 'drives' (or configures) system operation, has to be tested as such and in some cases is validated and verified as part of OBC.
- *PO Ltd Reference Data* – as required by the existing Horizon applications. It will be enhanced with additional products that represent the NBS transactions to be accounted for. It includes product specification data and Cash Account mapping data and will be enhanced for NBS to include data that configures the Counter application to support particular FIs and particular account types. This is likely to include the rules or constraints that apply to the account types operated by each FI, such as: minimum and maximum deposit, floor limit for fallback working, etc.
- *Riposte Configuration Data* – Escher Products use Reference Data. The data is delivered as part of the product or is required by the product. Some data is configurable and must be enriched by Pathway. The introduction of WebRiposte extends the use of Riposte Configuration Data.
- *Reference Data Files* – PO Ltd Reference Data is not only used by the Counter applications. It is also made available to other Pathway Host Systems through Interface files provided by the Pathway Reference Data Management System. The Data Warehouse uses this data flow.
- *Reference Data View* – PO Ltd Reference Data is not only used by the Counter applications. It is also made available to other Host Systems through Views to the Pathway Reference Data Management System. DRS will use this data flow.

8.4 PRODUCT AND TECHNICAL INTERFACES

There are a number of interfaces identified in Figure 12. Each is under Pathway's control. The following interfaces between Pathway and external parties need to be formally defined and agreed via AISs.

- Between Pathway and PO Ltd

The remaining interfaces are between components of the Horizon System.

- Interfaces from the Pathway RDMS to the Counter and Correspondence Server
- Interfaces between the Pathway RDMS and other Host Systems

- Interfaces between the Pathway Agents and the Systems Management Domain. The existing Reference Data Acknowledgement Agent interface with the Data Warehouse will be replaced by a new interface into the *Operational Management Database* (OMDB). The Reference Data Acknowledgement Agent harvests acknowledgements from the delivery of Reference Data to the Outlets. An additional interface between the OMDB and the Systems Management Database will be introduced to allow views into the estate Reference Data Inventory. This is part of the design and implementation of the System Management Domain

All these interfaces can be considered at a number of levels.

- *Physical* – in terms of the connectivity and communications protocols used.
- *Logical* – in terms of the application level protocols carried.
- *Data* – in terms of the data flows carried.

The following summarises each of these interfaces separately.

8.4.1 Between Pathway and PO Ltd

This is an enhancement to the existing RDS-to-RDMS interfaces. [NBR202]

A new interface will be defined between RDMS and PO Ltd OBC for the receipt of transaction definitions.

8.4.2 Interfaces between Host Systems

This is the existing interfaces provided between Pathway's RDMS and other Host systems. An enhancement to this interface will be required for the introduction of the DRS.

8.4.3 Interfaces from the RDMS to the Agents

This is the normal flow between the existing Campus and the Counter.

8.4.4 Interfaces from the Agents to the System Management Domain

The existing Reference Data Acknowledgement Agent interface with the Data Warehouse will be replaced by a new interface into the OMDB, to record the delivery of Reference Data to the Outlets.

An additional interface between the OMDB and the *Service Management DataBase* (SMDB) will be introduced to allow views into the estate Reference Data Inventory.

8.5 DESIGN PRINCIPLES AND ASSUMPTIONS

8.5.1 General

The principles taken to the development of enhanced Horizon Reference Data and an enhanced RDMS are as follows.

- Provide an enhanced OBC process that minimises Time to Market for changes to Reference Data
- Implement a Reference Data Model so that the integrity of data is assured
- Stage the implementation to minimise the impact on the Horizon infrastructure and SLAs
- Minimise the cost of the enhancements
- Minimise the disruption caused by the enhancements to RDMS

8.5.2 Summary of Design Changes

Enhancements are required to the Horizon Reference Data handling in the following areas.

- The Counter and Campus infrastructure will be upgraded to use later versions of many of the commodity products currently in use. Specifically, the RDMS applications will be supported on a later version of Oracle
- The RDMS will be enhanced to receive additional Reference Data entity types and attributes from PO Ltd through a changed interface, for example to support the PO Ltd organisational structure required for MIS reporting [NBR483]
- The RDMS will be enhanced to include additional integrity checking of Reference Data
- A new RDMS process will be developed to receive and register new and changed NBS Configuration Data through a new interface between Pathway and PO Ltd
- Remaining Reference Data Views will be enhanced to make available additional data types and attributes in support of transactions posted by NBS Transactions
- The Host Counter Reference Data View will be enhanced to deliver additional data types and attributes to the Counter
- A new Pathway OBC process will be developed to manage the receipt, and consequential testing, verification, signing and release of Reference Data comprising different types, specifically NBS Configuration and PO Ltd Reference Data
- New Processes will be introduced to support the receipt of data associated with the different Riposte Products and distribute in an orderly manner.
- Enhancements will be made to the Pathway Development Reference Data Production and enrichment processes to support the addition of NBS Configuration Data
- Enhancements will be made to the Pathway Release Management Processes for Reference Data to ensure the appropriate controls in the release and testing of changes to the system are managed and assured.
- Changes will be required to Tivoli, the OMDB and the SMDB to hold the inventory picture of Reference Data delivered to the Outlets and provide views for accessing that data
- Improvements will be made to the SLA measurement processes through enhancements utilising the SMDB and Data Warehouse

- A new Pathway Process will be developed to control and assure the interdependence of changes to Reference Data in its domain
- Pathway Testing processes will be enhanced to enable business assurance testing where required, in response to changes to Reference Data comprising 'code' sourced from a third party

8.5.3 Release Profile and Migration

The principle of the release profile for RDMS revolves around the following factors:

- Maintaining OBC for the existing Counters throughout
- Providing three phases of RDMS upgrade allowing fallback contingency positions to be taken in the event of problems, ensuring coordination of dependencies with PO Ltd to be satisfied at all times, yet allowing parallel development and test capability
- Allowing graduated introduction of new data

The RDMS changes to support new and changed Reference Data will mainly be made in BI3. Delivery of new Reference Data supported by the changes and the processes for its control, will also be a part of BI3, prior to activation of the applications that use that data. As a consequence, there is a need to incorporate sub releases within BI3 to recognise and accommodate the specific Reference Data increments and dependencies, together with their coordination with the introduction and activation of the NBS Counter applications.

- The host Reference Data Systems will be upgraded to Oracle 8i
- An enhanced RDMS will be introduced to allow new PO Ltd Product Reference Data (Type A, B and C) to be received and 'held', in support of the PO Ltd RDS data model implemented through an enhanced interface with PO Ltd
- The Pathway Enrichment Process will be similarly upgraded to support the enrichment of new or changed data.
- An enhanced RDDS will be introduced to allow new PO Ltd Product Reference Data to be released to the existing Counters. This stage will also introduce a new OBC Process in support of the new data model
- New Type A, B and C Reference Data may now flow from PO Ltd to the existing Counters under enhanced OBC. This process is necessary to enable OBC to continue throughout implementation of NBS.
- The enhanced Reference Data Release Management and Verification Processes and Service will be introduced to coordinate the release, validation and signing of new classes of Reference Data and their interdependencies, before allowing the live release of data.
- Reference Data Activation objects will be implemented under OBC to 'release' NBS Transactions to the estate. Activation Objects are any temporal item that allows a transaction to be 'executed'; i.e. they activate use of a transaction. Activation objects are not new, they are merely a label to existing objects that do something specific in terms of initiating NBS transactions.
- Full OBC commences

8.6 REFERENCE DATA ARCHITECTURE

This Section describes the end-to-end architecture of the enhanced Pathway RDMS in order to support NBS. It elaborates on Figure 12.

8.6.1 Reference Data Classifications

Reference Data takes many forms, and is used by Host systems and Counters alike. The main channels for accessing Reference Data are the Riposte Message Store for the Counter and Correspondence Servers, and Database Views or Data Files from the RDMC for other Host applications.

Reference Data defines a variety of aspects of the system and arrives from a number of sources. For example:

- Product definitions are sourced by PO Ltd and delivered by RDMS for use on the

Counter

- Menu Buttons are specified by PO Ltd but built by Pathway
- Riposte Configuration Data is sourced within the Riposte Product, customised by Pathway and delivered into the Correspondence Server Message Store directly

A number of Reference Data classifications have been introduced to differentiate between these provenances and usages. The full set of classifications is now as follows.

- *Type A*: 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 and Cash Account mapping data. It is enhanced for NBS to include data that configures the Counter application to support particular FIs and particular account types, and also to include the products that represent the NBS transactions for accounting purposes. Type A Reference Data is not configured by Pathway

- *Type B*: Temporal data transmitted electronically over a non-automated interface from PO Ltd RDS to the RDMS, enriched by data loaded manually by Pathway. Examples are Migration Data. This, too, is enhanced to include products that represent the NBS transactions

- *Type C*: 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. It will be further enhanced to handle the temporal control objects that are used to manage application activation

- *Type D*: Data prepared by Pathway, mainly non-temporal build dependent definitions. It is not loaded into RDMC. New Type D data will be required to define the new Counter applications (such as Operation Launch)

The type of Reference Data to which an object pertains can significantly influence the amount of acceptance testing required when that object is introduced or is changed.

8.6.2 Logical Processing Model

The following diagram extends the logic of Figure 12 to show the different handling for different types of Reference Data.

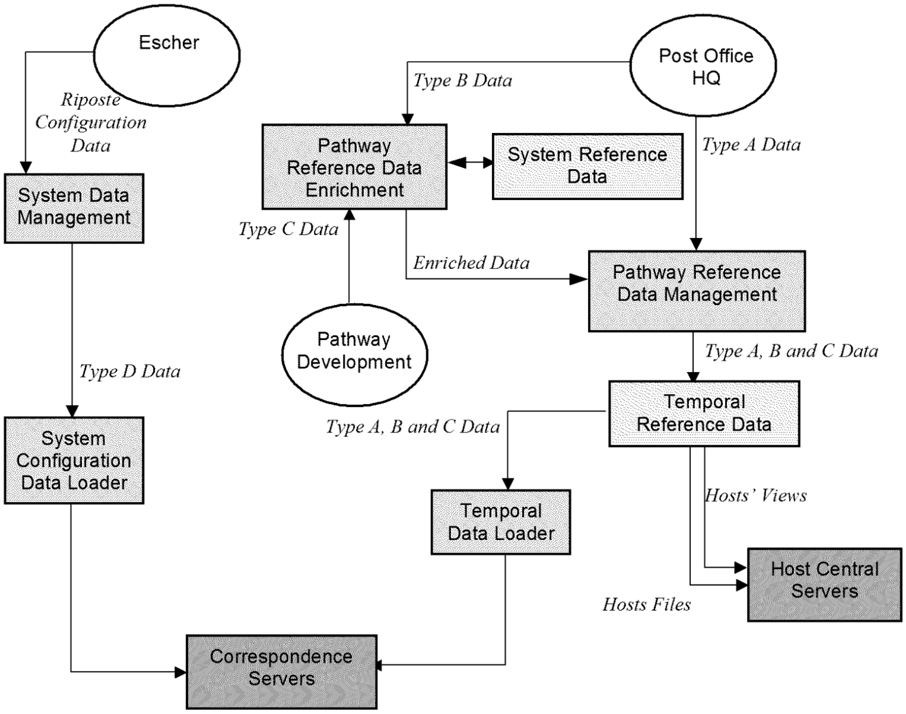


Figure 13 – Reference Data Logical Structure

The same external entities are shown, and the data flows to and from them remain the same. The logical representation, however, shows the Reference Data processes responsible for the receipt, control and delivery of Reference Data and the data flows between them.

8.6.3 Processes

- *Pathway Reference Data Enrichment* represents that part of the Pathway Development Directorate that is responsible for processing manually received data (for example changes to menu Buttons) in response to OBC or system changes
- *Pathway Reference Data Management* represents the RDMC that processes PO Ltd Reference Data changes and releases authorised changes to the Counter or other Host systems. It provides the primary means of managing Reference Data, ensuring a single source for all PO Ltd data available to the rest of the system
- *System Data Management* represents the existing process to receive and manage release of Reference Data that is required as an integral part of the Escher Product Set.
- *Temporal Data Loader* represents the existing process for loading Reference Data to the Correspondence Server from the RDDS for replication to the Outlets. No enhancements are required

- *System Configuration Data Loader* represents the existing process for loading Reference Data directly at the Correspondence Server for replication to the Outlets

The overall process of Receipt, Distribution and Activation of Reference Data is subject to OBC and Release Management and is managed by Pathway Customer Services. The Pathway entities represent the 'system' processes or activities to capture or enrich and manage Reference Data.

8.6.4 Logical Data Flows

Many of the data flows in this diagram are the same as in Figure 12. New or modified data flows are as follows.

- *Riposte Configuration Data* This encompasses data that is Type D, for example the existing Application *Dynamic Linked Libraries* (DLL) Registration Objects are Type D, as are the Riposte Signature Objects
- *Enriched Data –* Some Reference Data arrives or is specified in raw form that requires conversion or 'enrichment' before it can be released. Responsibility for this enrichment falls within Pathway Development. All enriched data is submitted to Pathway Reference Data Management for release to the Counter.
- *Type D Data* – the existing Type D data flow provides the configurable elements of the Escher Product Set to the Counter
- *Type A Data* – as required by the existing Horizon applications and enhanced as described above
- *Type B Data* – as required by the existing Horizon applications and enhanced for NBS
- *Type C Data* – as required by the existing Horizon applications and enhanced for NBS
- *Host Views* – PO Ltd Reference Data is made available to other Host applications through database "Views" to the RDMC
- *Host Files* – PO Ltd Reference Data is also made available to other Host applications through data files produced by the RDMC

8.6.5 Reference Data Changes at the Host Layer

8.6.5.1 Overview

The RDMC acts as a repository for the receipt of Reference Data, from either PO Ltd (Type A) or Pathway Development (Type B and C), the latter being enriched within the Pathway Reference Data enrichment process. RDMC will be enhanced to take responsibility for changes in the Type A data interface, and for the management of NBS Configuration Data.

Enhancements will be required to the Reference Data Enrichment process within Pathway Development to process additional data attributes and data types.

Counter applications may be received from different sources and there is a tight interdependency between the different types of data. RDMC includes a process that checks that these dependencies have been satisfied, and that version control is followed.

Processes outside RDMC handle the testing, inventory management, release management and operational business change of new applications. These will be enhanced as necessary.

8.6.6 Reference Data Changes at the Counter Layer

It is not envisaged that existing Counter applications require to change as a result of NBS.

Specifically additional data that is provided in support of NBS Transactions will be delivered as new Riposte temporal persistent object Collections or changes (additions) to existing Collections.

The structure of existing current Reference Data will not be changed, only additional attributes or Collections added.

New Collections and new attributes on existing Collections will both exist and be benign to existing applications.

8.7 HANDLING OF NBS CONFIGURATION DATA

8.7.1 Business Rules and Parameters

Business Rules and Parameters will be extended for NBS. Additional entities and attributes will be required and will form new elements of the PO Ltd Reference Data Model and interface. These will require extensions to the existing interface with PO Ltd. These changes are of two types:

- Changes to existing Reference Data
- The introduction of new Reference Data.

8.7.1.1 Changes to Existing Reference Data Flows

These are:

- Menu Buttons
- Product Data
- Impulses

8.7.1.1.1 Menu Buttons

Pathway Reference Data is used to define the menu hierarchy, based on information supplied by PO Ltd. This is then used by the MenuBuilder application during desktop initialisation to define the full menu hierarchy. This approach will continue.

8.7.1.1.2 Product Data

Product Data comes directly from PO Ltd. Each NBS Transaction will be associated with an appropriate Product to tie in with the accounting system. This in turn will require links into the accounting structures such as *CAMappings* and *EPOSSNode*s. However, this is similar to the introduction of any new product.

8.7.1.1.3 Impulses

Each bankcard Type will need to have an appropriate Impulse defined, to route the impulse through to the correct NBS transaction (and to differentiate these from APS or other token-based applications).

8.7.1.2 New Reference Data Flows

The following data will be provided by PO Ltd via RDS. [NBR045]

8.7.1.2.1 FI Details

Each FI for which PO Ltd supports NBS Transactions is registered in Reference Data, together with the different schemes that they operate. A scheme defines the set of common characteristics which each service that the FI offers possesses. New Reference Data is required to support this.

8.7.1.2.2 Outlet Groupings

Outlets may be grouped into sets, by defined criteria such as geographical locations or branch types. An Outlet may fall within a number of groupings.

The concept of Outlet groupings extends the current implementation of Outlet and organisational data. It is used for grouping of NBS transactions as described in [NBSMIS]. These groupings will be made available in the Data Warehouse.

8.7.1.2.3 FI Operations

There is a defined unique set of bank operations that will be supported by NBS transactions. A specific operation may be appropriate to one or more FIs

8.7.1.2.4 Authorisation Details

There may be different authorisation routes for a transaction. Each possible transaction is linked to one and only one such route, for example LINK.

In undertaking an operation, the outcome of the transaction (dictated by different authorisation responses) may be designated by a distinct Outcome, recorded on the transaction.

8.7.1.2.5 Verification Details

This defines the procedural process that will be adopted to verify a Customer's identity upon requesting a transaction, for example signature or PIN.

8.7.1.2.6 Method of Entry

Defines the permissible means of initiating a transaction, for example swipe or keyed. Certain tokens could potentially be inhibited from being entered by certain processes, e.g. manually.

8.7.1.2.7 Card Usage Checks

Defines the physical checks that the Counter Clerk should make when presented with a token. These depend on the card scheme, for example check hologram present on card.

The deployment of card checks is a new concept required for NBS and is assumed to be based upon APACS checks. [NBR161]

8.7.1.2.8 Account Details

There are currently no requirements to support account details

8.7.1.2.9 Card Types

Defines the cards that are valid and able to conduct NBS transactions, and the services each supports. This extends the use of tokens already supported within Horizon.

8.7.1.3 Reference Data to Control Application Definitions

The following diagram shows the relationship and navigation between the various entities involved in the model.

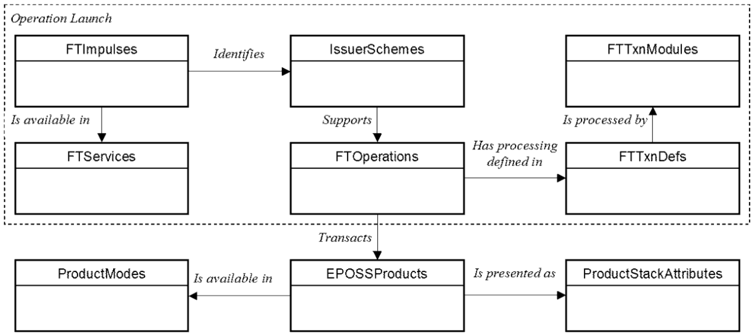


Figure 14 – Reference Data to Support the Framework

The following are the key points that arise from the data model in terms of implications for soft-centred applications such as NBS. The points are expanded on in the following section, which takes a more detailed look at the Data Model.

- All Reference Data Collection objects are temporal
- The application must be prepared for essential Reference Data to be missing (for example following operational errors). In such cases, it needs to fail gracefully with appropriate guidance to the Clerk
- The impulse identification process must restrict its matching to *FTImpulses* Collection objects for the current impulse type, e.g. magnetic card, and for the current service, e.g. NBS. It must support IIN range validation
- The impulse identification process must return issuer scheme, full card image, individual card element values and whether entry is swipe or manual
- Many *FTImpulses* Collection objects may exist for the same *IssuerScheme*. There must be a direct navigation route from the *FTImpulses* Collection to the parent IssuerScheme Collection
- The *FTImpulses* Collection objects identify the application (i.e. NBS or EFTPoS) to be invoked
- Each IssuerScheme may have many *FTOperations*. There must be a direct navigation route from the *IssuerScheme* Collection to the child *FTOperations* Collection objects. A new *IssuerScheme* can be introduced by the distribution of the appropriate Reference Data [NBR024]
- Different *FTOperations* will exist for PIN and signature verification. Business Rules must be defined for:
  - □ Visibility of PIN operations where no PIN Pad exists
  - □ Availability of signature operations where PIN Pads exist

- ▫ Fall back to signature operation where PIN operation is unsuccessful

- The presented list of *FTOperations* for the *IssuerScheme* must exclude operations that are not supported by the current method of card entry (swipe or manual).
- The list of *FTOperations* for the *IssuerScheme* must be presented in the sequence defined by PO Ltd RDS
- PO Ltd RDS will provide Reference Data that defines the operations that they require for each *IssuerScheme*. Pathway Reference Data will define which functions will support the transacting of each operation. Operation definitions will be maintained within RDMC and the system will validate that the PO Ltd Reference Data is consistent with the Operation to be invoked [NBR006]
- The *FTOperations* Collection identifies the function that is to be invoked
- Each *FTOperations* Collection object enables the transacting of a specific product. There must be a direct navigation route from the *FTOperations* Collection to the *EPOSSProducts* Collection
- Currently, all NBS products are deemed to be core – available at all Outlets. However, migration requirements and potential Customer change of requirements demand that the solution supports non-core banking products (i.e. only available at selected Outlets)
- *FTImpulses*, *IssuerScheme* and *FTOperations* Collections are core – distributed to all Outlets. *EPOSSProducts*, *ProductModes* and *ProductStackAttributes* Collections are non-core – distributed only to Outlets where the product is available. The design must cater for:

  - ▫ Selection of an operation where the associated product is non-core and thus not available at the Outlet – an appropriate message should be produced and the operation aborted
  - ▫ Selection of an operation where the associated product is not valid in the current mode (Serve Customer). An appropriate message should be produced and the operation aborted

  However, in both cases such checks should ideally take place before the operation is presented to the clerk and the operation should not be displayed if such checks fail.

8.7.2 Activation Objects

Activation objects, or trigger objects provide the vehicle to 'enable' transactions.

Activation objects provide the ability to ensure dependencies between data flowing along the external interface between PO Ltd's RDS and the NBE are not compromised and as that data is expired.

They are held in the message store as normal Temporal Persistent Objects, thus allowing a timed migration to new versions of an application definition.

Activation Objects will initially be defined as non-core data, allowing PO Ltd to manage Pilot introduction of NBS. However, given the volumes of Reference Data that are likely to be involved, it would be sensible to move these to Core Reference Data for full rollout. [NBR235]

8.8 SERVICE OPERATION AND MANAGEMENT

Operation and Management of the Pathway Reference Data Management Service is encompassed within the OBC Processes.

In addition to changes to the OBC Process within Customer services, service management activities will be defined within Pathway Development.

8.8.1 Service Management of Existing Reference Data

The following diagram represents the service management process for existing Reference Data. The process itself will remain unaltered and may be used for changes to (for example) introduction of a new IIN or changes to the treatment of an existing IIN. [NBR411, NBR416]

However, its interdependence with Service Management of Configuration Data requires to be defined.

The diagram illustrates the joint responsibilities of Pathway and PO Ltd for the release of Reference Data. The diagram does not show the involvement of other Host systems, though Reference Data released to the live estate must be consistent with that used by the other Host systems.

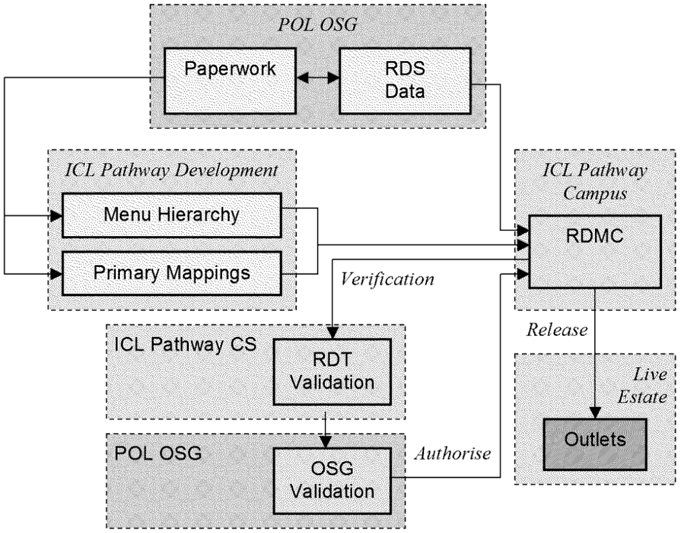


Figure 15 – Current Operational Business Change Processes

8.8.1.1 Pathway Development

Pathway Development is responsible for the production of Type B and C Reference Data using information provided by PO Ltd. This requires some enrichment before that data is passed to the Campus.

8.8.1.2 Pathway Campus

RDMC receives Product Reference Data from PO Ltd's RDS, encompassing product data, item transaction modes, tokens and Cash Account data. Data provided by RDS is received across an existing automated interface and centrally stored within RDMC. [NBR202]

RDMC also receives files from Pathway Development of changes to menu items, primary mappings or system changes.

8.1.1.3 Pathway Customer Services (CS)

CS formulate sets of Business Changes from changes held in RDMC. These are released to Pathway's *Reference Data Team* (RDT) for verification, and then to PO Ltd's OSG for acceptance.

Acceptance is notified to Pathway whereupon Business Changes are released to the Outlet estate and other Host systems.

Chapter 9 - Data Reconciliation Service

9.1 General

This Chapter discusses the *Data Reconciliation Service* (DRS), which is responsible for reconciling all NBS transactions reported to the NBE, and calculating the Settlement sums due to or from each FI.

This is discussed as a separate Chapter in the current SDS (and as a separate SDS in its own right; see [SDSREC] because of the significance of the DRS and its potential use for other applications such as EFTPoS.

9.2 Scope of Data Reconciliation Service

The DRS is an Oracle database application used to reconcile all parties' views on NBS transactions until all are agreed on the outcome. The shaded area in the diagram below describes the scope of the DRS.

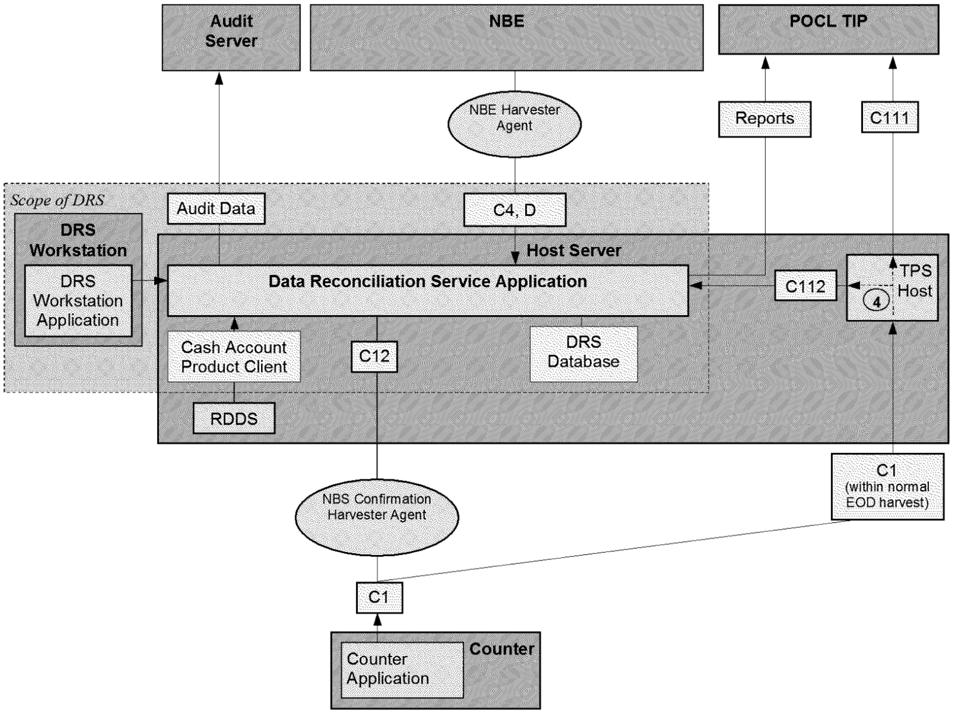


Figure 16 – Scope of Data Reconciliation Service

The DRS Host Application runs on the existing Host Central Servers as a standard Oracle database application. There is sufficient capacity on the Hosts throughout the day to handle the regular calculation and transfer of Settlement data to the NBE.

Running the DRS on the same platform as TPS also simplifies the integration with the data feed to TIP. That is the assumption made in the rest of this Section.

- Input to the DRS comes from the Counters via the *NBS Confirmation Harvester Agent* (see Section 5.7.4) and from the NBE via the NBS Gateway Servers (Section 5.8). These operate by populating a set of Interface Tables in the DRS Database.
- The input to the DRS from TPS will be by allowing DRS a view of TPS tables and is defined in [DRSIFS].
- The reports output to TIP are a set of text files as defined in [DRSREP].
- Reference Data needed to generate the reports will be available by allowing the DRS a view of RDDS tables (See Chapter 8 and [SDSRD])

> *Note that [SDSRD] is significantly out of date and so has been withdrawn.*

- All transactions recorded by the DRS, and all information exchanged with the NBE, will be archived to files that are made available to the Audit Server for auditing [HADDIS]. The reports sent to PO Ltd are also audited before they are deleted from the DRS.

The DRS Workstation Application provides access to the DRS to enable Pathway Customer Services' MSU to resolve exceptions. The requirements for this application are defined in [DRSWS].

9.3 Requirements Summary

The DRS requirements are set out in [SRS] and are summarised below.

The DRS covers both Reconciliation and Settlement Reporting. Reconciliation is handled in the sense of integrity checking and error detection, while Settlement Reporting deals with the reporting required to support FI settlement, including elucidation of timing differences.

9.3.1 Reconciliation Requirements

9.3.1.1 Overview

PO Ltd require an End-to-End Reconciliation service and procedures that will highlight and resolve all reconciliation exceptions.

Reconciliation within the NBE and between the NBE and the FI(s) is the responsibility of the NBE. For this purpose, LINK is a single Client.

9.3.1.2 Branching data-flows

The system will provide the ability to reconcile all branching data-flows. Within the Pathway domain this will be met by the reconciliation of transaction elements arriving at the DRS Host from three sources [NBR212]:

- *NBS Confirmation Agent* (i.e. the [C12] messages generated at the Outlet)
- The NBE (i.e. the [C4], [D] transactions) [NBR294, NBR389]

- TPS Host (i.e. the [C1] messages pickup up by the TPS Harvester and reformatted as a [C112] messages for the DRS Host)

The Confirmations from the three sources are known as Confirmation Sets.

The DRS Host Application will build up a view of each transaction. A logical view of the transaction tables is shown below.

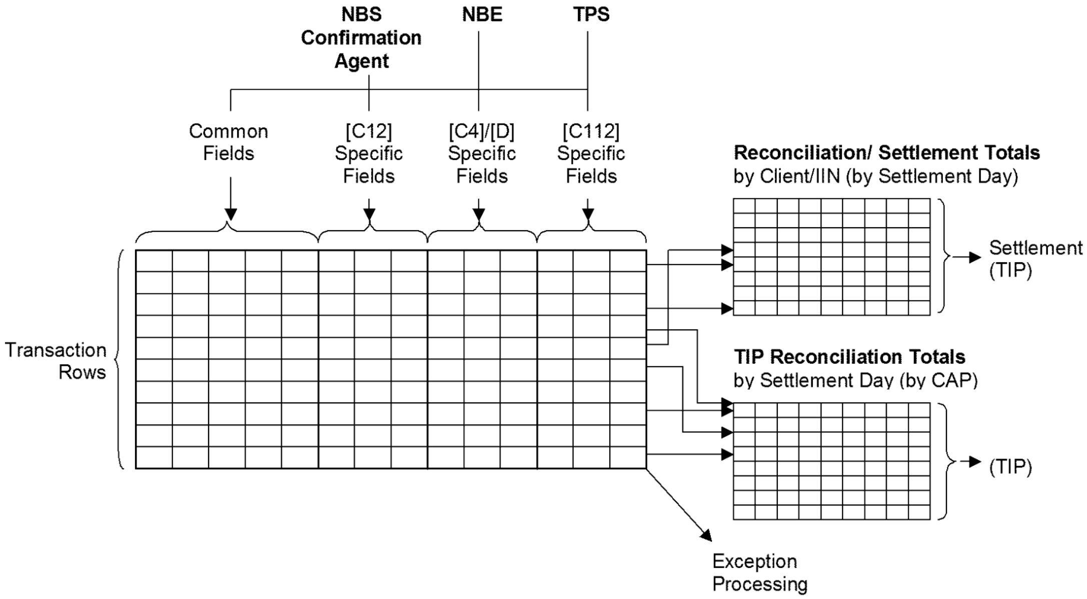


Figure 17 – DRS Logical Transaction Tables

The DRS transaction reconciliation function will monitor the Confirmation sets and alert states which are:

- Intrinsically anomalous, in that their occurrence implies malfunction in the end-to-end system
- Anomalous in that an expected state has persisted for an unexpected duration (e.g. [C4] present but [C112] has not arrived after an abnormal delay). The specification of the "normal" duration of expected states shall be easy to change~~ (probably controlled by Pathway Reference Data)~~.

The expected and exceptional transaction states are set out in the DRS Transaction State Table (see Table 17).

A facility will be provided to enable anomalous states to be flagged as cleared manually, so that they can be dropped from on-going reporting. Audit data relating to the resolution will be captured.

The DRS shall report exceptions requiring human analysis by checking automatically for conditions that would explain the exception as set out in [DRSREP]. For example reporting (to Pathway Customer Service) as requiring immediate analysis the non-arrival of a [C112] from an Outlet known to be non-polling would not be useful and would generate a high volume of exceptions.

There is no requirement for new reporting to relate NBS transactions included in Cash

Accounts to NBS transactions included in the Transaction files sent to TIP, as this will be covered by the existing EPOSS/TIP reconciliation reporting and processes.

9.3.1.3 Complete Processing

The DRS will ensure that all data received is processed. This implies checking for completeness of [C112]/[C2]/[C4](/[D]) sets and reporting exceptions for resolution. [NBR227, NBR229]

It will not attempt to reconcile [R]s with [C]s, as the above checks will identify all errors except the case of an [R] written at the Counter which did not reach the NBE and which, because of some system failure, did not result in a [C0] being written at the Counter. This will be picked up by the transaction recovery application at the user's next login.

9.3.1.4 Reconciliation Issues Notified by the NBE

In addition to reconciliation issues identified within the DRS, data will be received from or via the NBE notifying detected exceptions [NBR278]:

- Within the NBE or
- Between the NBE and FIs (in this context LINK is an FI).

The DRS will receive a [D] message from the NBE when the settlement figure differs from the [C0]/[A], for example because a [C0] was received too late to generate an [E1] to the FI and so settlement has occurred for the original transaction value. The DRS should not regard a transaction as complete until either a [C4] or a [D] has been received from the NBE, or the transaction has been flagged as complete following manual rectification agreed with PO Ltd.

9.3.2 Settlement Reporting

9.3.2.1 Overview

The DRS will send to PO Ltd daily summary reports (as per [DRSREP]) showing, at Client/product/settlement-date level, a summary of the amounts due to each FI. [NBR456]

The Settlement Date will be allocated by the FI (or failing that the NBE) and included in both Authorisations and Confirmations. The [C4] could contain a Settlement Date different from the [R]/[A]; for example if settlement was originally made without a [C2] and subsequently successfully modified to zero (using [E1]/[E2]) during the next Posting Day on receipt by the NBE of a [C2](decline).

Pathway notes that there is no requirement to list normal transactions (i.e. those which progress to a normal state as set out in the State Table) in the settlement reports. Inclusion in the summary figures is sufficient.

Abnormal transactions, whether identified by the DRS or notified to the DRS by the NBE, will be detailed in the reporting if impinging on Settlement or Reconciliation.

9.3.2.2 Detailed Requirements

Two sets of data need to be sent to the TIP gateway for accounting purposes:

- Reporting to support settlement with FIs
- Reporting to support accounting within PO Ltd

9.3.2.1.1 Data to Support Settlement with Fis

The settlement feed from the DRS to TIP is the primary feed of settlement data to PO Ltd. An exception is that transactions authorised via LINK will be settled by LINK, and in this case, PO Ltd will use the DRS Host settlement feed to verify the settlement data provided by LINK.

It is possible in the future that a particular FI may have both transactions that are authorised (and hence settled) by LINK, and transactions that are authorised directly. These would need accounting for separately in the settlement feed to PO Ltd, and posting to different Cash Account lines. It could only be accomplished by using a different Client ID for the two types.

It is noted that this can vary from FI to FI whether the basis of settlement is the FI Settlement Date or Post Office Settlement Date. However, the DRS does not need to understand this distinction, as the NBE will allocate a Settlement Date if not specified by the FI. For FIs settled via LINK, settlement is based on the LINK day, which closes at about 20:00. LINK will settle on the basis of an agreed view between it and the FIs of [R]/[A] pairs as modified by [C2] messages received before cut-off. Receipt of a [C4] from the NBE confirms to the DRS that the transaction is aligned with the FI and has been (or will be) included in Settlement for the day. In addition, the NBE will attempt to Reverse transactions for which it receives a [C2] message. If the settlement fails, the result will be returned as a [D] message. If it succeeds, the relevant [C4] message will be updated accordingly.

9.3.2.1.2 Data to Support Accounting Within PO Ltd

TIP needs to relate transactions settled to transactions taken into account via Cash Accounts. [NBR230]

PO Ltd needs reporting which will reconcile the timing differences between two different processes:

- PO Ltd's FI transaction ledgers will be fed from the values recorded on the Cash Account. Ledgering will be at FI level for deposits and withdrawals. For FIs using LINK, ledgering will be against a single FI, i.e. LINK. This will require appropriate setting up of Cash Account lines and Cash Account mappings via Reference Data (which is a PO Ltd responsibility).
- Settlement, however, will be based on the value of transactions 'Authorised' within an agreed settlement day (but ultimately reconciled and/or adjusted to Completed transactions at the Outlet). Settlement is a PO Ltd responsibility.

Reporting is required to identify, by CAP, for each Settlement day, the transaction total successfully delivered to TIP via Cash Accounts and the transaction total not yet successfully delivered to TIP via Cash Accounts. This report is required once a week, on a day to be defined by PO Ltd. As the CAP of a transaction will not be known by the DRS until the [C112] is received from the TPS Host (which derives CAP from EoD markers and adds it to the message) some transactions on the report will be classified as having no known CAP. These will be reclassified when the [C112] arrives.

9.3.3 DRS Transaction State Table

This Table is derived from [SRS] and defines the transaction state transitions to be handled within DRS.

Notes:

- Expected normal progression for a transaction is to move in order through states 1, 2, and 3
- In any state a value difference between [C112]/[C2]/[C4] would imply a system malfunction
- All records will be checked for corruption on arrival
- Arrival of any duplicate record will require appropriate investigation
- [C112] messages arrive only once per day, after TIP harvest. It is therefore only useful to investigate missing [C112] messages if an EoD marker for the relevant day has been found – i.e. the office is "polling"

In the following table, states that are not expected to arise for NBS with the abandonment of the NBE [S] flow are highlighted with a yellow background, like this. These states will be implemented within DRS to avoid major delays caused by making radical changes to the DRS at this point, and may be used by other applications such as EFTPoS.

State No.	Input received from			Implication and/or Action
	Confirmation Agent	NBE	TPS Host	
1	C12	-	-	This is normally the first state to be entered. This state signifies a transaction that has not been confirmed by the Banking Host. The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in. [RECIM]. Will move to state: 2 if NBE sends a [C4] message 6 after match with [C112] following TPS Harvest 10 if NBE sends an [S] message 13 if NBE sends a [D] message
2	C12	C4	-	This state signifies a transaction that has been confirmed by the Banking Host. The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. . This is an illegal state for EFTPoS. Will move to state: 3 after match with [C112] following TPS Harvest
3	C12	C4	C112	This is a normal final state for NBS. This state signifies a transaction that has been confirmed by the Banking Host. The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. The transaction will be archived after 3 months. This is an illegal state for EFTPoS.
4	-	C4	-	This state signifies a transaction that has been confirmed by the Banking Host. The transaction has not been harvested to TIP, and has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for EFTPoS. Will move to state: 2 if match with [C12] is subsequently made 7 after match with [C112] following TPS Harvest

5	-	-	C112	This state signifies a transaction that has not been confirmed by the Banking Host. The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. Will move to state: 6 if DRS receives a [C12] message 7 if NBE sends an [C4] message 9 if NBE sends an [S] message 14 if NBE sends a [D] message
6	C12	-	C112	This state signifies a transaction that has not been confirmed by the Banking Host. The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. Will move to state: 3 if NBE sends a [C4] message 11 if NBE sends an [S] message 15 if NBE sends a [D] message
7	-	C4	C112	This state signifies a transaction that has been confirmed by the Banking Host. The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state when it is listed individually on the reconciliation exception report [DRSREP]. This is an illegal state for EFTPoS. Will move to state: 3 if match with [C12] is subsequently made
8		S		This state signifies a transaction where the Banking Host has reported an expected future settlement position. The transaction has not been harvested to TIP, and has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state when it is listed individually on the reconciliation exception report [DRSREP]. This is an illegal state for both NBS and EFTPoS. Will move to state: 9 after match with [C112] following TPS Harvest 10 after match with [C12] following Confirmation Harvest 16 if NBE sends a [C4] message 20 if NBE sends a [D] message
9		S	C112	This state signifies a transaction where the Banking Host has reported an expected future settlement position. The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for both NBS and EFTPoS. Will move to state: 11 after match with [C12] following Confirmation Harvest 17 if NBE sends a [C4] message 21 if NBE sends a [D] message
10	C12	S		This state signifies a transaction where the Banking Host has reported an expected future settlement position. The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. Will move to state: 11 after match with [C112] following TPS Harvest 18 if NBE sends a [C4] message 22 if NBE sends a [D] message
11	C12	S	C112	This state signifies a transaction where the Banking Host has reported an expected future settlement position. The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM] Will move to state: 19 if NBE sends a [C4] message 23 if NBE sends a [D] message

12		D		This state signifies a transaction where the Banking Host has not been able to agree settlement with the client The transaction has not been harvested to TIP, and has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for EFTPoS. Will move to state: 13 if match with [C12] is subsequently made 14 after match with [C112] following TPS Harvest
13	C12	D		This state signifies a transaction where the Banking Host has not been able to agree settlement with the client The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for EFTPoS. Will move to state: 15 after match with [C112] following TPS Harvest
14		D	C112	This state signifies a transaction where the Banking Host has not been able to agree settlement with the client The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for EFTPoS Will move to state: 15 if match with [C12] is subsequently made
15	C12	D	C112	This state signifies a transaction where the Banking Host has not been able to agree settlement with the client The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for EFTPoS
16		S/C4		This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host has confirmed the settlement. The transaction has not been harvested to TIP, and has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for both NBS and EFTPoS Will move to state: 17 after match with [C112] following TPS Harvest 18 if match with [C12] is subsequently made
17		S/C4	C112	This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host has confirmed the settlement. The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for both NBS and EFTPoS Will move to state: 19 if match with [C12] is subsequently made
18	C12	S/C4		This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host has confirmed the settlement. The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for NBS. Will move to state: 19 after match with [C112] following TPS Harvest
19	C12	S/C4	C112	This is a normal final state for EFTPoS. This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host has confirmed the settlement. The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. The transaction will be archived after 3 months. This is an illegal state for NBS.

20		S/D		This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host notified the DRS that actual settlement did not match the expected position. The transaction has not been harvested to TIP, and has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for both NBS and EFTPoS. Will move to state: 21 after match with [C112] following TPS Harvest 22 if match with [C12] is subsequently made
21		S/D	C112	This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host notified the DRS that actual settlement did not match the expected position. The transaction has been harvested to TIP, but has not been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for both NBS and EFTPoS. Will move to state: 23 if match with [C12] is subsequently made
22	C12	S/D		This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host notified the DRS that actual settlement did not match the expected position. The transaction has not been harvested to TIP, but has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for NBS. Will move to state: 23 after match with [C112] following TPS Harvest
23	C2	S/D	C112	This state signifies a transaction where the Banking Host has reported an expected future settlement position. Subsequently, the Banking Host notified the DRS that actual settlement did not match the expected position. The transaction has been harvested to TIP, and has been harvested by the Confirmation Harvester. Investigation is required for a transaction in this state as defined in [RECIM]. This is an illegal state for NBS.

Table 17 – DRS State Transition Table

A number of Exception states will be used to signify a variety of errors including duplicate transactions, non-matching values etc.

A corruption of a transaction identifier could prevent a match between [C112], [C12], [C4], or [D] being recognised, in which case orphaned transaction elements will exist.

9.4 DRS Design Principles

The DRS will be an implementation of the Transaction State Table diagram above. Each transaction will have its own state history, showing when it entered each state as defined by the state table.

It is the nature of reconciliation that all transactions, including exceptions and duplicates, must be reported and accounted for. Exception and duplicate transactions are not exempt from this. By design, the DRS will receive exactly one copy of each and every Transaction Element generated by the Counter and the NBE (formatted for the DRS as [C112], [C12], [C4] and [D]). All duplicates will be treated as exceptions for MSU resolution as they will have been generated by some system fault.

Data flow splits will be avoided to keep the reconciliation as simple as possible.

Making changes to the data in long-term storage should be avoided so as to minimise *Symmetrix Remote Data Facility* (SRDF) traffic.

All stored transactions will have read-only access to the transaction content. Only audited DRS transaction state change will be allowable.

All modules on the DRS Host will be able to be re-started to provide failure recovery.

Any timestamps generated by the DRS will be recorded in *Universal Coordinated Time* (UTC) with a local time offset. The DRS will calculate its own offset for any timestamp it generates. Timestamps generated by the DRS that appear on human interface outputs, e.g. report production date & time, will be presented in local time. The DRS will not alter timestamps generated by any other components of the NBS, e.g. timestamps on transactions will remain unchanged.

Day to day operations will be scheduled by Maestro.

Application development will follow guidelines laid down in [HADDIS].

The DRS database design will be defined in Designer 6i.

9.5 SYSTEM COMPONENTS

9.5.1 Application Components

There are two application components:

- The DRS Host Application, which
  - Reports on Reconciliation and Settlement between major components of NBS
  - Makes data available to the audit server
- The DRS Workstation Application, which provides MSU with access to the DRS Host for exception resolution.

9.5.1.1 The Data Reconciliation Host Application

The DRS must reconcile and report on:

- [C12]s
- [C4] and [D] messages sent to it from the NBE
- [C112] messages viewed in the TPS Database
- All reconciliation exceptions

To achieve this, the DRS must have all these Transaction Elements available in Reconciliation Tables.

- The DRS must ensure that all data that it processes and all data that passes from the DRS to PO Ltd~~, and all data that passes between the DRS and the NBE~~ is made available to the Audit Server.

An overview of the DRS architecture is given below.

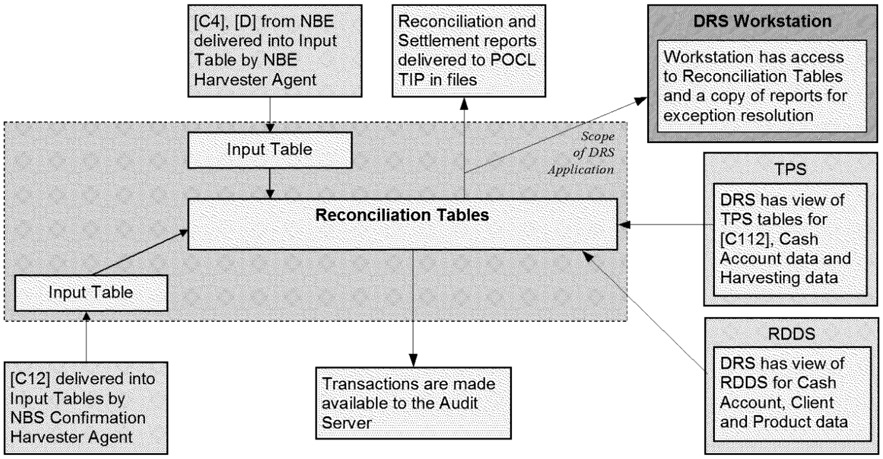

[C4], [D] from NBE delivered into Input Table by NBE Harvester Agent
Reconciliation and Settlement reports delivered to POCL TIP in files
DRS Workstation
Workstation has access to Reconciliation Tables and a copy of reports for exception resolution
Input Table
Scope of DRS Application
Reconciliation Tables
TPS
DRS has view of TPS tables for [C112], Cash Account data and Harvesting data
Input Table
RDDS
DRS has view of RDDS for Cash Account, Client and Product data
[C12] delivered into Input Tables by NBS Confirmation Harvester Agent
Transactions are made available to the Audit Server

Figure 18 – DRS Application Architecture

[C12] messages will be made available to the DRS in input tables loaded using an Oracle stored object as defined in [SDSAPP]. The DRS input tables will not be constrained, thus allowing the Agents to load data regardless of its quality. The Agent will be able to assign an error code and text to any [C12] message in the input tables to advise the DRS of any error that the Agent found. The DRS will copy every [C12] from the input tables to the reconciliation tables. This will take place in near real time, with input table extraction and reconciliation table loading expected to take place in direct response to Agent calling.

The [C4] and [D] messages arriving from the NBE will be controlled the same way as the [C12]s arriving from the Counter, with the DRS application moving [C4] and [D]s from the input tables to the reconciliation tables. Again, the Loader will be able to supply an error code and text for any message for which it detects an error.

~~To avoid the need to purchase disk storage for the Agents with the associated complexities, the DRS Database is used to store the audit records for the [C4] and [D] interface. The audit record will be written (as an unaltered text string) along with the actual data into the interface table of the DRS application. This is a single commit, so there is no risk of data not being audited due to failures. The audit record will be treated as an interface table and transferred to the Audit Server as the table is purged (expected nightly). By default, this will be written in the standard defined by [HADDIS]. It will need to be pulled back into a database to be read.~~

There is no requirement for the DRS to provide functionality to support auditing of DCS related [C4] and [D] messages.

TPS will avoid splitting the data flow of the [C1]s en route from the Counter to TIP (as [C111]s) by providing the DRS with a view of its tables (as [C112]s). The harvesting information necessary for the reconciliation and settlement reports is provided to the DRS in the same way. [DRSIFS] will provide the details. Once a day, after TPS harvesting, the DRS application will interrogate the TPS tables for [C112]s thus making them available to the reconciliation tables.

The reconciliation and settlement reports will be generated once every day in text file format and made available on the PO Ltd TIP gateway and to the MSU workstation by 08:00 following the previous day's processing. The reports will be held on the DRS for ten days, and will be made available to the Audit Server before deletion. The specification for the reports is given in [DRSREP]. Note that some reports will be repeated for each Routing Gateway for each Transaction Type grouping. Where this is the case, there must be a set of reports to provide for transactions for which the Routing Gateway and/or Transaction Type is not known. No report will mix currency, so if ever the transactions selected to appear on a set of reports are not of a single currency, then a separate set of reports will be produced for each currency. All the amounts in a single transaction will always use the same currency.

If the amount field in a transaction element contains a corrupt (non numeric) value then that value will be treated as a zero for any reports that use an aggregate of the amounts.

The Cash Account Week, Client, and Product information necessary for the reconciliation and settlement reports is provided to the DRS by a view of RDDS tables [SDSRD].

> *Note that [SDSRD] is significantly out of date and so has been withdrawn. However the information should be in the RDDS HLD.*

The internal working of the DRS Reconciliation Tables will be an implementation of the state table given in Table 17.

						When								
						C112	C12	C4	D	S				
	Prevalidation					Arrives, then: pre-validate								
	On Incomplete/Corrupt error go to:					E27	E28	E29	E30	E31				
											Validate on entry to State (# means 'not equal to')			
	State	Conf Agent	NBE	TPS		When valid, go to State:					Amount:Action	Amount:Action	Amount:Action	Settlement Date:Action
Start	0					5	1	4	12	8				
	1	C12				6	E02	2	13	10				
	2	C12	C4			3	E02	E04	E09	E06	C12#C4:E23			C4 SettleDt # RecDt:E39
Final	3	C12	C4	C112		E10	E11	E12	E13	E14	C112#C12:E20	C112#C4:E21		C4 SettleDt # RecDt:E39
	4		C4			7	2	E04	E09	E06				
	5			C112		E01	6	7	14	9				
	6	C12		C112		E01	E02	3	15	11	C112#C12:E20			
	7		C4	C112		E01	3	E04	E09	E06	C112'C4:E21			C4 SettleDt # RecDt:E39
	8		S			9	10	16	20	E05				S SettleDt # RecDt:E39
	9		S	C112		E01	11	17	21	E05	C112#S & C112#0:E22			S SettleDt # RecDt:E39
	10	C12	S			11	E02	18	22	E05	C12#S & C12#0:E24			S SettleDt # RecDt:E39
	11	C12	S	C112		E01	E02	19	23	E05	C112#C12:E20	C12#S & C12#0:E24		S SettleDt # RecDt:E39
	12		D			14	13	E08	E03	E07				D SettleDt # RecDt:E39
	13	C12	D			15	E02	E08	E03	E07	C12#D(C12):E26			D SettleDt # RecDt:E39
	14		D	C112		E01	15	E08	E03	E07	C112#D(C12):E25			D SettleDt # RecDt:E39
	15	C12	D	C112		E01	E02	E08	E03	E07	C112#C12:E20	C112#D(C12):E25		D SettleDt # RecDt:E39
	16		S/C4			17	18	E04	E09	E05	C4#S & C4#0:E32			S or C4 SettleDt # RecDt:E39
	17		S/C4	C112		E01	19	E04	E09	E05	C112#C4:E21	C4#S & C4#0:E32		S or C4 SettleDt # RecDt:E39
	18	C12	S/C4			19	E02	E04	E09	E05	C12#C4:E23	C4#S & C4#0:E32		S or C4 SettleDt # RecDt:E39
Final	19	C12	S/C4	C112		E10	E11	E12	E13	E14	C112#C12:E20	C12#C4:E23	C4#S & C4#0:E32	S or C4 SettleDt # RecDt:E39
	20		S/D			21	22	E08	E03	E05	D(A)#S:E33			S or D SettleDt # RecDt:E39
	21		S/D	C112		E01	23	E08	E03	E05	C112#S & C112#0:E22	D(A)#S:E33		S or D SettleDt # RecDt:E39
	22	C12	S/D			23	E02	E08	E03	E05	C12#S & C12#0:E24	D(A)#S:E33		S or D SettleDt # RecDt:E39
	23	C12	S/D	C112		E01	E02	E08	E03	E05	C112#C12:E20	C112#S & C112#0:E22	D(A)#S:E33	S or D SettleDt # RecDt:E39

		Exception States
	E01	Additional C112
	E02	Additional C12
	E03	Additional D
	E04	Additional C4
	E05	Additional S
	E06	S after C4

	E07	S after D									
	E08	C4 after D									
	E09	D after C4									
	E10	C112 after final state									
	E11	C12 after final state									
	E12	C4 after final state									
	E13	D after final state									
	E20	Amount of C112#C12									
	E21	Amount of C112#C4									
	E22	Amount of C112#S & C112#0									
	E23	Amount of C12#C4									
	E24	Amount of C12#S & C12#0									
	E25	Amount of C112#D									
	E26	Amount of C12#D									
	E27	Incomplete/Corrupt C112									
	E28	Incomplete/Corrupt C12									
	E29	Incomplete/Corrupt C4									
	E30	Incomplete/Corrupt D									
	E31	Incomplete/Corrupt S									
	E32	Amount of C4#S & C4#0									
	E33	Amount of D#S									
	E34	C112 arrived after state F99									
	E35	C12 arrived after state F99									
	E36	C4 arrived after state F99									
	E37	D arrived after state F99									
	E38	S arrived after state F99									
	E39	Settlement Date # Reconciliation Date									
Final	F99	MSU Resolved		E34	E35	E35	E36	E37	E38		

Table 18 – DRS State Transition Table Implementation

Each transaction in the reconciliation tables will consist of the elements [C112], [C12], [C4] or [D], and will have recorded on it its full transaction state history including a date and time stamp for each state entered.

The normal course of operation is that a [C12] will arrive and cause a new transaction to be recorded. The state will be set to 1. Some time later, the corresponding [C4] will arrive from the NBE. The [C4] will be placed with the [C12] as part of the same transaction, and the state will be set to 2. After TPS harvesting, the [C112] will be available to the DRS Host Application, and the state will move to 3. This is the final state, and signifies that all elements of the transaction have arrived. The reconciliation and settlement reports will reflect this. The state history will show states 1, 2, 3 each with a date and timestamp as to when that state was set.

On arrival of each transaction element ([C112], [C12], [C4] or [D]) in the input tables, the transaction element will be pre-validated to check it is complete and not corrupt. The validation will be applied according to the Table below.

	C112	C12	C4	S	D
Has Agent supplied an error code?	-	Yes: Fail No: Pass	Yes: Fail No: Pass	Yes: Fail No: Pass	Yes: Fail No: Pass
Are Amount(s) numeric or Null?	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail
Is Settlement Date present?	-	-	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail
If present, is Settlement Date a valid date format?	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail	Yes: Pass No: Fail

Table 19 – DRS Transaction Element Validation

Validation will stop at the first failure, as it is not necessary to find every fault in a transaction element.

A search of the reconciliation tables will try to find other Transaction Elements with the same primary key for the incoming Transaction Element. If a match is found, the new element will be added to the matched transaction, otherwise the new Transaction Element will be added to the table as a new transaction. ~~The search will always look for a matching transaction in states 1 to 23, E06 to E09, E13 to E14, E18, E20 to E39, and F99 before progressing to the exception states E01 to E05, E10 to E12, E15 to E17, and E19. Thus, if a duplicate transaction~~ If a transaction with a duplicate primary exists, the original copy will progress in preference.

If ever a Transaction Element arrives that has a duplicate primary key of a Transaction Element that is already in the reconciliation tables, then that new element will be entered as a new transaction with ~~the appropriate~~ an exception state ~~(E01 to E05, E10 to E12, E15 to E17, or E19)~~ being set as determined by the state table. The already existing element / transaction will remain unaltered.

If the pre-validation result is ‘Pass’, the state of the transaction will be set according to the state table above.

If pre-validation fails, the state of the transaction will be set to the appropriate exception state E27 to E31. Whenever states E27 to E31 are used, a suitable error code and text will be associated with the transaction to indicate the reason for that state being set. If an Agent has supplied a code and text, then that will be used.

Every time a transaction state (1 to 23) is set, value checking will take place as defined in the state table above. Value checking will take place on the amount and settlement date. For value checking on the amount:

- The [D] has an amount authorised value and an amount confirmed value described in the state table as [D](A) and [D](C12) respectively.
- The use of 0 in the state table is used to mean either zero or null. E.g. ‘C112#0’ is to be read ‘[C112] is not {zero or Null}’ i.e. ‘[C112] is not zero and [C112] is not Null’.
- The [C12] has two amounts associated with it, an Amount Confirmed (to be passed to the NBE), and an EPOSS amount. It is the Amount Confirmed that will be used.
- The [C112] has two amounts associated with it, an Amount Confirmed (to be passed to the NBE), and an EPOSS amount. It is the EPOSS Amount that will be used.

~~The Reconciliation Date is the date attributed to a transaction to allow POL to reconcile. It will be set to the first available Settlement Date from the transaction elements ([C112], [C12], [C4], [D]) that make up that transaction. If no Settlement Date is available, the Reconciliation Date will be set to the processing date that the DRS first recorded any element of the transaction. If a Settlement Date subsequently becomes available, the first available Settlement Date will replace the processing date. However, once a transaction has been accounted for on a reconciliation report, the Reconciliation Date will never change. It is therefore possible that a Settlement Date will differ from the Reconciliation Date. If this is the case, the transaction is moved on to an exception state.~~

The exception state will be set as defined in the state table if any value checking fails.

The Reconciliation Date is the date attributed to a transaction to allow PO Ltd to reconcile. It will be set to the first available Bank Settlement Date from the transaction elements ([C112], [C12], [C4], [D]) that make up that transaction. If no Bank Settlement Date is available, the Reconciliation Date will be set to the processing date that the DRS first recorded any element of the transaction. If a Bank Settlement Date subsequently becomes available, the first available Bank Settlement Date will replace the processing date. However, once a transaction has been accounted for on a reconciliation report, the Reconciliation Date will never change.

Transactions together with the full transaction state history will be held in the transaction tables for 90 days from the Receipt Date, after which time they will be made available to the Audit Server before deletion from the DRS. To make provision for any future changes, the 90 day figure will be configurable.

9.5.1.2 The Data Reconciliation Workstation Application

The DRS Workstation Application provides MSU with secure access to view the suite of NBS reconciliation reports and to allow real time processing of NBS exceptions. It will be a new application on an existing platform (the MIS Client PC). [NBR042]

It will allow MSU to:

- Select, view, format, print, and transfer to a floppy disk or *Compact Disk* (CD) the reconciliation and settlement reports for up to 10 days after their generation. The standard MS Office tool set will be provided to achieve this.

  The tool set will allow MSU to adjust the reports, as they are a local copy only. This facility may be used, for example, following investigation into system exceptions and or failure. MSU will be responsible archiving any report they produce in line with [SRS]

- Select, view, print and transfer to a local text file transactions based on an entered criteria so that MSU may generate a BIMS report. This facility will be available for transactions up to three months after their generation. The criteria are defined in [DRSWS]. Once transactions are in a local text file, the same facilities will be available as for the reports. When a transaction is viewed, printed or copied into a local text file, there will be an option to include the full transaction state history

- Move a transaction from its current state to state F99 so that the transaction is no longer reported as an exception. Any such state change will be recorded on the transaction along with date and time stamp to maintain the full transaction state history. When any transaction is moved to state F99, the user id of the DRS workstation operator will be recorded in the state history to maintain traceable accountability.

- MSU may cause the state to change as defined in the Table below.

						MSU Action
	State	Counter	NBE	TPS		Set state to
Start	0					-
	1	C12				F99
	2	C12	C4			F99
Final	3	C12	C4	C112		-
	4		C4			F99
	5			C112		F99
	6	C12		C112		F99
	7		C4	C112		F99

	8		S			F99
	9		S	C112		F99
	10	C12	S			F99
	11	C12	S	C112		F99
	12		D			F99
	13	C12	D			F99
	14		D	C112		F99
	15	C12	D	C112		F99
	16		S/C4			F99
	17		S/C4	C112		F99
	18	C12	S/C4			F99
Final	19	C12	S/C4	C112		-
	20		S/D			F99
	21		S/D	C112		F99
	22	C12	S/D			F99
	23	C12	S/D	C112		F99
	Exception states					
	E01 to E38					F99
Final	F99	MSU resolved				-

Table 20 – MSU Action State Table

The workstation will not allow any part of any transaction in the DRS Reconciliation Tables to be generated or updated other than the current state as defined by the table above.

Chapter 10 - Network Infrastructure

10.1 GENERAL

This Chapter covers the enhancements needed to the Horizon network to support the known business developments including NBS.

10.2 REQUIREMENTS SUMMARY

10.2.1 ISDN Network

The current Horizon network design is predicated on a predominant network usage pattern of intermittent short calls carrying transaction traffic in batches from approximately 18,000 Outlets to the two Campuses. This model of operation (ISDN, both way dial on demand) is generally well suited to this requirement. There is a small proportion (5% of all calls) where a real-time response is required, but the network can handle this.

A number of major new PO Ltd applications will force a significant change in this usage pattern.

- NBS will generate many more interactive short calls. This will result in several potential issues:
    - The call rate across the entire network will increase substantially. Utilisation of the central network components (ISDN *Primary Rate Interface* (PRI) connections and Routers) will increase substantially, requiring significant investment
    - There is limited space available in the Horizon Campuses to contain any additional equipment
- EFTPoS and other new applications (e.g. mobile phone top-ups) will have a major impact on Network requirements, with respect to on-line transactions.

The main implication, if the network infrastructure remains unaltered, is that network usage based on a metered tariff will be too expensive, with respect to additional equipment required (Pathway responsibility) and the actual costs of the metered NBS calls (PO Ltd responsibility).

10.2.2 Communication with NBE

A high-bandwidth network is required to link the Horizon Campuses to the NBE sites at IBM Warwick and Greenford.

10.3 ISDN Network

Pathway has investigated a number of options to improve the Horizon network capability. These cover the requirements of both NBS and EFTPoS, and the potential for the Horizon system to support the YG programme in a cost effective manner. The chosen approach is to introduce a data network service using an "always-on" connection over the existing ISDN2e service at a fixed usage tariff.

10.3.1 Network Congestion

There is evidence of network congestion within the ISDN network in certain areas at certain times. One effect of this congestion is to cause Outlets to fail to connect to the Campus when a call becomes due. This is not particularly significant where the traffic is batch-based, but will have a significant impact on the availability of NBS, which relies on real-time traffic.

10.3.1.1 Factors Limiting Network Availability

The factors that limit the service availability provided by ISDN include the following.

- *Call set-up failures due to congestion*. Successful call set-up requires that resources exist in the *British Telecom* (BT) and Energis networks
- *Failure detection for long-term outages***.** One problem with a switched ISDN network is that the service availability cannot be monitored proactively. It is only the attempt at a WAN connection that detects a failure in ISDN Service. But with a fixed network (where a data path is always expected to be available), a Network Management function can be used to detect a lack of network service and initiate repair
- *Call set-up failure due to Transient problems and handling these failures***.** For an ISDN call set up to result in a usable data path requires that a number of layered services are available

10.3.1.2 Availability Improvement Options

A number of options are available to improve the overall network availability. These are not mutually exclusive, and in practice, the most cost-effective solution is a combination of approaches.

- *Differentiated service levels for Customer transactions*
- *Permanent ISDN Connections based on move to non-metered access*
- *Differentiated service provider agreements*
- *Dual network technology in Outlets requiring high availability***.** For example, use of ISDN and Satellite
- *Use of Managed Router type functionality at Outlet*

A number of the above options revolve around the use of a fixed price unmetered data network service. OFTEL lay down the rules and charging arrangements for these, under the heading of *Fixed Rate Internet Access Call Origination* (FRIACO).

10.3.1.3 Asymmetric Networks

A data network is *asymmetrical*, in that calls can only be originated by the Outlet, not by the Campus. There are a number of cases where the Campus needs to make a call to the Outlet. Some of these can be modified such that the Outlet always makes the call. This is especially true of permanent connections, where the call can be originated by the Outlet and immediately reconnected if it is ever lost.

In other cases, forcing the call to originate at the Outlet is more difficult and involves significant development. As a last resort, it would always be necessary to retain a voice network capability to connect to any Outlet for support reasons.

However, despite these issues, there are significant benefits to using a FRIACO service for at least a portion of the Outlets. The most significant is that the line between the Outlet and the Campus can be left connected permanently, without substantial financial penalty, where the business needs can justify this.

- One option is to provide permanent connections to all 18,000 Outlets. In the event of the ISDN call "dropping out", the Outlet will attempt to reconnect. The benefit of this arrangement is that it saves both the call set-up time (around three seconds) and the chance that a call request will fail
- The second option is to use a permanent connection to around 10,000 Outlets, with a FRIACO dial-in service for the remainder
- The third is the same except that the FRIACO dial-in service is replaced by the existing ISDN dial-in service.
- There is a significant cost advantage in not having the Outlets permanently connected for 24 hours a day. Thus, a fourth option is a hybrid approach based on having them connected during the core business day plus an overnight slot for software and Reference Data distribution.

For Outlets where ISDN is unavailable, and which are currently connected by satellite communications (*Very Small Aperture Terminal*, or VSAT), the network connection will remain the same. However, the VSAT connected Outlets may be configured as Riposte permanent neighbours at some stage in the future.

Outlets in the Kingston Telecommunications area (Hull), where no FRIACO service is available, will continue to utilise metered ISDN for calls to the Campus.

The choice of Outlets to be permanently connected can be based on either the size of the Outlet or the level of business transacted, if this is predictable in advance. The latter option is preferred because the amount of business transacted in an Outlet is not necessarily proportional to the number of Counters. In either scenario, the network type (permanent or dial-in) will be configurable by Pathway, within the total number of FRIACO ports purchased. The decision on which Outlets are 'permanent connected' is based on a number of factors:

- Volume of traffic through an Outlet which at this point in time can only be based on current traffic and expected Network Banking traffic
- Number of Counter positions and hence the potential increase in the volume of Network Banking traffic
- PO Ltd nominated Outlets for whatever reason

In is envisaged that a quarterly review will be held between Pathway and PO Ltd to assess the mix of permanent and dial-in Outlets, and to agree on any modifications to the mix of permanent and dial-in connected Outlets.

However, if only a portion of the Outlets are permanently connected, then:

- The response time at some Outlets would be longer because of the connection time (dial-in).
- Different performance SLAs will be required for the various types of connection

10.3.2 Required Service Characteristics

The characteristics of the required service are as follows.

- *Outbound Call Mechanism* – It is necessary that all Outlets can be called from the Campus. Even in the case where all 18,000 Outlets are permanently connected, there is still a requirement for outbound calling for diagnostic reasons, for example if communication is lost. Outbound dialling should not take place to an Outlet if an inbound call from that Outlet is in progress
- *Fixed IP address* – Currently each Outlet has a fixed IP address for its ISDN interface. Moving away from this scheme would be highly disruptive to many aspects of the Outlet-to-Campus communication mechanisms
- *Fixed charge per 64 Kbps port*, allowing permanent connections where required at busy Outlets
- *Access from existing ISDN2e service at Outlets*, providing end-end 64 Kbps performance. The target throughput for a permanent 64 Kbps circuit will be defined and expressed as the average throughput over an hour period as well as the peak 5 minutes within the hour
- *National coverage* to support usage from any of the existing ISDN2e connections. A minimum coverage of 95% of all Outlets is required
- *Delivery to Pathway Campuses* at Wigan and Bootle over a fibre infrastructure. The presentation to the Campuses must not interfere with end-end IP Layer 3 and associated *Virtual Private Network* (VPN)
- *Resilient dial in* – alternative routing for avoiding single points of failure in Network infrastructure
- *Ease of migration* – an efficient and reversible mechanism for moving Outlets between different Network service classes (voice, dial-in, permanent)
- *Scalability* – the Network must be demonstrated to be scalable. This is in order to accommodated increased usage, for example more data throughput and/or more ISDN calls per second
- *Network management to deliver an agreed QoS*. For example, a QoS on ISDN dialling reaching dial ports will be required
- *Different QoS options at different times of the day*.

10.3.3 Network Solution Issues

There are a number of issues with each of the options discussed above. They can be summarised as follows.

- Voice network Dial-up and Leased Line connections will require extensive additional equipment in the Campuses
- A technology refresh exercise will be undertaken at both Campuses to provide additional space for NBS equipment.
- The FRIACO service provided by Energis will utilise the existing standard ISDN2e connection from the Outlets to the BT *Digital Local Exchange* (DLE) through which *all* FRIACO traffic flows. There is one or more 2 Mbps links from each DLE to the Energis network. There are around 750 DLEs in the UK, and hence in many areas, Outlet traffic would take a significant part of the available bandwidth of a single connection

The chosen solution is based around the use of FRIACO permanent connections for a large number of Outlets, with use of the existing (metered) dial-up network for the remaining Outlets.

10.3.4 Network Technology Terminology

10.3.4.1 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.

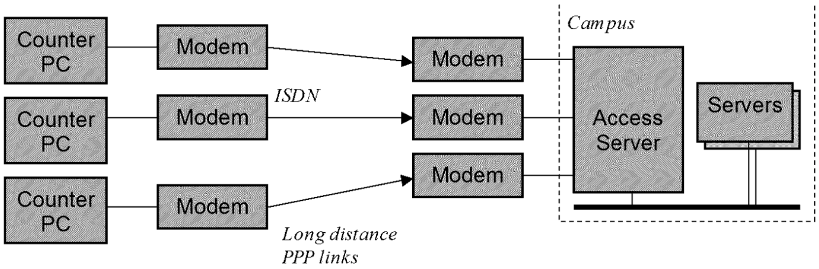


Figure 19 – Remote Access Without Point-to Point Tunnelling Protocol (PPTP)

With PPTP, it connects instead with a local *Internet Service Provider* (ISP), as shown below. 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.

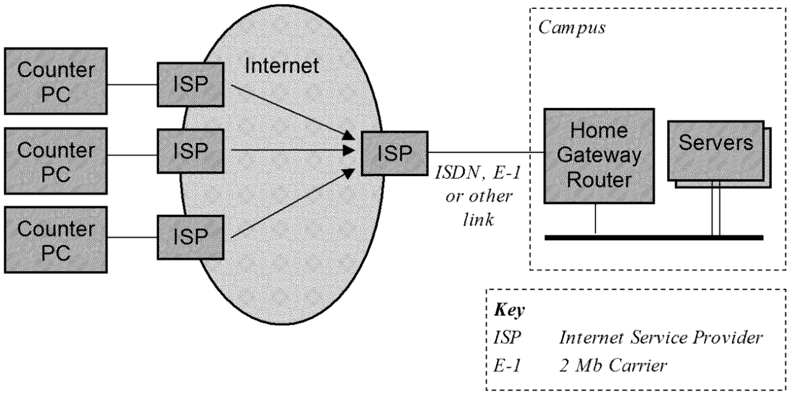


Figure 20 – Remote Access With Point-to Point Tunnelling Protocol (PPTP)

10.3.4.2 FRIACO service

With a FRIACO service, the primary protocol used is the IETF *Layer 2 Tunnelling Protocol* (L2TP), which is derived from Cisco's L2F (*Layer 2 Forwarding*) protocol. 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.

Tunnelling is the key to L2TP (and other virtual dial-up services). With tunnelling, protocol packets of one type of network are put inside or *encapsulated* in the protocol packets of another network for transport across that network.

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

Pathway would use an additional RADIUS server, to authenticate the in-bound call. Figure 21 shows the management boundaries for the standard FRIACO service.

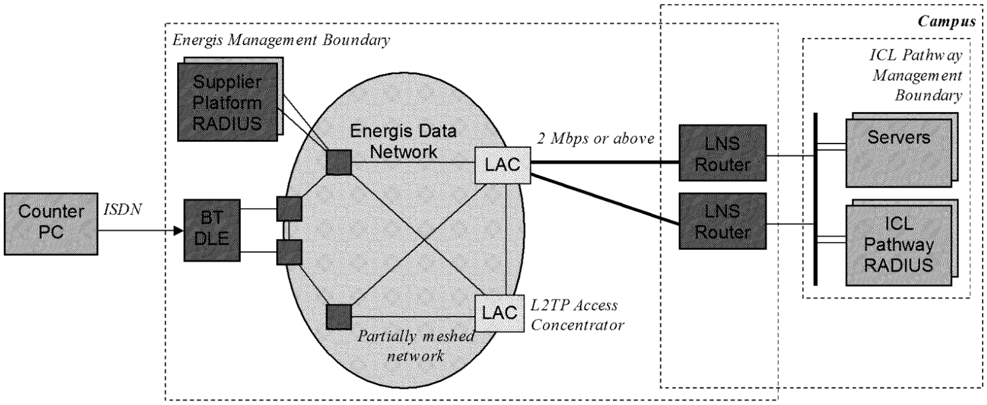


Figure 21 – Standard FRIACO Service Offering

10.3.4.2.1 FRIACO L2TP service

This moves the management boundary, as the tunnel termination is now under the control of Pathway and not the FRIACO service provider. The FRIACO service provider provides the link from the WAN interface Router, which is owned and managed by the service provider. The link may be of any size between 2 Mbps (E1) up to 155 Mbps (OC-3), depending on the number of FRIACO ports purchased. Moving the boundary into the Campus allows Pathway to implement and manage the LNS Routers (which terminate the tunnels) in order that they will 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. Figure 22 illustrates the shift in management boundaries.

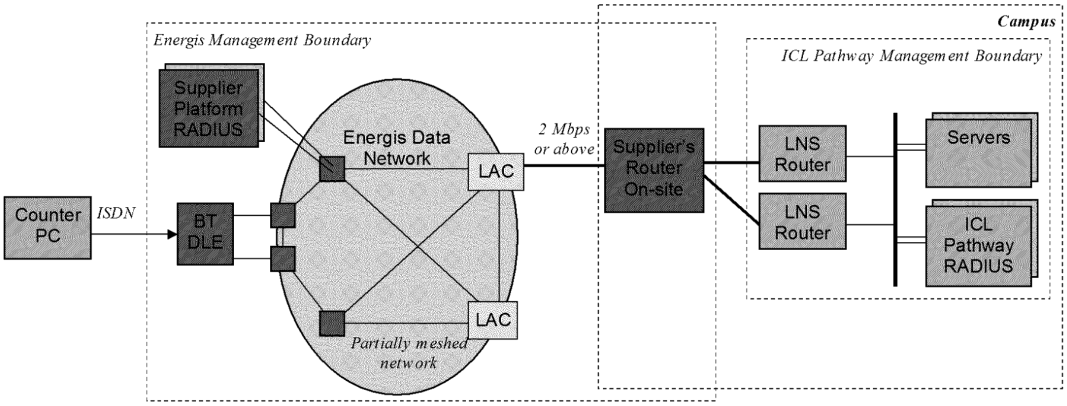


Figure 22 – FRIACO L2P Service Offering

10.3.4.2.2 L2TP Access Concentrator (LAC)

This is an L2TP device, that the client connects to directly, and whereby PPP frames are tunnelled to the LNS. The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. It may tunnel any protocol carried within PPP. The LAC is the initiator of incoming calls and the receiver of outgoing calls. It is analogous to the Layer 2 Forwarding (L2F) *Network Access Server* (NAS).

10.3.4.1.3 L2TP Network Server (LNS)

This is the termination point for the L2TP tunnel, and the access point where PPP frames are processed and passed to higher layer protocols. The LNS operates on any platform capable of PPP termination. It handles the server side of the L2TP protocol. 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, which in turns feeds the LNS routers via a Fast Ethernet connection.

10.3.5 Network Connection Types

Currently there are two Outlet connection types: satellite and ISDN. With the advent of NBS, a proportion of the ISDN dial-up connections will require to be permanently on-line during the business day, while others will remain on 'dial on demand' albeit into the Energis Data Network as opposed to the current Energis Voice Network. The two variations on the ISDN service are defined as *Silver* and *Bronze* service levels.

- *Silver* is defined as being an Outlet that requires to be permanently connected during the normal PO Ltd business day, or in fact in some instances for 24 hours. A 'Silver' defined Outlet will, in the majority of cases, be connected via the FRIACO service. However, not all Outlets requiring a Silver service will be capable of exploiting a FRIACO connection, owing to the fact that Energis currently do not provide a UK wide FRIACO service. In this scenario, a non-FRIACO Silver Outlet will use the Energis *RemoteConnect* service, which is a metered call. The RemoteConnect service utilises the Energis Data Network with call termination on the LNS routers as per the FRIACO service. A separate range of telephone numbers is used for the FRIACO and RemoteConnect services. If a Silver Outlet, is deemed to be for PO Ltd Business hours only, then outside of the defined hours of 'day-time' usage, the Outlet will be switched from a permanent connection to 'dial on-demand'. The majority of FRIACO ports to be purchased from Energis are for 'day-time' usage only. The Counter Network Infrastructure Manager (CNIM) will switch the ISDN telephone number to be called for the FRIACO service to that of the RemoteConnect 'dial on-demand' service. The ISDN number for the Eicon card, on the Gateway PC, is switched via an API call, which instigates an Eicon card reset in the process.
- *Bronze* is defined as being an Outlet that does not require to be permanently connected, as the volume of traffic does not justify the expense of having a FRIACO service or a permanently connected RemoteConnect service. Thus, Bronze Outlets utilise the 'dial on-demand' RemoteConnect service. However there is an additional requirement for Bronze Outlets to be capable of switching from Bronze to Silver for pre-defined times of the day on pre-defined days of the week. This is a cost reduction exercise where an Outlet on traffic volumes qualifies as a Silver Outlet, but outside the peak hours (08:30 to 10:30) on say Mondays & Tuesdays the volume of traffic is that of a Bronze Outlet. These sites are defined as *Silver Part Time* with the capability of switching to Silver via the CNIM at the appropriate time of day.

Note that a third, Gold, service level is described in [SRS]. This would provide higher availability levels by the use of additional connection routes to selected Outlets. However, this service level will not be available in NBS Release 1.

At this point, it is virtually impossible to ascertain the exact split between the permanently connected Outlets and those that 'dial-in' on the metered service. The split is dependent on a number of factors such as size of Outlet, location, cost of FRIACO service (based on the number of ports purchased). However, the mix of 'permanent' and 'dial-in' Outlets will be configurable within Pathway, based on close monitoring of the live estate when FRIACO is introduced. The current projected split is 12,000 'permanent' connections and 1,500 'dial-in' connections, at completion of the roll-out of NBS across the whole estate. With 1,500 'dial-in' ports available for 5,500 Outlets (17,500 – 12,000 permanently connected Outlets), this provides a contention ratio of 3.66:1 for port availability on a 'dial-in' connection. It is proposed that the 'permanently' connected Outlets applies to pre-defined times of the day, i.e. 01:00 through to 17:30, Monday to Friday, 01:00 to 13:00 Saturdays, and 01:00 to 08:00 Sundays, as outlined in [SDSINF]. It is proposed that a quarterly review will be established in order that the split between 'permanently' and 'dial-in' connected Outlets can be modified if required. Input from to the review will come from two sources, Pathway by way of Capacity Management analysis, and from PO Ltd, for specific Outlet changes required for whatever reason.

10.3.5.1 Resilience and Availability

The standard FRIACO service delivers the IP packets to a single host site. At least two LNS Routers are installed, depending on the number of FRIACO ports purchased.

- *Two LNS Routers* - may be run in parallel and load share, or run in "Hot Standby" mode where a single Router handles the workload with the second in standby mode. This is achieved by using *Hot Standby Routing Protocol* (HSRP) between the Routers. The Routers are set up with independent IP addresses, with a virtual IP address spanning both Routers on the same LAN. Traffic is directed to the virtual IP address, which maps on to the active Routers' IP address
- *Multiple LNS routers* - In the Horizon scenario, there will be six LNS routers per Campus. Resilience is provided by the fact that the Outlet will have more than one ISDN number configured in the Eicon driver. Thus, on the initial FRIACO connection attempt, if the call fails then the Eicon card will dial the second FRIACO number which will be directed to another LNS router. Each LNS router advertises routes (from Outlets), to the Summary Layer via the use of the OSPF protocol

Dual Campus Access. The Horizon requirement is that IP packets can be delivered to either Campus, in order to provide a fully resilient network. At present, the normal network workload is shared across both Campuses, in that 50% of Outlets use Wigan as their Home site and the other 50% use Bootle. In a disaster scenario, all traffic is automatically redirected to the remaining Campus. This is achieved by the Gateway PC having multiple ISDN telephone numbers, which it calls cyclically until one responds. The sequence currently is Primary number (at Home site), Secondary number (Home site – different router), followed by the Tertiary number, which resides at the other Campus. The ISDN Eicon card requires four telephone numbers, and the fourth is set to the primary number. The FRIACO service requires two sets of numbers, 'Permanent

FRIACO' and 'Metered Call'. The Sequence of telephone numbers allocated to the Eicon card at each Outlet is therefore, depending on the FRIACO access method defined for that Outlet, as shown in the Table below. Within the Energis network, if a connection to an LNS router fails, for whatever reason, the network will attempt to connect to a pre-defined alternative LNS router. This alternative LNS router is located at the other Campus. With the network providing this level of fail-over, the need for the Eicon card to employ Primary, Secondary and Tertiary ISDN numbers is removed. However, the Eicon card still requires four telephone numbers to be assigned. The sequence of telephone numbers for the two connection types is shown here.

Eicon Tel No.	FRIACO 'permanent'	Metered 'dial-in'
1	FRIACO 'permanent' No (1)	Metered 'dial-in' No (1)
2	Metered 'dial-in' No (1)	Metered 'dial-in' No (2)
3	FRIACO 'permanent' No (1)	Metered 'dial-in' No (1)
4	Metered 'dial-in' No (1)	Metered 'dial-in' No (2)

Table 21 – Dial Sequence with Eicon card

- *Dual LAN Connectivity for the LNS Routers* - as with the current Pathway implementation of ISDN Routers, each LNS in fact has two Fast Ethernet connections to two independent Catalyst switches. This provides a "dual LAN" capability with a further level of resilience. In addition, there will be two FRIACO 'Feed' routers at each Data Centre, these 'Feed' routers are provided by the Network supplier as part of the FRIACO service.

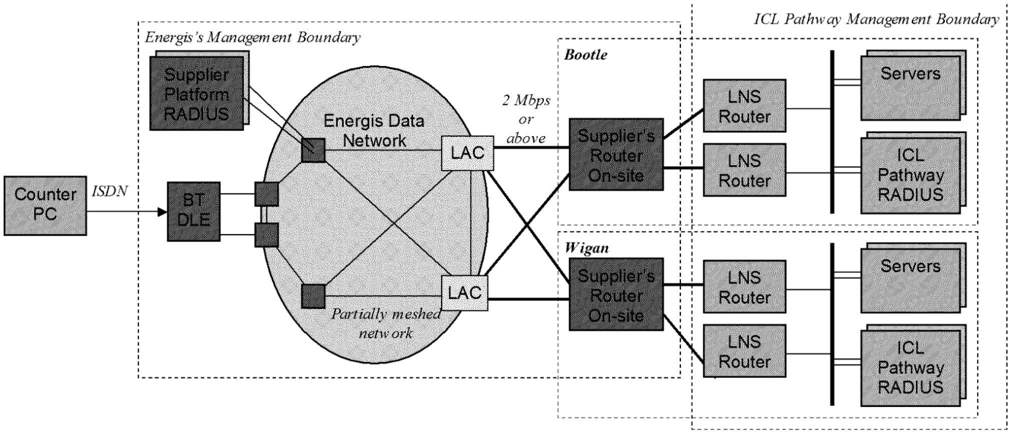


Figure 23 – Resilient Feeds to Two Campuses

10.4 DIAL AROUND FACILITY

A 'dial around' facility has been proposed by Energis, in order to overcome any potential FRIACO network congestion problems. This 'dial around' occurs when a 'Silver' Outlet loses its FRIACO 'nailed-up' connection for whatever reason during the day usage period, and cannot re-establish the service. A metered call is invoked at a reduced rate to that offered on the standard RemoteConnect service. This facility is only available during the day usage period; at all other times, the standard RemoteConnect service is invoked. The number of 'dial around' ports required has been assessed and is deemed to be 7.5% of the number of FRIACO ports. Thus, on the assumption that full roll-out will provide 12,000 FRIACO ports, there will be 900 'dial around' ports available during the day usage period.

10.5 NETWORK INFRASTRUCTURE AT THE CAMPUSES

Currently the Campus servers use 100BaseT connections to the Cisco Catalyst 5500 Switches. With the introduction of NBS, these switches will be upgraded to Cisco 6500s in order to provide additional port capacity. They will be further enhanced in the future, when the NBE begins to support multiple channels, to include an *Intrusion Detection System* (IDS).

10.5.1 Intrusion Detection System

Intrusion detection will become necessary because of the increasing number of connections to remote sites from the Campuses. A particular area of increased risk is the NBE, which is expected in due course to support multi-channels including Internet access. The need for high resilience for NBS means that it is necessary to provide more sophisticated monitoring than previously. IDSs will provide "content aware" monitoring of the data passing through the network. The IDS will be attached to the switch and monitor all traffic through that switch, including any originating in the outside world at the NBE sites or Outlets. The IDS module available for the Cisco 6500 catalyst switch is an integral function of the switch, thus bringing both switching and security functionality onto the same chassis. [NBR588]

In summary, IDS systems provide the following:

- They analyse the packet data streams within the network, searching for unauthorised activity, such as attacks by hackers, enabling users to respond immediately to security breaches
- On detection of unauthorised activity, the IDS module sends an alarm to the Management Console with details of the detected event
- Pathway Security and/or the Network administrator specify the network traffic that must be inspected by the IDS module
- The IDS module is transparent in operation, as it does not impact switch performance
- It is a passive monitoring module that inspects copies of packets and is not in the switch-forwarding path
- The IDS module provides real-time, around-the-clock, network surveillance, designed to address the increased requirements for security visibility, denial-of-service protection, anti-hacking detection, and e-commerce business defences
- The IDS module detects a wide range of attacks, and the signature engine on the IDS module is easily updated with new "hacker signatures" without any impact on the switch
- The IDS module has the ability to monitor multiple VLANs simultaneously, using either the VLAN *Access Control List* (ACL), or *Switched Port Analyser* (SPAN) functionality

10.5.2 Campus Network Infrastructure for NBS

The basic Campus infrastructure to accommodate NBS is shown in Figure 24.

10.5.2.1 Campus Routers

10.5.2.1.1 LNS Routers

There are six of these per Campus. They are 7200 Routers, and replace the Cisco 7576 Campus ISDN Routers.

10.5.2.1.2 FRIACO Feed Routers

These are provided by the FRIACO service provider.

10.5.2.1.3 Outward Call Routers

To retain an ISDN "dial out" capability for software distribution and support purposes (see Section 12.6.1), three Cisco 5350 Routers are introduced per Campus. These are 1U in height, and contain two Fast Ethernet ports and two PRI ports (providing 60 ISDN ports per Router, or 180 channels per Campus).

10.5.2.2 Campus Servers

10.5.2.2.1 Cisco Secure Server

This new server is dedicated to monitoring all data transfers through the FRIACO LNS Routers.

10.5.2.2.2 Cisco Syslog Server

This new server is dedicated to logging all data transfers through the FRIACO LNS Routers.

10.5.2.2.3 RADIUS Server

The Radius Servers are called, by the LNS routers in order to provide *Challenge Handshake Authentication Protocol* (CHAP) authentication for the FRIACO in-bound calls. There will be three Radius servers per Campus. They all contain the same authentication information. On an authentication request, if a call fails to a specific RADIUS server the request will be repeated to another RADIUS server either at the same Campus or the other Campus.

The RADIUS servers accept a data feed from the Auto Configuration Database Server so that they know which Outlets to accept calls from.

10.5.2.3 Campus LANs

As can be seen from the diagram new LANs are introduced:

10.5.2.3.1 FRIACO LAN

This supports the FRIACO feed Routers as provided by the Network supplier. These Routers are owned and managed by the network supplier. On the FRIACO LANs reside the LNS Routers, which terminate the tunnels from the PO Outlets. The LNS Routers internal to the Campus connect on to the PO Access LANs as do the ISDN Routers, and Frame Relay Routers (connection to Milton Keynes for VSAT). The

Routers on the PO Access LAN advertise routes (to the PO Outlets), to the Summary layer by the use of the OSPF routing protocol. The Summary Routers and the associated LNS Routers are in 'cells' as per the current implementation of the ISDN Routers. The RADIUS servers, which authenticates calls from Outlets that are delivered to the Campus via a FRIACO call, and the ISDN 'dial out' routers, are also resident within these cells.

10.5.2.3.2 NBS Internal LAN

This is a dedicated and isolated LAN that supports solely the *NBS Agent Servers* and the NBS Firewall systems. The Servers communicate with both the internal Correspondence servers and the NBE(s) at IBM Warwick and Greenford. In order to safeguard the NBS Agent Servers and the rest of the Campus, the NBS Agent Servers connection to the NBE is only through the Firewalls, where the firewall Rule-base(s) restrict access through the use of Access Lists and protocol restrictions. Similar firewalls are used to isolate the LAN from the rest of the Campus.

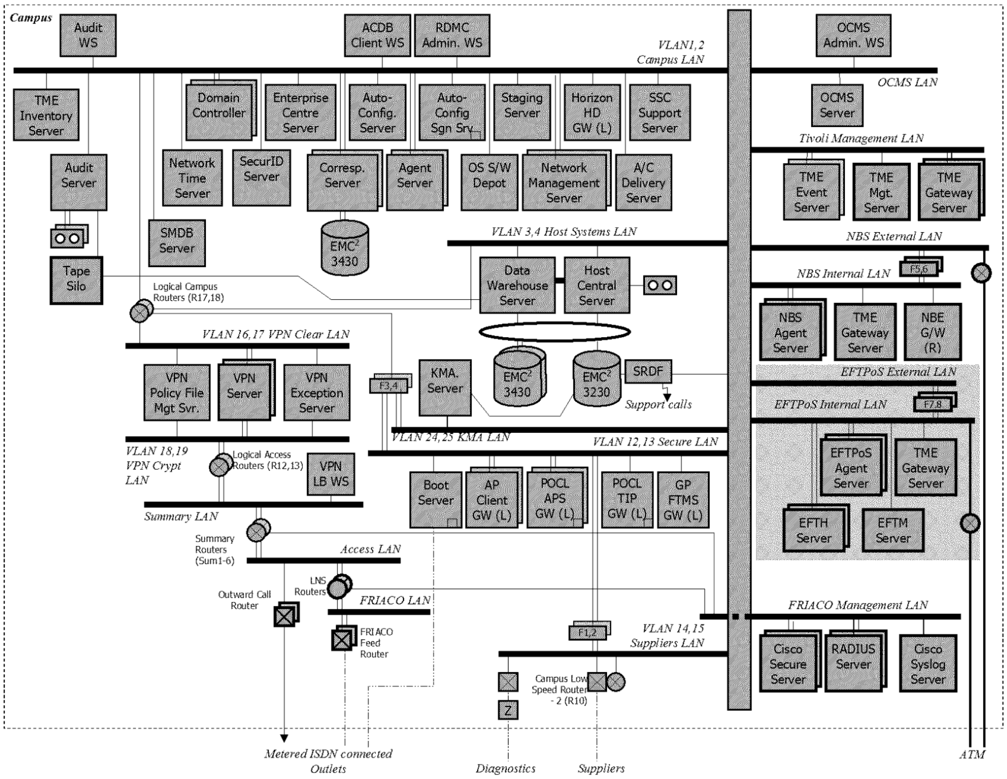
10.5.2.3.3 NBS External LAN

This is a dedicated and isolated LAN used solely for the external side of the NBS firewall systems and their access to the NBE.

10.5.2.3.4 FRIACO Management LAN

This is a dedicated and isolated LAN that supports the *Cisco Secure server* and the *Cisco Syslog server*.

As per standard practice within the Horizon infrastructure the Campus concept is expanded to include two Catalyst 6500 Switches, and all servers are dual LAN connected for resilience. This is shown below.



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

Figure 24 – Campus Infrastructure Layout at BI3

10.5.3 Summary Routers and Cells

Under the current implementation of ISDN, the ISDN Routers advertise routes "learned" by the act of an Outlet "dialling-in". The Routers advertise the routes to their peers within a "cell", or OSPF area. This cell is a replicatable unit and is the basis for the network scalability. A cell is managed by a Summary Router and contains two LNS Routers, one ISDN Router and a RADIUS server, as shown here.

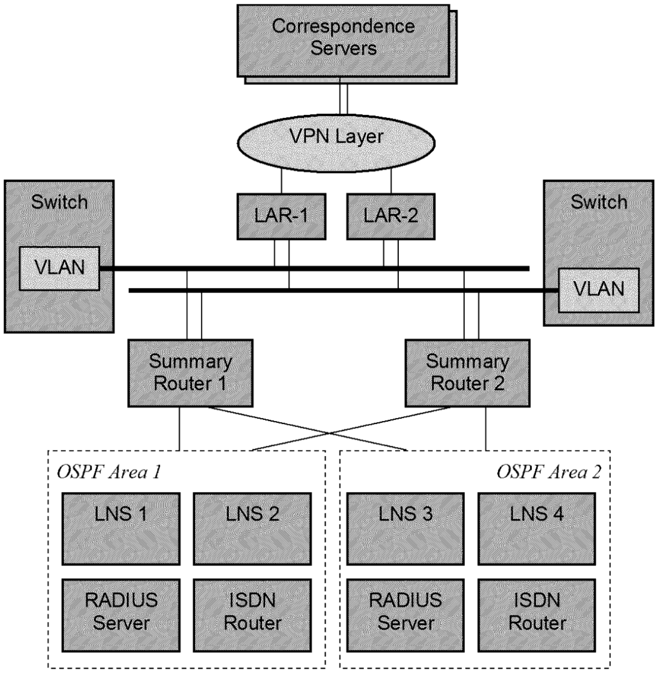


Figure 25 – Summary Layer with Resilience

However, this configuration is still vulnerable in that if the Summary Router layer is lost at a Campus, all in-bound connections are also lost. Thus, the Summary Router "pairs" are configured across the two Campuses, as shown here.

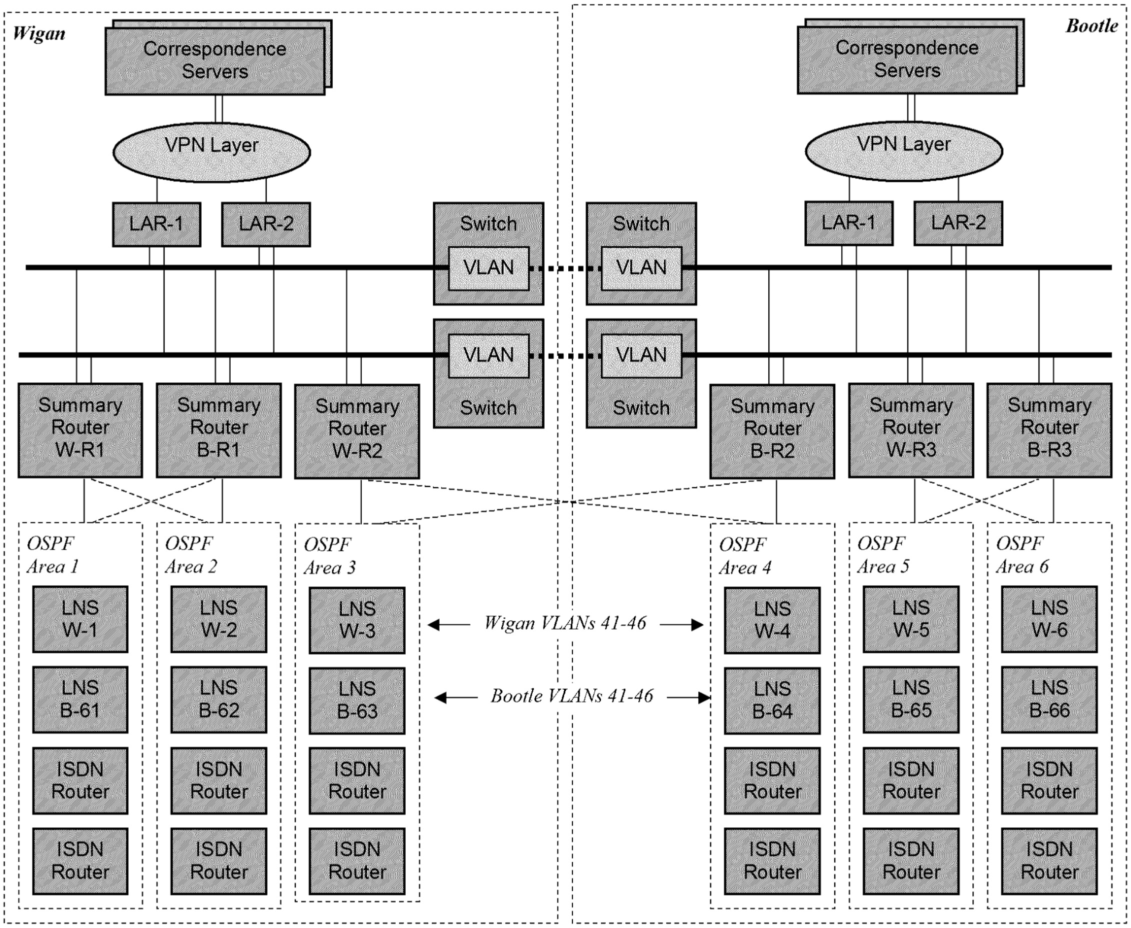


Figure 26 – Summary Layer Cross-Campus Links

10.6 INTER-CAMPUS NETWORK

Currently no additional Routers or *Asynchronous Transfer Mode* (ATM (2)) links are envisaged. There are two x OC-3 links (155 Mbps each), via Pathway's managed ATM switches. A number of the Campus LANs are carried across these links as *Permanent Virtual Circuits* (PVCs) within ATM. For resilience, the FRIACO service will also utilise this cross-Campus facility, as shown here.

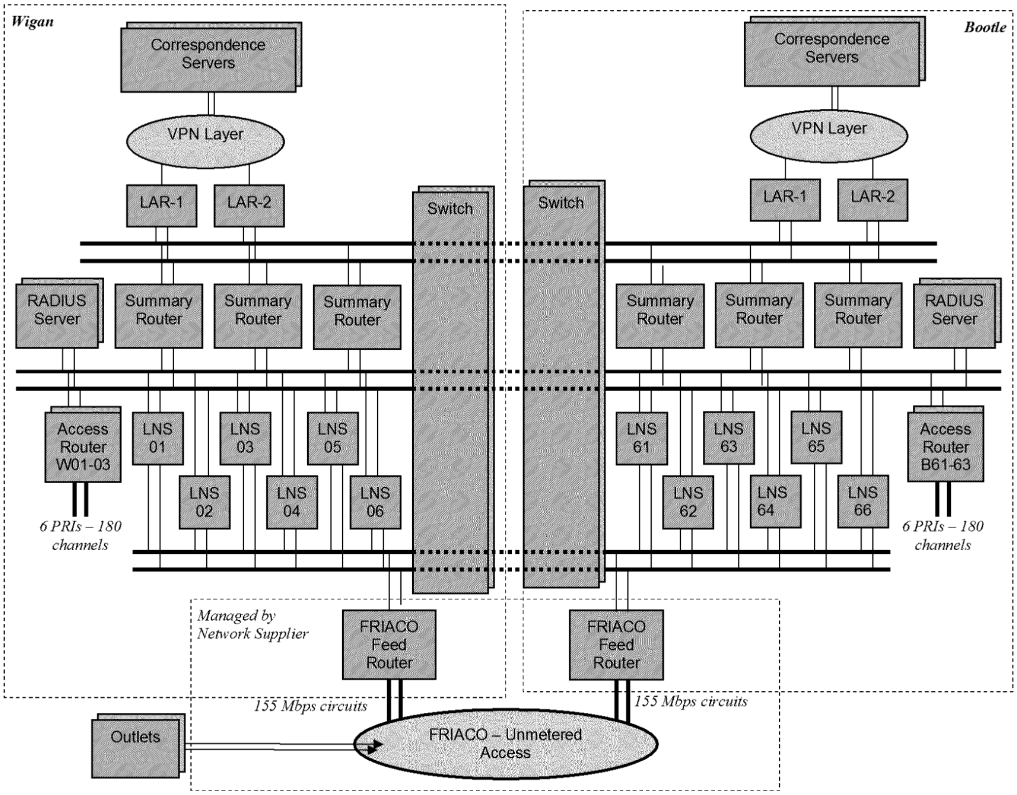


Figure 27 – FRIACO Service Across Campuses

10.7 Network Connection – Horizon to NBE

Links are required to the live and standby NBEs, located respectively at IBM Warwick and IBM Greenford. [NBR285]

10.7.1 Link to NBE

The bandwidth required is expected to be in the region of 6 to 8 Mbps. Encryption is required, which due to the high speed of the circuits cannot be standalone hardware encryption. The alternatives are LAN encryption or encryption within the routers. The Cisco routers proposed will employ hardware encryption utilising an Integrated Service Adapter which provides IPSec Triple DES encryption. Similar Routers will be located at each NBE site. The Routers at each site must be resident on a common LAN (cross-Campus VLAN) and advertise their routes to both Wigan and Bootle. In this scenario, the fault tolerant firewall farms resident at each Campus must be party to this Router VLAN, in order to ascertain which Router to use.

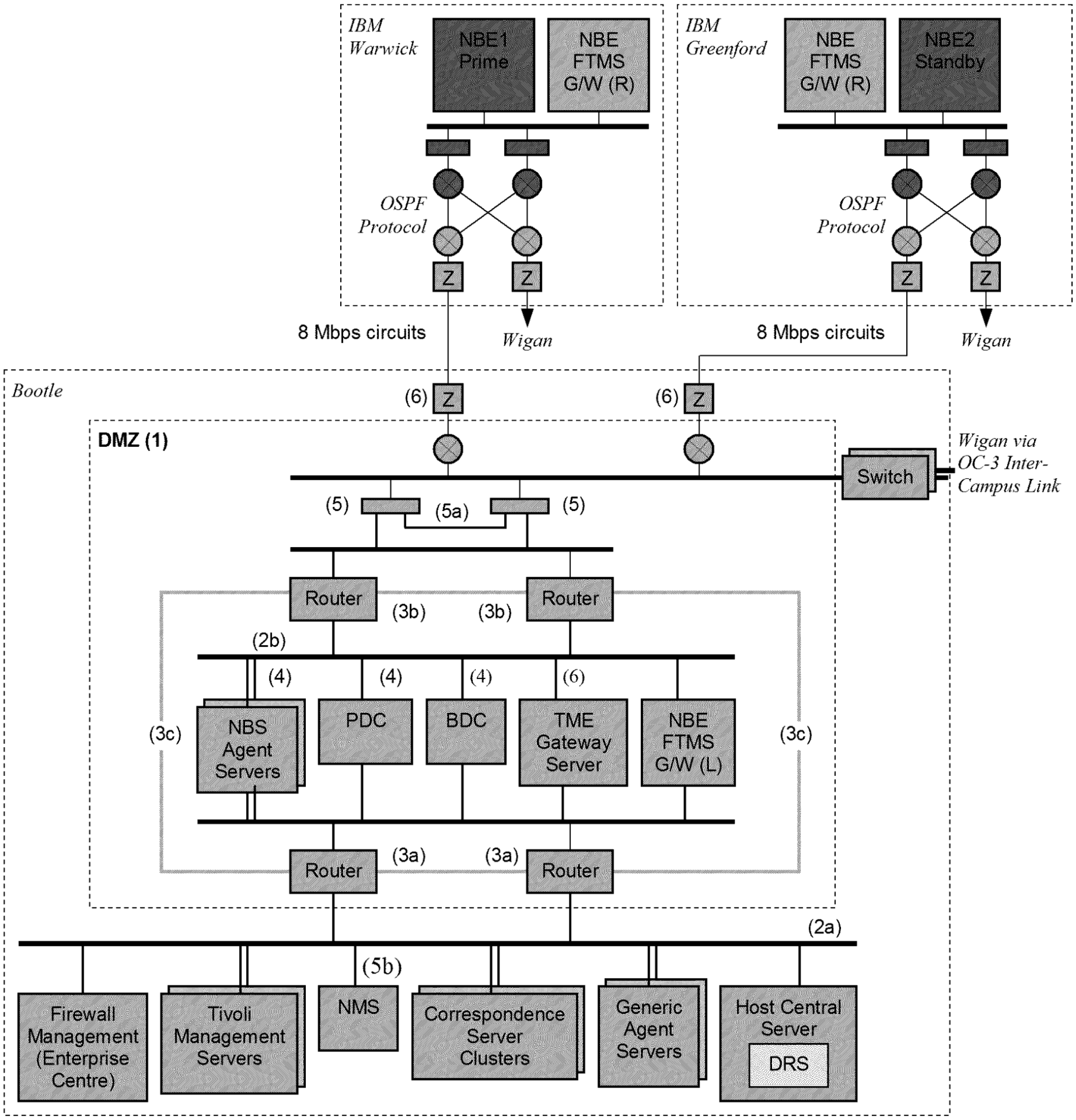


Figure 28 – Secure Network Architecture – DMZ

10.7.2 Boundary Protection – Horizon to NBE

The interface between the NBE and the Horizon security domains will be subject to a Boundary Protection System. The purpose of this is to protect the Horizon environment from unauthorised interactions with the NBE.[38] [NBR571]

The elements of the Horizon system that directly interact with the NBE will be contained within a secure component of the Campuses, called a *De-Militarised Zone* (DMZ). The components of the DMZ are also shown in the diagram above. [NBR558]

The following sections refer to the items numbered in parenthesis in Figure 28

[38] *Note that there is no direct connection from the Horizon system to the Internet. This protection is to guard against unauthorised public access via the NBE.*

10.7.2.1 NBS Agent DMZ (1)

The DMZ is a secure processing environment whose primary function is to protect the Horizon environment from unauthorised interactions with the NBE.

As a secondary function, the DMZ will protect the NBE interaction from unauthorised activity that may originate from within the Horizon system itself. The principle characteristics of the DMZ are:

- It is a separate network from the Horizon Campus Network
- The NT Systems within the DMZ form their own NT Domain
- All systems within the DMZ are Tivoli managed in accordance with current practices (e.g. event forwarding). The Tivoli services will be configured to only use known port numbers (i.e. no ephemeral ports)
- Systems are protected by fault tolerant firewalls

10.7.2.2 Sub-Network Separation (2)

Logically, there is no direct (data) network connection between the entry and exit from the DMZ. Network connections 2a and 2b are separate. In physical terms, the network components are set up as discrete VLANs whose interconnections are "policed" by the Switch Router module and rule-base. Note there is a separate connection for network management (3c & 3d) – see Section 10.7.2.5.

10.7.2.3 Fortified Switches and Routers (3)

Router functionality is provided either side of the systems within the DMZ, by the Campus switches, and is used for both Networking and security purposes.

The characteristics of the these devices are as follows:

- They use a fortified configuration to protect them from unauthorised access attempts (protocols, services and addresses)
- Filters are defined to only allow authorised protocols and services for identified addresses (source and destination). Address ranges are validated according to the following scheme.
  - Switches 3a only allow communications between authorised Campus system addresses and the *NBS Agent Servers* (or PDC/BDC or TME Gateway) addresses
  - Switches 3b between NBS Agent Servers and Firewall addresses
- Network and Router management commands can only originate from the authorised NMC workstations. All configuration changes are recorded and old versions of the configuration are archived to tape
- Switches 3b are "load balanced"
- There are separate circuits for network management (3c & 3d) and data flows. Filters are defined on the Routers to preclude the unauthorised use of these connections.
- An Intruder Detection System (IDS) will be deployed on the Routers at 3b when the NBE supports multi-channel access (internet/WAP etc.). In physical terms, this will be mounted in a separate card that that "slots" into the backplane of the Router (Switch)

Note: the Switches at 3a are used instead of Firewalls for two main reasons:

- Mediating the interconnection via a firewall would raise performance problems because of the higher message rates between the Correspondence Servers and the NBS Agent Servers (multiple [R&C] messages)
- The lower risk of the inter-connection between the DMZ and the Campus systems as opposed to the connection to the NBE.

10.7.2.4 Strengthened NT Build (4)

The secure build of the NT system will be upgraded to reflect the potential risk arising from external system connections. This will entail applying all reported and applicable "hot fixes" after the Service Pack 6a release, and strengthening the security configuration of the NT systems themselves. (This is applied across the Campus servers, not just in the DMZ.)

10.7.2.5 Fault Tolerant Firewall Farm (5)

Firewalls are used to mediate the interactions between Horizon and the NBE. 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 NBE
- Applies *Network Address Translation* (NAT) to conceal Horizon addresses from the NBE
- Uses Firewall clustering to provide a resilient and scalable solution (5a).
- Audit files are to be transferred to the Firewall Enterprise Centre (5) 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 is a cross-Campus VLAN as shown in Figure 24
- The Firewalls are Cisco PIX 515URs
- The WAN Router is a Cisco 7204V XR with an *Integrated Service Adapter* (ISA) providing IPSec Triple DES encryption [NBR573]

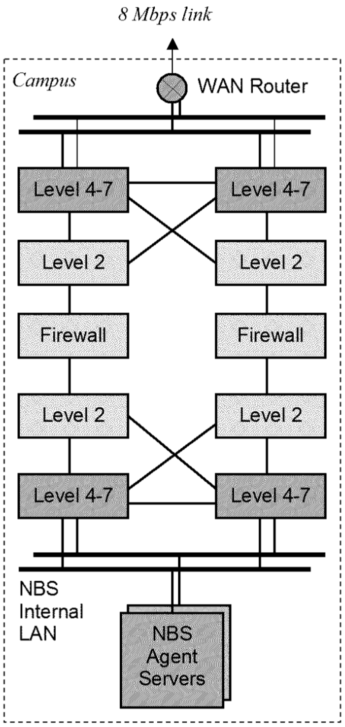


Figure 29 – Fault Tolerant Firewall Farm

10.7.2.6 Tivoli TME Gateway Server (6)

As described in Section 12.3.1.1, the standard Tivoli action is to use ephemeral port numbers, which contravenes the Firewall requirement for use of fixed port numbers. To permit Tivoli management of the *NBS Agent Servers* within the DMZ, a TME Gateway Server is included within the DMZ. The management exchanges between the central Tivoli Management system (TMR) and the TME Gateway Server will use fixed ports.

10.8 NETWORK MANAGEMENT

Network Management can be divided into a number of categories namely:

- LAN Management at the Campuses
- WAN Management of the Routers
- Management of the Network Infrastructure
- Management of Counter Network Infrastructure

10.8.1 LAN Management

LAN Management Solution (LMS) is provided as part of the CiscoWorks2000 family of products. LMS provides operational focused applications for configuration, fault monitoring and troubleshooting fore the Campus networks. A browser interface provides access to topology maps, configuration services and performance information. A Resource Manager (Cisco Resource Manager) provides a Web-based management tool for managing Inventory, configuration and software updates for the

Cisco routers and switches. A Real Time Monitor (Genius Real Time Monitor) is available which is a web enabled system delivering multi-user web access to network wide, real time RMON information from the RMON enabled 6500 Catalyst Switches.

10.8.2 WAN Management

The Cisco Routed WAN Management Solution (WMS) is part of the CiscoWorks2000 product family, providing enterprise management applications to configure, administrator, monitor, and troubleshoot routed wide-area networks. In addition to a Real Time Monitor and a Resource Manager (as per LMS) there is an Access Control List (ACL) Manager function.

10.8.3 Management of the Network Infrastructure

The network infrastructure, i.e. the FRIACO and RemoteConnect services as provided by Energis are managed and controlled by Energis. However, within Pathway there is a need to monitor the network infrastructure in order to ascertain usage trends, hot spots etc. Three functions are required with any Remote Access service: Authentication, Authorisation and Accounting (AAA). The RADIUS servers located in the Campuses perform these functions, namely:

- Verification of the user dial–in name and password, (Authentication)
- Controls access to services, (Authorisation)
- Record details about each call, (Accounting)

The RADIUS servers collect many details about the data sessions. However, they do not provide any trend analysis, such as:

- Usage patterns
- Duration of calls
- Number of DNIS ports used
- Variations in connectivity during the day
- Variations in connectivity over the week

In order to provide full trend analysis, a separate platform will be employed which will obtain the call logging information from the RADIUS servers located at both Campuses.

10.8.4 Management of Counter Network Infrastructure

With the developments described in this Section, it is necessary to ensure that an Outlet (a) knows what type of network connection it is expected to use, (b) be capable of changing the connection type at various times of the day, and (c) monitors that connection to provide the necessary degree of availability.

10.8.4.1 Counter Network Information Monitor

A new software component, the Counter Network Information Monitor (CNIM) will be developed and installed in the Gateway PC at each Outlet. This is introduced at BI2 and enhanced at BI3. It will carry out the following tasks.

- Understand the type of network available at that Outlet, as recorded in the Gateway PC's registry. The types are:

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

- *ISDN voice* - calls can be originated in both directions
- *Metered dial-in* (Bronze) - calls are made when required and closed when no longer needed)
- *FRIACO permanent* (Silver) - calls are made when required and are not closed unless or until the service availability window closes
- *Metered permanent* (Silver) - calls are made when required and are not closed unless or until the service availability window closes. This is employed in those areas where the FRIACO service is not available
- *Metered permanent* (Silver part time) – calls are made when required and are not closed until the service availability window closes (08P30 to 10:30)

- Make calls as required in support of application requests
- Within a time span that may be specified by a calling application, reject a call to the Outlet from the Campus and immediately make an inward call to the Campus ("call reversal")
- Keep the call live as dictated by the network type and availability window, and close it when no longer required
- Report on the availability of the network to application level processes that wish to know. Classes are:
  - *Network unavailable* (tried to connect and couldn't)
  - *Network available* but not connected (last call attempt succeeded)
  - *Network available* and connected

  A *Comms Status DLL* is provided, and is invoked by the CNIM when a network status change occurs
- Following a detected network outage, attempt to make regular calls to the Campus until service is resumed. (This is the only circumstance in which the CNIM will make a call on its own volition, rather than following a request by a calling application)
- On request, gather network statistics and trace data according to a supplied trace level, and make the relevant trace and log files available to Systems Management processes

The CNIM provides interfaces (via a CNIM client .dll) to allow the current network status to be checked and also to provide notifications of any future changes. In particular it will provide details of network availability from the Outlet to the Campus, and whether the current call (if there is one) is *Optimal*.

In some cases, although the Outlet is configured as a Silver Service Outlet, the connection may not be of the required quality and cost, and so CNIM should be able to drop the connection and try and obtain a better quality connection when it is not in use by Riposte. This means it need make the connection quality available to its callers.

On initialisation, CCS will check the current Network Status and ensure that this is reflected in the *Network Status Object*. It then registers itself for any future notifications of Network Status changes. Should any such change occur, it updates the *Network Status Object* and the way in which it handles Riposte connections.

The position of the CNIM within the Counter architecture is as shown here.

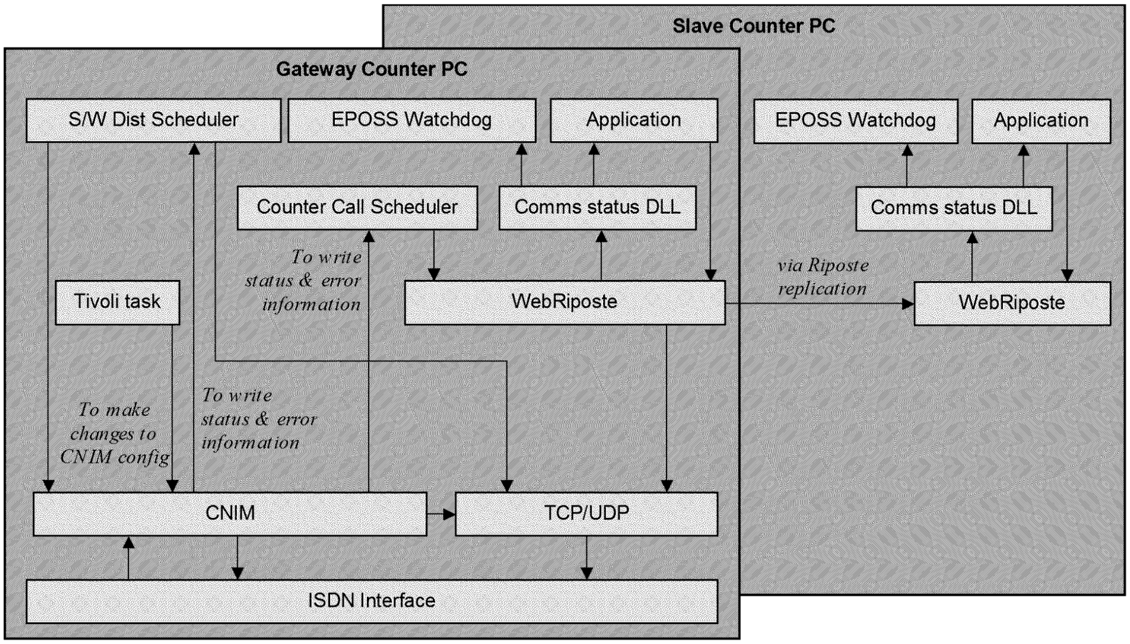


Figure 30 – Counter Network Information Monitor

It is invoked by the Outlet Software Distribution Scheduler to define the beginning and end of the software distribution window. During this window, the CNIM should reject calls from the Campus and immediately make a return call, as described in Section 12.6.1.4

Chapter 11 - Platforms Infrastructure

11.1 GENERAL

This Chapter covers the impact of NBS on the platforms that constitute the Pathway live estate. It addresses:

- New platforms introduced to support NBS
- Platforms that require hardware upgrades to support NBS
- Platforms reconfigured to increase the resilience in response to NBS requirements
- Upgrades to commodity software products required as a consequence of the implementation of NBS
- Other software upgrades required to existing platforms.

It focuses on the changes required. Their sequencing is covered in Chapter 19.

The platforms or upgrades described in this Chapter are deemed sufficient to support the NBS volumes as described in [SRSVOLS] [NBR459]

11.2 REQUIREMENTS SUMMARY

The following requirements arise from Pathway's established approach to the provision of and sizing of platforms for Horizon.

- It should not be necessary to upgrade the Counter hardware
- PIN Pads are required on the Counter PC population
- It is Pathway's practice, for support reasons, to use the same version of a product across all platforms on which it is installed. Thus, a set of similar upgrades is required on the Campus platforms.

11.3 GENERAL PLATFORMS CHANGES

This Section describes the generic changes that are made to a number of different Platform types across the Horizon estate. A later Section discusses the changes that are made, over and above these, to particular Platform types.

11.3.1 Platform Locations

This Section is written on the assumption that:

- Only two Campuses are required to support NBS
- Sufficient space can be found in the existing Campuses to support the platforms needed for NBS, for example by reducing the space used by existing systems[39]

[39] *This may require changes to power and/or air conditioning to support the higher density of systems*

- PO Ltd will provide a primary and a standby NBE system, and the capability to create a Disaster Recovery system at a separate site. None of these is located within an Pathway Campus

11.3.2 Commodity Software Product Upgrades

A number of the third party software products that will be in use in Horizon at S10 are no longer supported by their suppliers. These cover the Counters and all NT, Solaris and Dynix platforms at the Campuses. In these cases, the supplier's usual approach to any support issues is to advise an upgrade to the latest available version.

This may be appropriate in some cases, but needs to be approached with care. There are a number of complex interdependencies between the versions of many of the products used. An upgrade of one product may well require an upgrade to the version of the NT service pack used on that platform, and this can have a knock-on effect on many other product versions.

The approach to software versions taken during the development of Horizon was based on the following principles.

- Use the latest version of NT (4.0) and Service Pack (SP3) available when a decision needed to be taken as to the version used
- Use the same SP across all workstations and servers platforms
- Use the latest stable versions of other products that ran on this SP

Pathway has now agreed with PO Ltd that the BI1 and BI2 Releases will include upgrades to major system components where these can be justified.

11.3.2.1 Upgrade Strategy

In making these upgrades, it is sensible to adopt the same approach, viz:

- In general, upgrade to the latest available version of the SP
- Upgrade all products to the latest stable versions that run on this SP
- Resolve any difficulties that this approach throws up

The upgrades described are those needed within the timescale of the introduction of NBS. Some are required to meet explicit requirements relating to NBS. Others are required to ensure that the underlying infrastructure remains up-to-date and supportable.

11.3.2.2 NT Operating System Versions

11.3.2.2.1 Current Service Pack Situation

The current Horizon system (in particular the Counter PC) uses NT 4.0 SP3. The decision to use this SP was taken as late as possible prior to National Rollout, in the knowledge that it would be exceedingly difficult to switch to a later SP during the Rollout.

However, that baseline is now significantly out of date. NT 4.0 itself has been followed by Windows 2000, and SP3 by Service Packs 4, 5 and 6a[40].

[40] *SP6 was replaced rather hurriedly by SP6a*

11.3.2.2.2 Benefits of a Service Pack Upgrade

Now that the rollout is virtually complete, moving to a later Service Pack is a sensible and positive move that, in Pathway's view, is a *sine qua non* for the increased resilience and availability requirements of NBS and EFTPoS (see [EFTPoS]). The consequence of moving to a later Service Pack will be to prevent future recurrences of the following classes of problem.

- *Better memory management*. There are a number of "memory leakage" fixes in each of SP4, SP5 and SP6a. Most of these fix problems where the virtual memory available to applications progressively decreases over time until the system is rebooted. There is evidence that Counter systems are suffering from memory leakage problems. Although all Counters are installed with 128 Mb of memory, WebRiposte will increase the memory footprint by up to 30 Mb and thus there is considerable benefit to be gained by installing any available memory leak fixes
- *Reduced number of "blue screen" events*. The Microsoft *Blue Screen of Death* (BSOD) occurs with depressing regularity on an ill-constructed system, less frequently on NT and is not particularly a problem with Windows 2000. SPs 4, 5 and 6a each remove a number of instances where the system can stop with the BSOD. While the Counter infrastructure is particularly stable, BSODs do occur more frequently than Pathway would like, and there is considerable benefit in reducing the number of instances of these by installing a later SP.
- *Improved Counter Stability*. There are instances of problems where the Counter, or components of it such as the touch-screen driver, can "hang" either for a time or until the Counter is rebooted. A number of causes of this type of problem are fixed in SP4 and later. These conditions are particularly prevalent in communications stacks including TCP/IP and ISDN.
- *Improved Security*. There are instances of problems where excessive access rights are granted to users by certain system functions
- *Data or Line Loss*. There are instances of data loss (for example, a prematurely terminated file transfer)

11.3.2.2.3 Which Service Pack?

There are considerable difficulties associated with any upgrade to the Service Pack level on the Counters. A system reboot is required to implement the new SP. The speed at which it can be implemented is affected by this, and it takes longer to implement a fix that requires a reboot than one that does not. However, the complexity of this migration is not increased by the identity of the target Service Pack. It is no more complex to upgrade to SP6a than to SP4. Thus, Pathway's position is that once the decision to upgrade the SP level on the Counters is taken, the upgrade should be to the latest stable SP upon which stable versions of each of the third party products are available. This implies SP6a.

A further consideration is that the same SP should be used across the whole estate – servers as well as Counters – to simplify the support procedures and diagnostic skills required in the *Systems Management Centre* (SMC). This argues in favour of SP6a across the estate.

11.3.2.2.4 Implications of a Service Pack Upgrade

A number of third party products will need to be upgraded because of a move away from SP3. This is because the current versions of these products are not supported on any later SPs.

11.3.2.2.5 Recommendations

In the light of the support problems that are already being experience on the live estate, and the greater stress that NBS will place on the ISDN network and the memory occupancy of Counter PCs, Pathway's recommendation is that an upgrade to SP6a is made across the estate as part of BI2.

11.3.2.3 Recommended Upgrades

The following upgrades are proposed for the BI1 and BI2 Releases. Many are a consequence of the upgrade to SP6a.

Ideally, all of these upgrades could be carried out in one stage. That may not be possible, and it may in some cases (particularly on Counter PCs) be necessary to carry out a number of partial upgrades, separated by reboots, and spread over a period of time, to arrive at the desired configurations. The introduction of the facility to invoke unattended reboots, introduced at S10, will greatly facilitate these complex upgrades.

There are in fact a set of factors (described below) that make it necessary to split the BI1 and BI2 Releases into a number of *Service Improvement Packages* (SIPs), as was done at CSR+, to limit the scope of each change and arrive at a sensible and realistic set of smaller upgrades, rather than one unmanageable, interminable and error-prone "big bang". These issues are discussed in Section 19.3, which defines the Release names used below.

The following Sections list all the commodity products used on each platform type, and the upgrades proposed, if any. Following each recommended upgrade is an indication of the Release or Increment at which it should be performed.

11.3.2.4 Counter PCs

11.3.2.4.1 Platforms Affected

This includes all categories of Counter PC, that is:

- Counter PC – Gateway
- Counter PC – Non-Gateway
- Counter PC – Standalone
- Counter PC – Mobile

11.3.2.4.2 Upgrades Proposed

Product	S10	Upgrade	Notes	Release
NT Workstation	V4.0		No change	
Riposte Message Service	6.0.3.nn	V6.2.nn (WebRiposte)	WebRiposte (mandated by PO Ltd) replaces Riposte Message Service. V6.2.5 of Riposte Message Service is V2.0.2 of WebRiposte	BI2OB
Riposte Desktop	B223/nn	B223/mm	B226 is significantly different from B223, and Escher have promised that any changes made to support WebRiposte will be retrofitted to B223. Counters will thus stay on B223, though at a later	BI2OB

			(as yet unknown) build level.	
Internet Explorer	Cut down IE4.0 SP2	IE5.5 SPn	IE5 is needed to support WebRiposte	BI2OA
NT 4.0 Service Pack	SP3 with W2K fixes	SP6a plus all Hot Fixes	Fixes included in SP6a are needed to improve Counter stability and to handle the increased memory footprint of WebRiposte	BI2OA
Sapher Layer7	V1.30.4	V1.31	V1.31 was introduced on Campus platforms at S10.	BI2OB
Utimaco SGVPN	V2.39.5.2	V2.39.5.5	This upgrade is to be made on Campus platforms at S10, but the Counter upgrade is deferred to BI2O	BI2OA
Microtouch Screen drivers	V4.3	V5.53	Likely to need to be updated for SP6a	BI2OB
Specialix drivers	V1.0		Likely to need to be updated for SP6a	BI2OB
Visual Studio run-time	V5	V5 and V6	Code compiled with V5 can co-exist with code compiled with V6, so applications will be upgraded to V6 only where it is necessary to recompile them for any reason	BI2OB
Eicon ISDN Drivers	100-62	??	101-64 is installed on the Boot Server at M1R.	BI2OB
Europa test software	???		No change	BI2OB
Smart Card drivers	???	??	Not know if an upgrade is required	(BI2OA)
SysInternals Blue Save	V1.0	??	Not known if an upgrade is required	(BI2OA)
Athene Performance Monitoring Client	???	??	Not known if an upgrade is required	(BI2OA)
ACFs			These are generated by ACDB and will need to be refreshed to support the Counter changes in BI2OB	BI2OB

Table 22 – Counter Software Upgrades

11.3.2.4.3 Notes

11.3.2.4.4 VPN

It is necessary to introduce VPN on the LAN as part of the NBS upgrade (BI2OB). Further security upgrades may also be required once the full set of NBS requirements are clarified.

11.3.2.4.4.1 Drivers

As well as the Specialix drivers listed above, by the time NBS is deployed there are likely to be additional Counter drivers for:

- Talexus smart card read/writers (if required)
- PIN Pads (see Section 11.5.1.1)

11.3.2.4.4.2 Upgrades to Common File Set

These are required as a consequence of the above. The current Common File Set includes components from NT 4.0, SP3, Riposte Desktop and the VB and VC runtimes.

11.3.2.4.4.3 Upgrades to NT Secure Build

These are required as a result of improvements to the security policy and the introduction of new Protection domains.

11.3.2.5 Other Workstations

11.3.2.5.1 Platforms Affected

This applies to all NT 4.0 Workstations installed in the Campuses or at Pathway support sites including Feltham, Stevenage and Bracknell. The set of platforms affected is:

- Audit Workstation
- Auto Configuration Database Client
- Business Support Unit Client Workstation
- CA Workstation (part)
- DRS Support Workstation (new at BI3)
- Generic Support Workstation
- Horizon Help Desk Terminal
- MIS Client PC
- KMA Workstation
- KMS Admin Workstation
- Migration Training Counter
- OCMS Client Workstation
- One Time Password Workstation
- Performance Management Console
- RDMC Administrator Workstation
- SecurID Admin Workstation
- SSC Support Workstation
- Systems Management Access Workstation
- Tivoli Support Workstation
- VPN Loopback Workstation

11.3.2.5.2 Upgrades Proposed

Product	S10	Upgrade	Notes	Release
NT Workstation	V4.0		No change	
Riposte	V6.0.3	WR V2	Replaced by WebRiposte	BI2C
NT 4.0 Service Pack	SP3 with W2K fixes	SP6a plus all Hot Fixes		BI2C
Oracle Client Software	V7.3.4.5	V8i	In line with proposed Oracle server upgrades. This upgrade may be phased such that it is applied first to Workstations accessing an Oracle 8i database	BI2C
Legato	V5.5.1	V6.0.2	See below	BI2C
ADO	V2.1	V2.6 (MDAC 2.6)	Required to support access to SQL Server 2000	BI2C
Seagate Crystal Reports	V7	V8.5	Only version supported with SQL Server 2000 (see below)	BI2C
PKZIP	V2.04g	V4.0		---
Tivoli	V3.6/7		MANLCF: No further upgrade required	
SecurID Agent	V4.2	V4.4	V4.4 is only version supported on NT SP6a	BI2C

Maestro	V6.1.150	V6.1.170		BI3
Hummingbird NFS	V6.1	---		---
Internet Explorer	IE4.0 SP2	IE5.5 SPn		BI2C
ODBC	V2.65	3.6		BI2C
Visual Studio run-time	V5	V6		BI2C
SQLS Client	V6.5 SP5	V2000	Depends on SQL Server databases (ACDB, OCMS, KMS) being upgraded to V2000. Interception at BI3 is easier than at BI2	BI3
Business Objects	V4.1.10		V4.1.10 is not actually formally supported on SP3, and Horizon should be using V4.1.7 at present. No further upgrade is required. V4.1.10 is supported on SP6a.	---
Adaptec Drivers	2940	---	No upgrade required	
IomegaWare Jaz Drive Software	---	---	No upgrade believed to be required	---
QNG Device Drivers	V1.0	---	No upgrade required	---
TextPad	V4.1	---	No upgrade required	---
WinZip	V7.0	---	No upgrade required	---

Table 23 – NT Workstation Software Upgrades

11.3.2.6 NT Servers

11.3.2.6.1 Platforms Affected

- [Generic] Agent Server
- AP Client Gateway – Local
- AP Client Gateway – Remote
- Audit Server
- Auto Configuration Database Server
- Auto Configuration Delivery Server
- Auto Configuration Signing Server
- Boot Server
- Capacity Management Server
- CM Signing Server
- Correspondence Server (plus existing “wing” servers)
- Domain Controller
- General Purpose FTMS Gateway – Local
- General Purpose FTMS Gateway – Remote
- Horizon Help Desk Gateway – Local
- Horizon Help Desk Gateway – Remote
- KMA Server
- OCMS Server
- Outsourcing Software Depot
- POCL APS Gateway Server – Local
- POCL APS Gateway Server – Remote
- POCL Standby Gateway – Remote
- POCL TIP Gateway Server – Local
- POCL TIP Gateway Server – Remote
- Service Management Database Server
- SSC Support Server
- Staging Server
- VPN Exception Server
- VPN Policy File Management Server
- VPN Server

11.3.2.6.2 Proposed Upgrades

Product	S10	Upgrade	Notes	Release
NT Server	V4.0		No change	
Riposte Message Service	V6.0.n.n	V6.2.n	Replaced by WebRiposte	BI2C
NT 4.0 Service Pack	SP3 with W2K fixes	SP6a plus all Hot Fixes	Retain consistency with Counters	BI2C
Legato	V5.5.1	V6.0.2	Significant performance improvement for Audit; needed because of increased audit volumes caused by NBS. (These are Improved index handling with a claimed 300% improvement; and Removal of 2Gb saveset size limit where any larger saveset is converted to 2Gb linked chunks Approx 50% 0f our backups exceed this 2Gb limit.)	BI2C
SQL Server	V6.5 SP5	V2000	See Notes below	BI3
ADO	V2.1	V2.6	Required to support SQL Server 2000	BI2C

		(MDAC 2.6)		
Tivoli	V3.12	V3.6/7	MANSYS -> MANNTEP	BI1C
SecurID Agent	V4.2	V4.4	V4.4 is only version supported on NT SP6a	BI2C
Hummingbird NFS	V6.1	---		---
EMC Software	V2.0	???	Upgrade required for new hardware cabinet	BI2C
Internet Explorer	V4.01 SP2	V5.5 SPn	Required for consistency with Counters	BI2C
Maestro Scheduler	V6.1.150	V6.1.170		BI3
Oracle Server for NT	V7.3.4.5	V8i	Used for OMDB	BI2C
DAO	V2.1	V3.6		BI2C
Visual Studio run-time	V5	V5 and V6		BI2C
Oracle for NT	V7.3.4.5	V8i		BI2C
Microsoft Office	V97	---	No upgrade	---
Athene Performance Management Agent	???	??	Not known if an upgrade is required	(BI2C)
Eicon ISDN Drivers	V220UP	---	No upgrade believed to be required	---
Sapher Layer7	V1.31	---	No upgrade required	---
Utimaco SG VPN	V2.39.5.5	---	No further upgrade required	---

Table 24 – NT Server Software Upgrades

11.3.2.6.3 Notes

11.3.2.6.3.1 SQL Server

The assumption in this Document is that all the existing SQL Server databases (KMA in particular, but also ACDB & OCMS) are upgraded to SQL Server V2000 in BI3, at the same time as major change are made to these applications. Again, the client software is upgraded to Back Office 2000 variants at the same Release, and again there is the option of not upgrading the client software until a later release.

It is understood that the new Audit Checksum Database (see Section 13.5.3) will be built using SQL Server

11.3.2.7 DYNIX Servers

11.3.2.7.1 Platforms Affected

This encompasses the following Platforms.

- Host Central Server
- Data Warehouse Server

11.3.2.7.2 Upgrades Proposed

Product	S10	Upgrade	Notes	Release
Dynix	V4.4.8	V4.4.9	This is required to support new processor types	BI2C
Oracle	V7.3.4.5	V8i	See Notes below; upgrade does not apply to all	BI2C

			applications at this stage	
Tivoli	V3.1	V3.6/7	MANSEQ: Upgrade to same level as on Counters. However, this is done in BI2 rather than BI1	BI2
Maestro Scheduler	V6.1.150	V6.1.170		BI3
EMC Driver Software	V3.2.2	???	Upgrade believed to be required to support new cabinets, but no details available as yet	BI2C
SecurID Agent	V4.2	V4.4		BI2C
BMC Patrol Agent	V3.4.00	---	No upgrade required	---
Patrol Console	V3.4.00	---	No upgrade required	---
Alexandria tape management software	V4.50.70	---	No upgrade required	---
Hytec Sonnet FTF Software	V2.11.02	---	No upgrade believed to be required	--
Performance Measurement System	---	---	No upgrade required	---
Proxima LogManagerKM	---	---	No upgrade required	---

Table 25 – Dynix Server Software Upgrades

11.3.2.7.3 Notes

11.3.2.7.3.1 Oracle

Both Dynix platforms currently run under Oracle 7.3.4.5, which is somewhat out of date and no longer supported by Oracle.

Oracle 8i introduces support for Parallel Queries, which is required by the DRS application. This database is introduced at BI3 and will be based on Oracle 8i.

Existing Oracle databases and associated Clients remain on Oracle V7.3.4.5 at BI3 unless there are significant application upgrades. This applies only to RDMC/RDDS, and hence these applications will be upgraded to V8i.

This approach causes some issues with the Client applications that access these databases. Given the approach adopted, this would only be an issue if existing MIS Client PCs were to have a requirement to access the DRS database. It is proposed that new Workstations are required to meet any such need, and that at BI2 the MIS Client PCs will specifically *not* be able to access the DRS. All existing Oracle client software on NT Workstations will remain at Oracle 7.3.4.5 for now. Agents (including the new NBS Agents) will use Oracle client V7.3.4.5.

11.3.2.8 Solaris Servers

11.3.2.8.1 Platforms Affected

- Firewall Management Server
- Firewall Module
- Network Management Server
- SecurID ACE Server
- TME Event Server
- Tivoli Gateway Server (introduced at BI1)

11.3.2.8.2 Upgrades Proposed

Product	S10	Upgrade	Notes	Release
Solaris	V2.6		No change, though at some stage the Solaris servers should be upgraded to V8	---
ACE/Server	V3.3.1	V5.0	This upgrade is the subject of CP2963 (currently suspended)	BI2C
Tivoli	V3.1	V3.6/7	MANSOL will include a mix of V3.6 and V3.7B products.	BI2C
TACACS	???		No upgrade believed to be required	---
Firewall Management Software	V4.0	???	No upgrade believed to be required	---
HP OpenView Network Management	V3.2	---	No upgrade believed to be required	---

Table 26 – Solaris Server Software Upgrades

11.4 NEW PLATFORMS

A number of new Platform types are introduced in support of NBS.

11.4.1 NBS Agent Server

This supports the *NBS Authorisation Agent* (see Section 5.7.2), which handles the [R]/[A]/[C0] interactions to the NBE

This process needs hardware cryptographic support for signature checking and verification.

In live running, four instances of the server at one Campus will be scheduled to run *NBS Authorisation Agents*. Four instances at the other Campus will act as "hot standbys".

11.4.1.1 Hardware

The basic hardware unit of scalability will be a Compaq ProLiant ML350 NT server with the following minimum configuration.

- Minimum Form Factor (dependent on number of PCI cards required). The Compaq ML350 allows six PCI cards and is a 5U high rack mount server
- 2 x 1.5 GHz Intel Pentium 4 Processor
- 512 Mb of memory
- Internal PCI *Hardware Security Module* (HSM) for hardware checking or creation of MAC codes; hardware encryption of the sensitive data in the [R] and for PIN Block translation
- Four Network ports. One is used to connect to each of two Correspondence Servers, and two for connection to the NBE and its standby
- No significant storage is required on this system – standard system disk will be sufficient

The target configuration for these Agents is six per Campus, which equates to one server per Correspondence Server Cluster for the *NBS Authorisation Agent* and *NBS Expedited Confirmation Agent*, and two running the NBS Confirmation Agent and other Agents. In the event of a server failure, these processes may be redistributed across the working servers.

11.4.1.2 Software

The software set of the NBS Agent Servers is the same as for the existing Generic Agent Servers with the addition of new Agent applications to support NBS as defined in Section 5.7

11.4.1.3 Configuration

The Riposte services on these servers will connect to the Correspondence Servers in the same way as the existing Generic Agent Servers.

11.4.1.4 Networking Services

Four network cards are provided. Each NBS Agent Server will be configured to connect to the Host Central Server though a different network path. It will also connect to each Correspondence Servers in its Cluster located at the same Campus via different paths. A separate network path is used to connect to the NBE and to its standby.

11.4.1.5 Resilience

Each instance of the *NBS Authorisation Agent* will support a proportion of the Outlet estate. This Agent is a single instance Agent, and as such, its failure will result in loss of service to 25% of the estate, assuming one Agent per Cluster. Each active Agent has a hot standby at the other Campus, and use a form of “heartbeats” is used between those instances so that the standby server will take over if the active server fails.

11.4.1.6 Other Impacted Areas

- Tivoli enhancement to support the new platforms
- Inclusion of the platforms in the Host fail over procedures (if required)
- Maestro dynamic scheduling needs to change to understand about the new type of Agent Servers

11.4.2 HSM Key Generation Workstation

This is introduced to support initial key loading on the HSM modules used in the NBS Agent Servers and KMA Workstation. See Section 13.4.6.

11.4.2.1 Hardware

This is a standard Fujitsu ErgoPro PC. It operates in conjunction with the hand held Atalla *Secure Configuration Terminal* (SCT), which generates the HSM keys. The SCT is connected to it via a standard RS232 cable.

11.4.2.2 Software

This platform is a standard NT Workstation running the Atalla Key Loading Software tool.

11.4.2.3 Resilience

There are two instances of this platform, located in the Feltham and Bracknell secure areas.

11.4.3 Support Terminal Servers

This is a new platform, introduced at BI3, which enables SSC and other support staff to access and diagnose Counter problems via a Microsoft Terminal Server type interface rather than via the Correspondence Server. It is a standard NT Server running Microsoft Terminal Server

11.4.4 Vulnerability Detection Server

This is a new Compaq server that hosts the new WebTrends master console. It collects information from the WebTrends analysis software running on the platforms in the DMZ, and produces appropriate reports.

11.4.5 Cisco Syslog Servers

This is a new platform, introduced to support the FRIACO service, as described in Section 10.5.2.2.2. It is a Compaq ProLiant DL360 NT server.

11.4.6 Cisco Secure Servers

This is a new platform, introduced to support the FRIACO service, as described in Section 10.5.2.2.1. It is a Compaq ProLiant DL360 NT server.

11.4.7 RADIUS Servers

This is a new platform, introduced to support the FRIACO service, as described in Section 10.5.2.2.3. It is a Compaq ProLiant DL360 NT server.

11.4.8 Outward Call Router

This is a new platform, introduced to support continued outward calls from the Campus to Outlets, for example to initiate inward connections for software distribution purposes. See Section 10.5.2.1.3. It is a Cisco 5350 Universal Router.

11.4.9 NBE Gateway Server – Local

This is a standard FTMS Gateway server configured to handle the batch file flow between the Horizon Campuses and the NBE. One instance is located at each Campus. Files received from the NBE will be delivered to the DRS Host via NFS.

The platform contains an HSM crypto co-processor, and Crypto libraries and support software to enable the *EoD File MAC Checker* process to verify the integrity of files after they are copied to the DRS Host.

11.4.10 NBE Gateway Server – Remote

This is a standard FTMS Gateway server configured to handle the batch file flow between the Horizon Campuses and the NBE. Two instances are located at each NBE site. As well as the standard FTMS software, this server supports an FTP Server that is used by the NBE to transfer files to the Gateway Server. FTMS is then used to transmit files between the Local and Remote Gateway servers.

11.5 Specific Platform Changes

This Section discusses changes that apply to particular platform types that existed prior to BI3. All of the following descriptions assume that the relevant commodity product upgrades described in Section 11.3.2 are applied, either as an upgrade to an existing platform or as part of the build for a new platform.

Note that this Chapter discusses the particular characteristics of single instances of the Platforms described. Their interconnections and replication for resilience reasons are discussed in Chapter 14.

11.5.1 Counter PCs

11.5.1.1 Hardware Changes

A Hypercom HFT117 PIN Pad will be added to each Counter position in a phased rollout. See [PPSPEC].

There is no expected need for changes to disk or processor. There is sufficient free capacity on the Counter disks for the increased NBS load. Thus, at this stage, the current Counter hardware specification is expected to prove adequate to meet the requirements of NBS. However, there are two provisos.

- The addition of a PIN Pad will require a visit to the Outlet, possibly preceded by a survey to determine where the PIN Pad is to be located at each Counter position, and how it is to be connected to the Counter PC.
- The Counter PC specification includes 128 Mb of memory. This has proved adequate for desktop applications up to and including M1. However, WebRiposte and NBS, will increase the memory footprint of the combined application set. Early indications are that this increased footprint will still fit within the available memory without excessive paging activity. This will be confirmed by stringent performance tests to ensure that any performance shortfalls that may occur, particularly with the performance of existing applications such as EPOSS or OBCS, are identified in time to rectify them. In addition, as described in Section 11.3.2.2 above, Pathway's recommendation is that the Counter population is upgraded from SP3 to SP6a as part of BI2. This is intended largely to exploit a number of memory-related fixes that have been issued by Microsoft since SP3. These will improve the handling of memory within NT.

11.5.1.2 Software

In addition to the Commodity Software upgrades described above, there are a number of changes to or additions to the Counter software baseline, including the following.

11.5.1.2.1 VPN on the LAN

BI2 will introduce the use of encrypted communication between Counters on the same LAN as well as between the Gateway PC and the Campus. This is to increase the security of the Horizon system.

11.5.1.2.2 PIN Pad Test Software

Software is provided on each Counter to enable the engineer to test the operation of a PIN Pad once one is installed.

11.5.1.3 Configuration

The configuration of Riposte on the Gateway PC will change to “know” about four Correspondence Servers, rather than the two that each Outlet knows about at S10.

Changes to Reference Data for the Counter Call Scheduler are also needed to remove the need for bulk outward connections from the Correspondence Servers to the Outlets.

11.5.1.4 Resilience

As described in Section 14.3.1, Outlets will be progressively assigned to one of two classes of Outlet, depending on the availability requirements.

- The *Bronze service* represents the current service and availability levels, based upon metered dial-up
- The *Silver service* switches to a permanent FRIACO network connection, using the current ISDN circuit. Counter software will ensure that a connection to the Campus is re-made as soon as possible should it be lost

11.5.2 Host Central Servers

The main change to the Host Servers for NBS is an increase in processing power and disk storage to provide capacity for the DRS.

11.5.2.1 Hardware

It is Pathway’s intention to locate the DRS within the existing Host Central Servers. There are two reasons for this.

- Spare capacity exists within the daytime schedule and early morning schedule where most DRS activity will take place.
- DRS will require access to the TPS and other databases, and this is best provided (under controlled conditions) if they are all located within the same platform.

The EMC Disk Arrays that hold the major Oracle databases and KMA Database will be enhanced to cater for the DRS database, the extended MIS database and the increased space requirements of the KMA Database.

In addition, it is necessary to upgrade the Host Central Server to accommodate the DRS workload at full volumes. It is expected that the existing server will be sufficient for NBS up to April 2003 at the earliest.

11.5.2.1.1 Processor Power

The processor board on the Host Central Server will need to be upgraded to the latest specification available (900 MHz) to provide sufficient processing power for the additional DRS service. (IBM have indicated that the 900 MHz board is the last NUMA-Q they will be making. Manufacture will stop in Q4 2002). An operating system upgrade is required to support these new processors and is made at BI2C.

The hardware upgrade needs to be done by around April 2003, to accommodate the increase in NBS transactions. The actual time will depend on the growth of volumes, and results seen in testing.

11.5.2.1.2 Memory

There is sufficient memory (2 Gb) on the live Host Servers (at least 800 Mb free) to support the DRS without change. However, some test systems (particularly those used for performance and scalability testing) will need to be upgraded to support this new application. These are currently 1 Gb systems.

11.5.2.1.3 Disk Capacity

The main area of change is the EMC disk array. It is estimated that between 100 Gb and 300 Gb of slower speed devices is required to support the three-month online storage required for DRS data and 50 Gb of high-speed storage to support the reconciliation function.

The current EMC cabinets have no spare disk capacity and will therefore need to be upgraded. The Host cabinet will be upgraded separately from the Data Warehouse cabinet.

11.5.2.2 Resilience and Recovery

The DRS application will follow the same approach to resilience and recovery as existing Host applications, as defined in [HADDIS]:

- All DRS data filestore will be locally mirrored within the EMC array
- All DRS data filestore will be mirrored using the EMC SRDF product to the array located at the alternate Campus
- Nightly cold backups will be taken, the backup tapes being cloned to ensure they can be read, as well as providing a second copy of the data. Note that this is a change to the current approach of taking two backup copies of the data. Due to time and resource restrictions on the Host, this approach will be employed on the other Host databases. Note that the whole 350 Gb of DRS data storage will not be backed up every night. The 50 Gb of active DRS filestore, plus any new data added to the long-term storage, will be backed up nightly. Any long-term storage that is unchanged since the previous backup will not be backed up. Backups tapes for long-term storage will be recycled after the three months
- As data drops out of the long-term storage (as it is over three months old) it will need to be archived onto permanent tapes
- Archive redo logs will be employed to speed up the recovery process

11.5.3 Data Warehouse Server

11.5.3.1 Hardware

The processor on the Data Warehouse will be upgraded in line with that on the Host Central Server and at the same time. This provides additional processing power for any new reports and SLA calculations for NBS.

A memory upgrade is not required, as there is sufficient free on the existing system.

To provide additional storage capacity, the existing EMC cabinet will need to be upgraded. The Data Warehouse will continue to use a separate EMC cabinet from the Host Server.

11.5.3.2 Software

Changes to the MIS application will be required to support NBS SLA calculations (see Section 5.11 and [SDSAPP]).

11.5.4 Correspondence Servers

The number of active Correspondence Servers (those communicating with Outlets and Agents) in each Riposte Cluster will be increased from two to four, as described in Section 14.5.1. The main justification for this is to provide the resilience needed for NBS. There are a number of consequences of this change. In addition, other software changes will need to be made to the Correspondence Servers.

11.5.4.1 Hardware

11.5.4.1.1 Compaq Recovery Option

The Compaq recovery option on the existing active Correspondence Servers will be removed. The eight servers that are freed up by this (four per Campus) will then be used to provide the processing platforms for the additional Correspondence Servers in each Cluster.

The existing wing Correspondence Servers will be upgraded to a faster processor using the servers freed from the removal of the Compaq Recovery option. The Compaq disk array that is freed will be used for the new Bootle Correspondence Servers. New Compaq Disk arrays will need to be purchased for the new Wigan Correspondence Servers. These will need to be the same specification as the existing Bootle wing.

Performance enhancements may be required, dependent on testing.

11.5.4.2 Software

The software build for the new Correspondence Servers will be identical to the existing ones, except for differences in hardware drivers and the changes to the Common File Set and NT Secure Build made to all NT platforms.

The following change also need to be made to all Correspondence Servers:

- Introduce the Legato Networker Client software

11.5.4.3 Configurations

The Riposte Message Stores on the Correspondence Servers will be configured so that they are all neighbours of each other, in a fully meshed configuration. Dual network paths will be configured for each Correspondence Server neighbour.

The new Correspondence Servers in each Cluster will be configured so that the Audit Agent does not run on them. All other Correspondence Server-based Agent software runs as normal.

11.5.4.4 Networking Services

The Correspondence Servers will continue to have dual network paths between them. To support a single IP address per Correspondence Server at the Outlet, the network route to the Outlets will be pre-configured to only use one of the network paths.

The two Correspondence Servers on each Campus for a Cluster should be configured to use a different network path to the Outlets to maintain resilience against network failure.

Agent Servers will be configured to use the opposite network path to the one that the Outlets use, in order to spread the load across the two different LANs.

11.5.4.5 Resilience

The Correspondence Server layer is highly resilient to failure. However, there are a number of areas where enhancements are needed to support NBS. The new real-time service requires enhanced protection against failure, including Campus failure. This coupled with change in the profile of the data volumes introduced by NBS, necessitates the move to four Correspondence Servers per Cluster, all in active communication with Outlets.

The NBS will be operational 24 hours per day, 7 days per week, every day of the year. Pathway has operation requirements to take Correspondence Servers out of service for maintenance activities. The addition of two active Correspondence Servers to each Cluster provides the necessary operational flexibility, allowing a Correspondence Server to be removed from the Cluster for maintenance without impinging on the resilience of the Correspondence Server messaging layer, and therefore reducing the risk to loss of availability of NBS to the Outlets. [NBR245]

The resilience offered by Riposte will remain unchanged, that is messages received by one Correspondence Server will be reliable replicated to other servers within the Cluster, over either of two network routes. Single network failure will not stop a Correspondence Servers within the Cluster replicating to servers at the other Campus. Failure of a Correspondence Server’s default gateway will have stopped communication with Counters therefore there is no risk of delaying or impacting the [R]/[A] message flow.

11.5.5 Generic Agent Servers (were Agent Servers)

The term “Generic” is used to differentiate these from the new *NBS Agent Server* platforms, which have particular security requirements that make it inappropriate to run them on the existing platforms. These servers will be upgraded to provide additional processing power.

11.5.5.1 Hardware

To provide additional processing capacity for the harvesting of confirmation messages and to reduce harvesting time, the existing (Generic) Agent Servers will be upgraded. This upgrade should be required no earlier than April 2003, and is therefore targeted at BI4.

The specification for these platforms is:

- Minimum Form Factor (1U Compaq Servers).
- 2 x 1.5 GHz Intel Pentium 4 Processor (or faster)
- 512 Mb memory
- 2 Network Ports
- No significant storage is required on this system – standard system disk will be sufficient.

11.5.5.2 Software

The *NBS Confirmation Harvester Agent* (see Section 5.7.4) will run on this platform.

11.5.5.3 Configuration

The four Generic Agent Servers at each Campus will be configured so that two will use the existing Correspondence Server and two will use the new Correspondence Server on that Campus as shown in Figure 42.

The configuration of the existing Interactive Agents need to understand the new Correspondence Server configuration. This is done by changes to the *Look Up Cluster* (LUC) software.

The Riposte services on the Agent Servers will be changed to connect to the same four IP addresses that the Counters use – one per Correspondence Server.

11.5.5.4 Networking Services

The Agent Bulk Servers will continue to use a single network path to the Correspondence Server. They will be configured to use the opposite network path to the Correspondence Server to the one that the Outlets use, in order to spread the load across the two different LANs. This is to make the network easier to understand and implement. In the event of a network failure, one Correspondence Server is effectively “dead”, with the other taking the full workload.

11.5.5.5 Resilience

By splitting the Agent load on each Campus across two Correspondence Servers, the Generic Agent Servers are inherently more resilient.

The *NBS Confirmation Harvester Agent* has been specifically designed as an Interactive Agent to protect against the performance impact of pulling messages from the Correspondence Server disk. Adversely long delays in recovering the Agent will result in the recovered process needing to pull a significant number of messages from Correspondence Server disk filestore.

11.5.5.6 Other Impacted Areas

Tivoli *Agent & Correspondence Server Resilience & Recovery* (ACRR) will be updated to reflect the new Agent/Correspondence Server configuration.

11.5.6 VPN Servers

11.5.6.1 Hardware

To deal with the expected increase in network traffic in peak periods, the VPN Servers need to be upgraded. The new specification needs to be:

- Fastest single processor Intel Processors available, that have the desired form factor
- Dual Network Cards
- 256 Mb memory
- Minimum on board disk storage (standard system disk will be sufficient).
- Minimum form factor (1U Compaq Servers).

Note that this change will save an estimated two 19" racks per Campus.

11.5.7 KMA Server

The KMA server needs to be able to support an increased number of keys for NBS, and to distribute these to the *NBS Agent Servers* and *NBE Gateway Server – Local* platforms.

11.5.7.1 Hardware

No change is expected in the current processor or memory of the KMA server. In order to support the significant increase in keys for NBS, more disk capacity is required in the new EMC disk array for the Host system.

11.5.7.2 Software

In support of the upgrade of the KMA Database to SQL Server 2000, a number of workarounds introduced for CSR+ need to be removed.

11.5.8 Audit Server

This platform will be provided with additional disk storage to deal with the additional audit streams. (BI3)

The enhanced *Audit Checksum Database* (see Section 13.5.3) will be built using SQL Server, so the software required to support this needs to be added to the platform.

Add a Tape Silo as described in Section 13.5.4.3, and appropriate silo management software.

11.5.9 SSC Support Server

This platform will be provided with additional disk storage to deal with the additional support requirements. (BI3)

11.5.10 Domain Controllers

The NBS Agent Servers will operate in a separate security domain (PWYPUB). A PDB and a BDC is required for each Campus. These are low-specification NT servers.

11.5.11 Firewall Modules

Eight additional Firewalls are required, two pairs per Campus, to surround the DMZ (see Section 10.7.2.5).

11.5.12 Campus LAN Switch

These are upgraded to Cisco 6513 Routers as described in Section 10.5. There are two switches at each Campus.

11.6 OTHER PLATFORMS

The IBM site at Warwick contains a pair of S/390 Computer Systems that provide the NBE service. They are in a clustered (Sysplex) configuration running (in Main-Main mode of operation) the *Connex* software package which supports the interface between the NBS Agent Servers and the Financial Institutions, via LINK or directly.

A standby single S/390 system is provided at IBM Greenford. This is normally assigned to other work It will require around 30 minutes to close down and reload as an NBE in a disaster situation.

11.7 PLATFORM INTERCONNECTIONS

The full set of Platforms installed at BI3 is as shown here. This diagram is derived from the [TED], and will be used to update that document in due course.

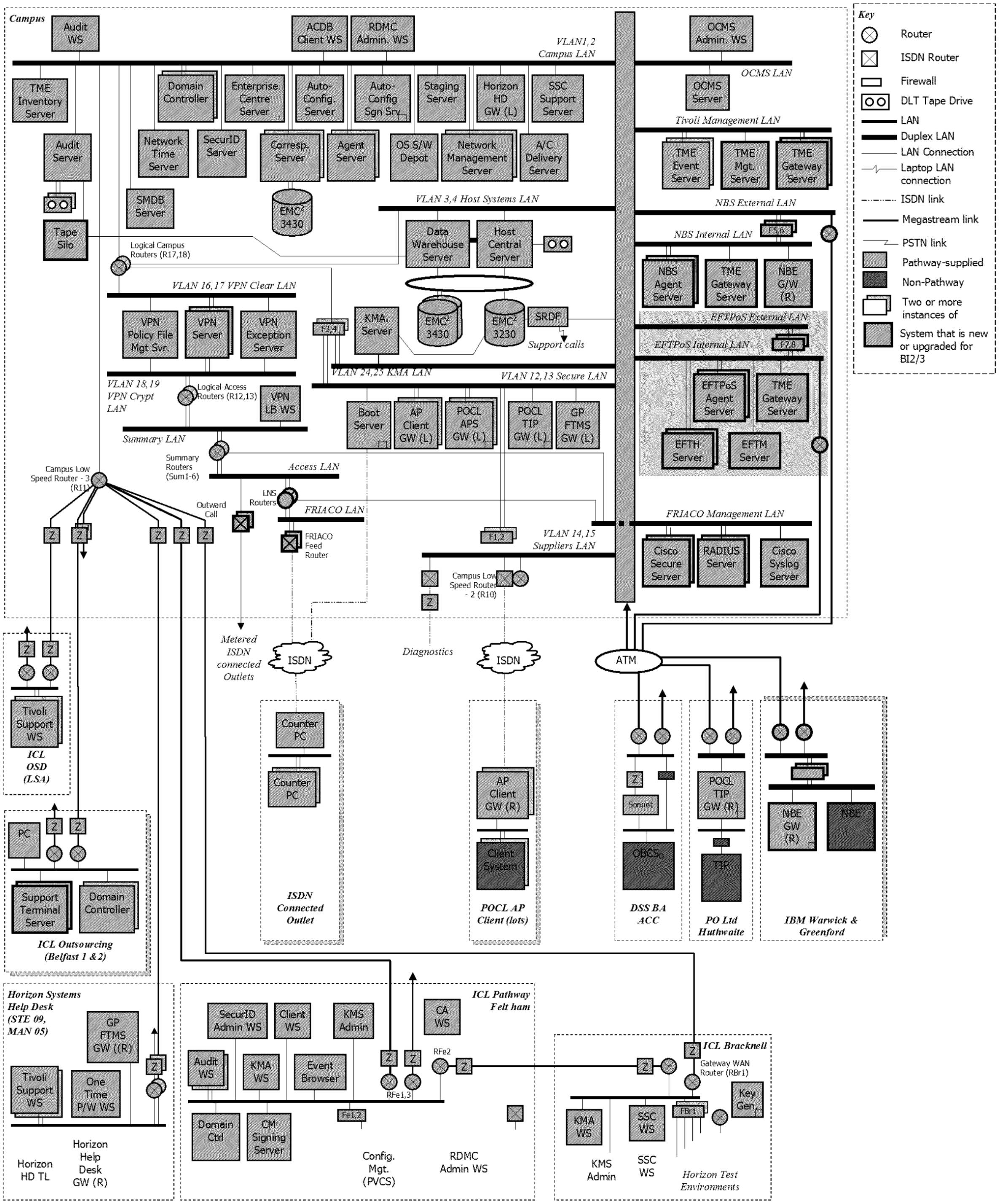


Figure 31 – Horizon Platform Interconnections at BI3

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

Chapter 12 - Systems & Estate Management Infrastructure

12.1 GENERAL

This Chapter discusses the enhancements to the Horizon Systems Management products and toolkits needed to support NBS.

12.2 REQUIREMENTS SUMMARY

- Changes are required to the software distribution mechanisms to handle the introduction of FRIACO network technology, in particular the fact that this is a dial in-only network
- Estate Management changes and bulk migration tools are needed to support the new network types for FRIACO
- PIN Pads must be included in the systems management facilities
- The enhancements to the Horizon application architecture introduced by the use of WebRiposte cause various changes to the configuration of the Counters. Counter configuration information is held within ACDB and "replayed" when a new Counter is introduced or when substantive changes are required. ACDB itself must change to accommodate the changes introduced for NBS, and all configuration information will be replayed as a result
- A number of new platform types are introduced at BI3. These require management in the same way as other Campus platforms

12.3 IMPACT ON EXISTING TOOLSET

Pathway has developed an extensive Systems Management infrastructure to support the complexity and scale of the Horizon infrastructure. These core services include the following.

- Time synchronisation
- Event management
- Software distribution
- Remote operations
- Distributed monitoring
- Estate Management

These services are provided within management domains using a range of management products and bespoke software. These domains are:

- The Counter estate, comprising the Counter PCs in Outlets
- Campus NT platforms and remote FTMS platforms

- Campus Dynix platforms
- Campus Solaris platforms, firewalls
- The network infrastructure (ISDN and other routers)

The management products deployed in these domains are as follows.

- The enterprise level product is Tivoli
- The Counter estate management product is Tivoli
- The Campus NT server and remote FTMS platforms management product is Tivoli
- The Campus Dynix domain management product is BMC Patrol. A gateway is provided to enable overall management by the Tivoli enterprise management product
- The Solaris domain management product is Tivoli
- The network infrastructure is managed by HP OpenView. A gateway is provide to enable overall management by the Tivoli enterprise management product

These domains and the products used continue unchanged for NBS.

12.3.1 Tivoli Management Framework

12.3.1.1 Tivoli Scalability

Extra Tivoli management platforms will be added for NBS commensurate with the reduction in software distribution windows, so that software distribution concurrency can be increased.

12.3.1.2 Tivoli Security

The *NBS Agent Servers* are protected from the main Campus platforms by firewalls. The firewall rules mandate the use of fixed TCP ports. Tivoli, in its standard deployment, uses ephemeral ports and so the port allocation number is unpredictable. The standard Tivoli approach to this is to deploy a TME Gateway Server on the same side of the firewall as the managed platform and enforce fixed ports in the management exchanges between the central Tivoli Management system (TMR) and the TME Gateway Server. This will be adopted and validated for NBS.

12.3.2 BMC Patrol

There will be a need for a new Knowledge Module for the DRS applications and database.

12.3.3 Maestro

This is upgraded to Version 6.1.170 to fix a number of outstanding PinICLs. Versions beyond V6.1 either remove support for facilities that we use, or are no longer supported on Dynix.

Maestro scripts will be enhanced to support scheduling of new NBS platforms.

12.3.4 HP OpenView

12.4 TIME SYNCHRONISATION

The existing solution is based on GPS satellite receivers in the Campuses as the primary time source. Campus platforms poll for the time in UTC and convert to local time using native operating system facilities. The Counter estate uses time synchronisation capabilities inherent in the Riposte replication protocol. This continues unchanged for NBS and new platforms (such as *NBS Agent Servers*) will conform to this architecture.

12.5 EVENT MANAGEMENT

The basic event management architecture consists of selected events being forwarded from individual platforms to a central complex of TME Event Servers (aka *Tivoli Event Console*, or TEC). They are stored in the OMDB. The TEC platforms are used by the System Management Centre to process events that require human intervention. The OMDB provides both SQL access and a web interface for use by browsers.

This basic architecture continues unchanged, and new platforms will conform to it. This will include the *NBS Agent Servers* that communicate with the NBE. Existing platforms will be reviewed as to the selection of events to be forwarded to the central event system.

NBS introduces many new real time components into the Horizon system. Selected events from NBS applications will be provided with an enhanced presentation paradigm over the current TEC interface. Further discussion can be found in Chapter 20.

12.6 SOFTWARE INVENTORY AND DISTRIBUTION TOOLSET

The existing software distribution facilities will be used for the new platforms introduced in support of NBS; principally the NBS Agent Servers.

ISD (with Pathway) have developed an extensive set of bespoke facilities on top of these standard products, particularly to support Software Distribution. These include a Web enabled repository (using Oracle) that records:

- Events from all platforms
- Details of all Outlets and Counters
- Software inventory for each Counter (and Campus platforms)
- Details for automated estate management (roll out and steady state)
- Details of all Campus platforms (and remote FTMS platforms)

- This is known as the Operational Management Database (OMDB). It is exploited by a layer of bespoke software that sits above the Tivoli software distribution product. This software component (the *Automatic Targeting Engine, or* ATE) aims to minimise the time taken to distribute new or upgraded software to the Counter estate by optimising the use of the ISDN network. It will be enhanced to handle the move towards a FRIACO-based network as described in Chapter 10

12.6.1 Software Distribution in a FRIACO Based Network

This Section describes the changes that need to be made to the Software Distribution mechanisms to support the FRIACO-based network described in Chapter 10. The principal feature of this is that the new network will be based around an asymmetric paradigm in which the vast majority of Outlets communicate with the Campuses solely by means of Outlet-initiated ISDN. This is in contrast to the current service, where ISDN calls may be established at the Campus or Counter with no difference in financial cost or quality of service.

12.6.1.1 Current Software Distribution Model

The current ATE system controls and optimises the use of ISDN lines from the Campus, and therefore assumes it is in control of call establishment. It is Campus-centric, in that all distributions are “pushed” from the Campus. It control the targeting of end systems, based on the current network architecture and is designed to optimise the use of the existing 1,440 ISDN lines**.** The *Tivoli Management Regions* (TMRs) are replicated across a number of TME Management Servers, and Outlets are allocated to these TMRs such that effectively the network resource is partitioned between them.

At BI1, there is a single TMR (with warm standby) that 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

With this configuration, any increase in ISDN lines would require the deployment of extra TME Gateway Servers.

The software inventory (part of OMS) is developed by Pathway. It relies upon analysing the Tivoli logs for a particular distribution, and updating the OMDB with package installation details for each Counter.

12.6.1.2 Basic Requirements for a New Model

Any new model must meet the following constraints.

- Use Tivoli, though new versions may be acceptable subject to commercial constraints
- Minimise the disruption to existing management organisations and processes (including ISD SMC, ISD MSS, Pathway Release Management, Pathway installation script production (IPDU))
- Be available in good time to support the introduction of the new network topology
- Support all existing *Operational Level Agreements* (OLAs) and SLAs in this area
- Minimise bespoke development

- Exploit the new network architecture and its capability for cost reduction but retain agility for emergency situations

12.6.1.3 Characteristics of the New Model

From the Software distribution perspective, the network service can be characterised as:

- Connectionless network service over IP
- Secure network level provided by VPN

There are three types of underlying ISDN Layer 2 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 is the current ISDN service, but at BI3 will see a drastic reduction in the number of ISDN lines
- *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 will be differences between the QoS of each service, but is assumed that these will not be apparent to a (primarily) TCP based application like Tivoli, and that 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 exact mix of services to be purchased is the subject of current negotiation.

12.6.1.4 Operation of the New Model

It is very much more efficient to continue with the scheduling located in ATE rather than adopt a Counter centric polling strategy. This also minimises the amount of redevelopment needed in response to the changed network architecture. Thus, a facility will be provided in the Counter to provide an ISDN call back capability. A small number of ISDN PRI lines will be retained in the Campus, and these can be used by the ATE to initiate a call to a dial-in FRIACO Outlet. The Gateway PC in the Outlet will be set to reject any such call and immediately calls back the Campus. The application (i.e. Tivoli software distribution) will sees a successful TCP connection, and proceeds with its distribution.

The ATE can thus also continue to handle permanent FRIACO Post Offices as in the current implementation.

The ATE changes are therefore constrained to the connection scheduling subsystem, where the algorithm will be changed to take account of the new network types. The type of network available will be held within the system management data for an Outlet. The components involved are as shown below.

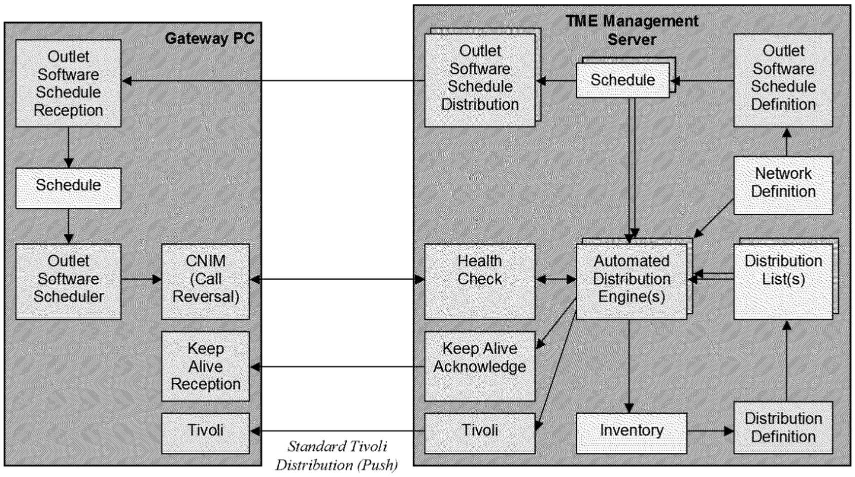


Figure 32 – Software Distribution with Call Reversal

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 D*istribution List.* The current Pathway product is the ATAD
- At well-defined periods (the Software Distribution Schedules) 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; see Section 10.4).
- Distribution then proceeds as in the current model.

The attraction of this approach is that there are no major changes in the Campus components. The principal change is enhancement of the *Health Check* algorithm to batch the checks. The batch size will be determined by the number of (retained) outward call lines divided by the number of ATEs. The *Outlet Software Scheduler* informs the CNIM function when it is to perform the call reversal, and when it is to cease to do so.

12.6.1.5 Scheduling

Initial implementation will maintain the current number of TME Management Servers, which are sufficient to drive 1,440 ISDN lines as in the current solution. This is sufficient for normal software distribution needs if the current overnight windows remain the same. However, the introduction of a large number of permanently connected Outlets does provide the potential to increase the number of TME Management Servers and thus reduce the software distribution window. Each additional server can handle up to 100 lines.

12.6.2 Management of PIN Pads

Software distribution facilities will be provided for PIN Pad software to exploit the facilities supported by the firmware, and to enable update of this firmware, of the Hypercom HFT117. The serial numbers of PIN Pads will be recorded in the OMDB inventory, and associated with the Counter to which they are attached. [PPR031]

12.7 REMOTE OPERATIONS

Within the Tivoli management system, remote operations are handled through the provision of Tivoli tasks. These provide the ability for a Tivoli user to execute a nominated script on a selected platform under Tivoli management. Role control can be applied to the Tivoli user and the scope of the nominated platforms. Auditing is also automatically performed on script invocation.

The task infrastructure continues to be available and will be further exploited for NBS diagnosis and repair. Chapter 20 identifies some of the new requirements in detail.

12.8 DISTRIBUTED MONITORING

Distributed monitoring provides a framework within which specified scripts can be periodically executed on a platform. These scripts can return status or other conditions that can be forwarded to the central Tivoli systems. This permits the status of the nominated resources to be monitored.

New resources and scripts will be developed as required for new platforms and applications. Chapter 20 discusses some changes.

12.8.1 Agent and Correspondence Server Monitoring

The NBS Agent resilience strategies defined in Section 5.7 require extensive enhancements to the current monitoring model. This will be built around the Sentry monitors on these platforms writing status information into a new decision processing engine, rather than (as at present) the central TME software carrying out extensive monitoring of these platforms.

12.8.2 Performance Monitoring Service

Performance monitoring of the live system needs to be improved to support the On-line nature of the NBS workload.

Changes are TBA.

12.8.3 Counter Network Monitoring

The new Counter Network Information Monitor (CNIM) operates at Level 2. It implements the Outlet's network connection type policy (voice, FRIACO dial-in or FRIACO permanent), and monitors the status of the network connection for interested applications. It also gathers and provides network information which is sent to Tivoli via the CCS which places it in the Riposte Message Store, from whence it is harvested to the OMDB.

12.8.4 PIN Pad Monitoring

PIN Pads will be brought under the distributed monitoring architecture according to the facilities of the supplier's management API. At minimum, this will include low battery conditions and total unit failures. The support tools and services to be provided will enable Pathway to monitor major failures and report them to the support centre for immediate action. [NBR534, PPR029]

12.9 ESTATE MANAGEMENT

12.9.1 Introduction

The Estate Management infrastructure provides services to manage change throughout the Counter estate of over 30,000 individual Counters located in over 18,000 Outlets. The infrastructure consists of the following key components:

- *Outlet Change Management Service* (OCMS) – this captures and validates requested changes to an Outlet or the installation of a new Outlet. It passes these requests to the Autoconfiguration subsystem and System management, together with data provided by bodies outside Pathway (e.g. ISDN numbers, FAD code, number of Counters)
- *Autoconfiguration Database* (ACDB) – is used to personalise new Counters when they are first installed in Outlets, either following the introduction of a new Outlet or when introduced as a spare replacement in an existing Outlet. It generates and stores the Counter configuration data (known as an *Autoconfiguration File*, or ACF) for all Outlets. The ACF is passed to the System management service and is used at Counter install time to automatically configure all subsystems with Outlet and Counter specific data. Subsequently, many changes to the system that affect the properties or configuration of Counter PCs are made by modifications to and replay of these stored ACFs. The ACDB has algorithms to automatically allocate many subsystems parameters (e.g. IP addresses).

- *System Management*. The bespoke software added to the Tivoli product includes a suite of processes that takes requests from OCMS and ACF(s) from ACDB and uses this data to automatically configure or re-configure many Campus subsystems with new or updated information on an Outlet. It also maintains a central store of data relating to each Outlet.

For NBS, Estate Management needs to encompass:

- New or modified change requests
- New parameters
- Configuration of new Campus platforms
- Changes to configuration of existing platforms
- Changes to configuration of the Counter subsystems

The most significant change arise from the introduction of FRIACO network services, as these introduces changes such as:

- New network types (dial-in only, permanent)
- Changes to the ACF (phone numbers, Riposte parameters)
- New Routers and Router configurations
- New platforms (NBS Agent Servers)

Riposte configuration also changes to increase the number of Correspondence Servers to four per Cluster.

The following Sections look at each Estate Management component.

12.9.2 Auto Configuration

A number of such changes are required to support NBS.

12.9.2.1 Auto Configuration Database Server

All Counter ACFs will be affected by one or more of these changes, and hence all will need to be replayed as part of the introduction of NBS.

- Introduction of WebRiposte and consequential Riposte configuration parameters
- Addition of IP addresses for the new Correspondence Servers
- Change to Correspondence Server neighbour definitions for Gateway PCs in Outlets
- Change to Outlet neighbour definition for Correspondence Servers
- Recognition of new network types (FRIACO dial-in and permanent)
- Change to ISDN phone numbers at the Outlet, for example to switch to a FRIACO service
- Changes to the call characteristics at certain Outlets, for example to leave the ISDN line permanently connected
- Possible changes to the Eicon settings at the Outlet

New feeds will be required from OCMS to initiate some of these changes.

The ACDB must feed CHAP information to the new Radius Server (see Section 10.5.2.3.4) to enable it to authenticate incoming calls from Outlets.

12.9.3 Auto Configuration Counter Component

New (and changed) data fields in the ACF need to be actioned. This will include:

- New ISDN numbers (e.g. to initiate a change of network type)
- New Riposte parameters
- New Eicon parameters

12.9.4 Cluster Lookup Service

This is strictly part of the Agent subsystem. Configuration will need to be changed to support a four-Correspondence Server model. This is a configuration-only change.

12.9.5 Maestro Schedule

Changes to the Maestro schedule are needed for the following.

- Know about the additional Correspondence Servers
- Know about the additional *NBS Agent Server* platforms, and reschedule new Agent instances on failure to meet NBS SLAs
- Changes to the scheduling of index rebuilds and archiving on the Correspondence Servers
- Removal of outward call windows at 02:00, 11:00 and 14:30.

A consequence of this is that some of the associated Riposte configuration changes (for example *MaxMarkerBurst* and *MaxClientConnections*) can be set back to fixed values.

12.9.6 Operational Management Database (OMDB)

This will be enhanced to recognise the new network types within the ACF, and to store the relevant data. The Web presentation interface will be enhanced to indicate an Outlet's network type.

Riposte configuration updates for a Cluster will need to be extended to cater for the new Correspondence Server in each Cluster.

In a subsequent Release, OMDB will also handle the SLA monitoring of Reference Data delivery, and provide a data feed to the DW (as described in Chapter 8)

12.9.7 Outlet Change Management Service (OCMS)

This is enhanced to support new network types (FRIACO services), both on initial installation of an Outlet and to initiate a change to a different service type[41]

These changes need to be fed through to ACDB and Tivoli.

In addition, the OCMS database is upgraded from SQL Server V6.5 to V2000

12.9.8 Service Management Data Base (SMDB)

This mirrors part of the OMDB, and enables access to service data by users who are not permitted to access the OMDB directly. Its data feed from the OMDB will be

[41] *Bulk changes needed as the FRIACO service is progressively introduced across the estate are handled by OMDB.*

enhanced to include new network type data, and the Web presentation data will be enhanced to include this.

Chapter 13 - Security Infrastructure

13.1 General

NBS has unique security properties and requires a specific secure operational environment over and above that applicable to the existing Horizon system. Horizon will be enhanced for NBS to provide customer initiated real time financial transactions, and as such requires conformance to additional standards and practices. This Chapter provides the outline design of how conformance to these standards is to be achieved and the additional operational procedures that are needed. [NBR567]

For the security requirements of EFTPoS, see [EFTSDS].

13.2 Requirements Summary

NBS requires a level of security similar to a retail banking system. It also imposes security requirements on all organisations developing and maintaining the system.

The additional security needed for NBS is determined by the differences between the current Horizon security policies and the requirements, listed in [SOR], imposed by:

- Applicable Legislative and Regulatory obligations
- Current Contractual arrangements and Schedules for **NBS**
- PO Ltd specific requirements and constraints
- Certification and Acceptance criteria

13.2.1 Legal and Regulatory Controls

NBS should adhere to the requirements of the law and of the financial services industry.

Pathway has requested formal notification by PO Ltd of the exact nature of this requirement. [NBR503]

Pathway assumes that the relevant laws and standards are defined in [SOR], which states that Pathway and the Horizon system are required to conform to the following Laws and Regulations:

- The Computer Misuse Act
- The Electronic Communications Act
- The Regulation of Investigatory Powers Act
- The Data Protection Act (1998) ([DPA]) [NBR061]

In addition, [CAN01] states that compliance is required with:

- The Regulation of Investigatory Powers Act 2000 ([RIPA])

and that this overrides any provision in [CA].

Any additional security measures arising from contractual agreements between Consignia and partner FIs (especially the Universal Bank) will be reflected as a Change Control item to the Horizon system.

13.2.2 Current Contract and Schedules for NBS

[CA] contains several clauses that require Pathway to provide for the secure operation of the Horizon system and thus ensure the integrity, confidentiality and availability of the contained data and system against fraud and unauthorised access. The additional schedules for NBS (e.g. [CAN01]) do not reduce or mitigate these contractual requirements.

13.2.3 PO Ltd specific requirements

13.2.3.1 Audit

All transactions must be fully auditable, including voided transactions (i.e. after a [R] Request has been generated) [NBR016, NBR536]

The Audit Trail must conform with Banking Standards, PO Ltd Information Security Policy and [SECCOP]. [NBR441]

The confidentiality, integrity, validity and completeness of data has to be maintained throughout e.g. storage, processes and transmissions, including during periods of service failure and recovery from service failure. [NBR445]

Data held in Outlets can be accessed to enable PO Ltd and Consignia audit requirements to be met. Also, assistance has to be provided during the life of the contract and for six years afterwards to allow information to be accessed to fulfil obligations to supply information for Parliamentary, judicial or administrative purposes. (This implies that NBS will not require any additional audit reports to be available at the Counter). [NBR443]

Access to archived transactions (i.e. over three months old but within seven years) must be available within 24 hours of any request. [NBR260, NBR315]

Pathway notes that a Fraud Risk Management Service is outside the scope of the NBS.

Pathway will ensure that the relevant information is produced by the system, at PO Ltd.'s request, in support of prosecutions. [NBR446]

The system should be capable of supporting:

- 29 million NB transactions in year 2002/03
- 270 million NB and *Universal Bank* (UB) transactions in year 2003/04
- 532 million NB and UB transactions in year 2004/05
- 638 million transactions in years 2005/06 and 2006/07 [NBR459]

The current Audit subsystem has functioned well since it was first implemented. However, it is operating at its limits and will not, in its current guise, continue to meet the new, increased operational requirements brought about by NBS. A number of enhancements are required, as described in Section 13.5

13.2.3.2 Security Standards

Pathway will provide System Security in line with existing Horizon Security Standards.

Pathway will ensure that the Horizon system adheres to the relevant parts of PO Ltd's security standards and requirements, listed in the following [NBR501]:

- *Social Security IT Security Standards* ([DSSSEC]) – to the extent applicable to OBCS and the PO Ltd infrastructure necessary to deliver OBCS
- *Post Office Counter Information Systems Security Policy* ([POLISSP])
- A Code of Practice for Post Office Information Systems Security ([SECCOP])

13.2.4 Testing, Acceptance and Certification Criteria

13.2.1.1 Testing and Acceptance

Security testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. The detailed security tests will demonstrate that all security requirements within the Pathway operational domain meet the agreed acceptance criteria. [NBR059, NBR474, NBR549, NBR550]

13.2.1.2 Certification (Acceptance)

It is Pathway's understanding that three further levels of acceptance or certification are required for NBS:

- *BS7799 Policy and System Audit*: (see [BS7799]) An external audit of the policy and systems within each of the domains will be performed to validate conformance to BS7799 [NBR479, NBR501]
- *LINK Acceptance*: Prior to System Live Operation the end-to-end NBS Service will be required to pass the criteria identified within the document LINK Test Strategy (see [LINKTS])
- *LINK Compliance*: Annual renewal of the LINK Compliance Certificate.

PO Ltd reserves the right to carry out such checks as are deemed necessary to ensure that the specified requirements have been implemented, and the resultant systems and services are secure.

13.3 Design Principles

The following principles have been adopted in the development of the NBS security solution.

- To build on the existing Horizon system and to only require developments where they are required for the NBS project
- To minimise timescales and costs by re-using or extending existing Pathway systems or components wherever appropriate
- To provide facilities for managing cryptographic keys that are simple and cost-effective to operate and that meet all security requirements
- To provide secure, reliable components that have no single point of failure such that the predicted peak loads can not be handled

- Applications operating and or using security facilities will be required to conform to the design principles.

13.4 NBS SECURITY ARCHITECTURE

13.4.1 Security Domains

From a security view point the NBS system can be viewed as a set of intersecting security domains as shown in Figure 33. The major security issues are concerned with preserving the following properties when information transits the Horizon domain, the interfaces between Horizon and the other domains and when it is held and permanent data stores within Horizon (e.g. audit logs):

- Integrity
- Confidentiality
- Availability

For NBS, this means transition to and from:

- The Horizon and NBE domains
- The Horizon and PO Ltd domains.

The security aspects of the domains with which Pathway has no direct connection are beyond the scope of this document.

Figure 3 above shows the Operational Domains that exist within the end-to-end NBS system. The following diagram elaborates on this, and shows the Security Domains and how they map onto the operational structure.

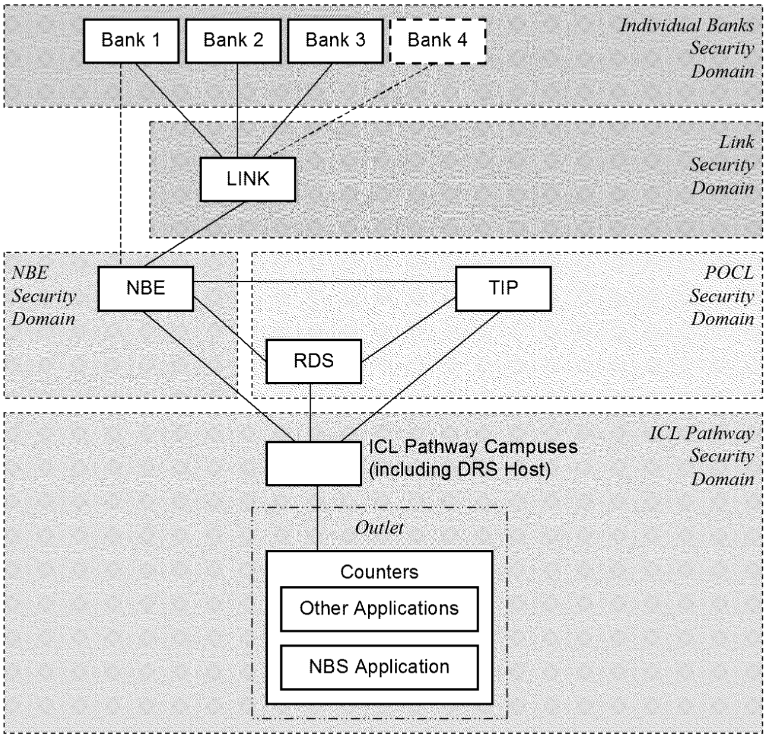


Figure 33 – NBS Security Domain Structure

13.4.2 Horizon NBS Security Architecture

The Horizon NB Security Architecture is concerned with the following components:

- The Counter and PIN Pad [NBR509]
- The Horizon NBS Security Infrastructure Services
- The Horizon-NBE boundary

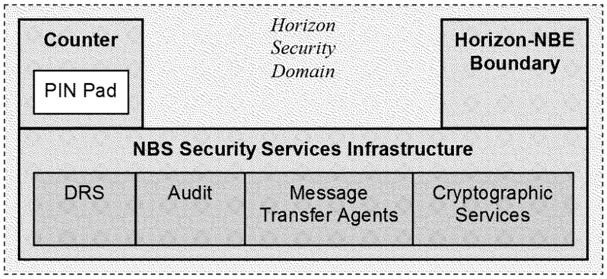


Figure 34 – Horizon NBS Security Architecture

The Counter provides a secure environment for the execution of the NBS applications. The NBS Security Services Infrastructure provides a secure environment for:

- Transferring and receiving business transactions between the Counter and the NBE
- Management of the secure environment
- Generation, distribution and storage of cryptographic keys
- Remote management of secure software and firmware components
- Providing secure facilities for the DRS and Auditing of the business transactions
- Management and use of PIN Pads at the Counters

The Horizon-NBE boundary provides a secure environment for:

- The exchange of information with the NBE
- Distribution of cryptographic keys (if required)

Within the Horizon Security Domain, any key that could directly or indirectly expose plain text PIN values and any keys used in association with MACs will be managed in accordance with the principles established in [ISO 8732] or [ISO 11568] [NBR506].

13.4.2.1 NBS Counter Security Architecture

The developments for NBS will follow the principles of [ISO 17799]. Note that Pathway is registered for ISO 9001. [NBR501, NBR559, NBR560]

The Counter Transactions have four specific security requirements:

1. Authorisation of all customer transactions
2. Protection of sensitive or confidential data
3. Ensuring the Integrity and Authenticity of all NBS transactions
4. Protection against replay of PIN Pad authorisations.

13.4.2.1.1 Verification

All NBS transactions will be authorised by the Customer prior to their completion, using either of the following mechanisms: [NBR250]

- *PIN Entry*. If a PIN Pad is available at the Counter, the Customer will authorise the transaction by entry of their PIN[42]. The customer entered PIN will be securely captured and protected by the Horizon system.
- *Customer Signature*. Reference Data may permit the Customer to authorise the transaction by signing one copy of an Office Receipt. This depends on the transaction type and IIN, and may be a blanket process for that transaction/IIN combination, or permitted only where there is no PIN Pad installed and active at the Counter position. The signed copy of the Office Receipt will be retained by the Clerk and another receipt passed to the customer. This authorisation process is outside of Horizon and is not the responsibility of Pathway or the Horizon system. A central facility outside of the responsibilities of Horizon and Pathway for the storage of receipts will be provided.

The Request [R], including the method of authorisation and any supporting data (e.g. PIN Block) will be transmitted to the NBE for onward transmission to the applicable FI for validation. [PPR001, PPR002]

13.4.2.1.2 Protecting Sensitive and Confidential Data

Sensitive and/or Confidential data recorded within NBS only relates to information that can be used to execute a fraudulent transaction. There is no *personal* data recorded that falls within the scope of [DPA]. [NBR061]

Sensitive and/or Confidential data is only processed within an [R] and consists of two classes of information:

- *Customer PIN* – entered at the PIN Pad
- *Card Details* – Discretionary data held on Track 2 of the card (captured when the card is swiped at the Counter) or card information (Start Date, Expiry Date and/or Issue Number) entered by the Clerk when the card cannot be swiped at the Counter. Note the PAN is not regarded as confidential information since it cannot be used, by itself, to execute a fraud

The mechanisms for the protection of this data are:

- *PIN*: Customers will authorise their transactions by entering their PINs at a PIN Pad. The PIN Pad is a specialized device that is connected to the Counter PC. Application transactions will interface to the PIN Pad via Riposte Peripheral Broker. The PIN Pad has a number of specific security features that include tamper resistant and/or tamper evident construction, non-echo of PIN entry and cryptographic capabilities. When entered, the PIN will be cryptographically encoded (according to the standards of [ISO 9564]) within the PIN Pad. The encoded PIN is combined with other information within a specific structure and format, and transmitted to the Counter PC together with the *Key Serial Number* (KSN)[43]. The application will include the PIN Block and the KSN (as part of the PIN_Block_1) within the [R] passed to the Campus. The cryptographic mechanism used, *Derived Unique Key Per Transaction* (DUKPT), will provide a unique cryptographic key value for every PIN encoding request. [NBR575, NBR576]

[42] *If the customer doesn't have a PIN or does have a PIN but for some reason is not able to enter it then customer signature could be used.*

[43] *The KSN reveals to the recipient which PIN Pad was used and which BDK the PIN Block encryption key is based on, as well as a transaction sequence number*

- *Card Details*: The Card details are captured either when the Clerk swipes the Card or when it is manually keyed. This information is sent to the NBE within the [R] message. The sensitive data is encrypted prior to passing the message outside the Counter.

  Encryption is carried out by the Crypto API. This interface will be enhanced for NBS. The encryption algorithm used is Red Pike and will employ a single key that is applicable across the whole estate. [NBR538]

  The purpose of this encryption is to prevent the card details being visible to any person with access to the Horizon systems through which it passes.

13.4.2.1.3 Integrity and Authenticity

Across the Horizon infrastructure, NBS transactions are potentially exposed to a number of different attacks; for example change of message content or insertion of false messages. Countermeasures to forestall these threats are to ensure the Integrity and Authenticity of messages that originate at the Counter.

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 in the Outlet, the signature is generated and applied in the *Request/Reply* hook (for [R] messages) and the *Finalise* hook (for [C] messages) and is applicable to the XML content of the message i.e. the XML attributes and values, 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 *Request/Reply* hook at 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 (OCPR). 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 (COPR). Further details on the cryptographic features are provided in Section 13.4.3.

13.4.2.1.4 Protection against Replay

The communications link between the PIN Pad and the Counter does not employ any specific protection mechanism e.g. encryption. As such, it is possible to tap this connection and mount a Replay attack, at the same or another Counter at the Outlet, using the recorded value of the encrypted PIN and KSN. To forestall this threat security relevant features will be added to the PIN Pad Driver in the Counter: [NBR580, NBR581]

- When the PIN Pad is first installed, the Driver will record and securely store the PIN Pad Serial Number and transaction sequence count
- On every subsequent interaction with the PIN Pad, the Driver will check all return values to ensure that the PIN Pad Serial number is the same as the stored value and that the returned Transaction Sequence count is greater than the stored value. If either of these checks fails then an error code will be returned to the calling application that will abort the transaction and report the error in both the Security and Application Log Files for onward reporting to the Security and System

management authorities. Note for a successful transaction the stored sequence count will be updated with the received sequence value

- The stored values will be held under an appropriate protection mechanism[44]
- Under certain conditions (e.g. OBC – for Multi-Counter Offices) it is possible that the pairing of the Counter PC and PIN Pad could be "mixed" within the Outlet. On boot up, code within the Counters will validate the presence of their initially installed PIN Pad. If this validation fails, then the engineer will be requested to perform a process to confirm installation of new PIN Pad[45]. See Section 12.6.2.

13.4.2.2 Message Processing Security Architecture

13.4.2.2.1 Authentication Message Processing

Figure 35 illustrates the major architectural components of the secure Counter to NBE environment for processing [R]s and [A]s. It shows how:

- Messages in transit are protected by a Digital Signature between the Counter and the *NBS Authorisation Agent*, and then by a MAC from the NBS Authorisation Agent to the NBE [NBR228, NBR570]
- PINs are protected by hardware encryption.

This architecture assures:

- The Integrity, Authentication and Non-repudiation of NBS Transaction across the Pathway Infrastructure
- The Integrity and Authentication of exchanges with the NBE.

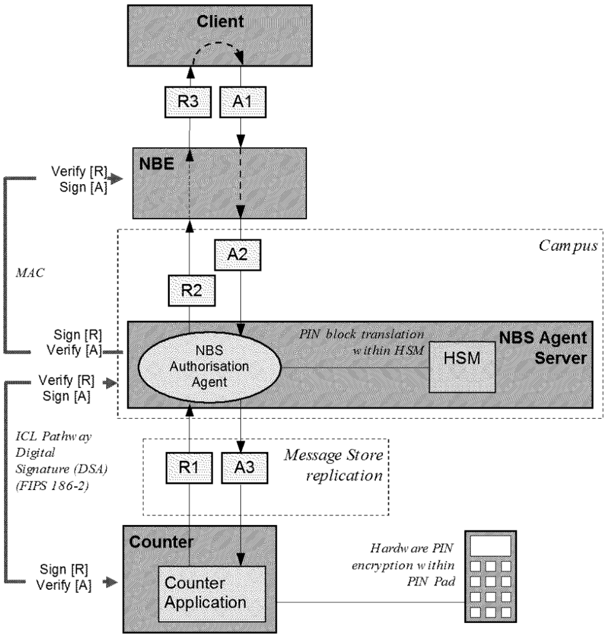


Figure 35 – Protection of Authentication Messages

[44] The mechanism for protecting these values will be determined as part of the design activity for supporting PIN Pads

[45] This proposal is subject to detailed design investigations.

The HSM in the NBS Agent Server is used to meet LINK and other requirements on the translation of the encrypted PIN value between the Horizon and NBE domains. In addition, the HSM is used for MAC authentication and verification, and re-encryption of sensitive data in messages exchanged with the NBE.

The message content may be considered as shown in Figure 36, which illustrates that certain messages attributes are encrypted, and the whole message digitally signed. All fields (including the digital signature) are represented by XML constructs.

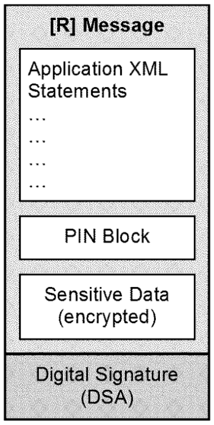


Figure 36 – Logical [R] Message Content – Security Perspective

13.4.2.2.2 Confirmation Message Processing

Note the more complex architecture for processing [C]s and [D]s messages, as shown here.

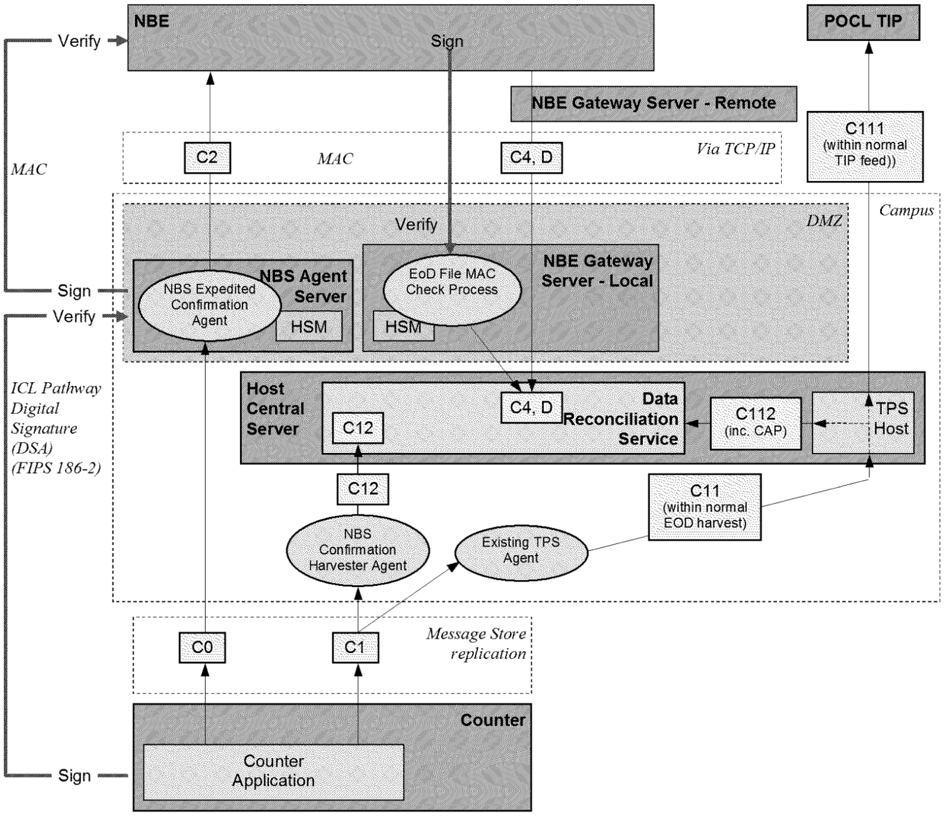

NBE
Verify
Sign
POCL TIP
NBE Gateway Server - Remote
C2
MAC
C4, D
Via TCP/IP
C111 (within normal TIP feed))
MAC
Campus
DMZ
Verify
NBS Agent Server
NBS Expedited Confirmation Agent
HSM
EoD File MAC Check Process
HSM
NBE Gateway Server - Local
Sign
Verify
ICL Pathway Digital Signature (DSA) (FIPS 186-2)
Host Central Server
C12
C4, D
Data Reconciliation Service
C112 (inc. CAP)
TPS Host
C12
NBS Confirmation Harvester Agent
Existing TPS Agent
C11 (within normal EOD harvest)
C0
C1
Message Store replication
Counter
Counter Application
Sign

Figure 37 – Confirmation Message Processing

The [C0] message will be signed and verified during transit of the Horizon infrastructure in a similar manner to [R1] messages,

Files of [C4] and [D] messages received from the NBE will be copied to the DRS Host, and then verified by an *EoD File MAC Checker* process running on the *NBE Gateway Server – Local.* This platform will be provided with an HSM and the relevant Crypto libraries and supporting software.

Once the MACs are confirmed, the files can be loaded into the DRS and used in the reconciliation process.

13.4.2.3 Boundary Protection – Horizon to NBE

The interface between the NBE and the Horizon security domains will be subject to a Boundary Protection System. The purpose of this is to protect the Horizon environment from unauthorised interactions with the NBE. The detailed network configurations are described in Chapter 10.

13.4.3 Key Management Model

The Key Manager will view the task of key management from an understanding of the Pathway technical environment and the business functions it supports. He will therefore think in terms of keys under his management control. Each of these divisions is a "Protection domain".

Within one protection domain, the cryptographic functions implement a particular "Cryptographic algorithm" (e.g. DSA, Red Pike). Conversely, one algorithm may be employed in several domains.

Within one protection domain there may be many separate "Cryptographic relationships". For example, every individual Outlet is accountable for the AP transactions that it conducts. Therefore, the AP Transaction Harvester must be able to distinguish the digital signature of one Outlet from those of another. That is to say that each Outlet has a separate relationship with the Harvester within the AP protection domain.

A cryptographic relationship is distinguished by the fact that the participants share a unique "Key set". At first sight, one might therefore expect a 1:1 relationship between "Cryptographic Relationship" and "Key Set". However, the entity relationship takes into account the fact that the keys in a particular relationship will be changed at routine intervals, or in case of compromise. So, over time, one cryptographic relationship will use a series of key sets. A cryptographic relationship may also use more than one key set at the same time. [NBR574]

The protection domains for NBS are described in Table 27 and use the following convention[46].

- Names are 5 characters or less
- "NB"' in the first 2 characters denotes a Protection Domain applicable to NBS
- "O" denotes Outlet
- "C" denotes Campus
- "P" denotes PIN Pad
- "TD" denotes Transaction Data
- "MC" or "MAC" denote Messages Authentication Code

Protection Domain	Application area	Algorithm	Comments	Key Names	Number of Keys in Use	Key Life Time
NBOC	NBS: Outlet to Campus	DSA1	Counter signs NBS Authorisation Agent verifies [NBR569]	OCPR, OCPU (aka APPR, APPU)	20,000	2 years
NBCO	NBS: Campus to Outlet	DSA1	NBS Authorisation Agent signs Counter verifies [NBR558, NBR569]	COPR, COPU	1	2 years
NBC2N	NBS: MAC Campus to NBE	Triple DES	Transient key NBS Authorisation Agent generates [NBR569, NBR570]	NBMCC	1 per NBS Agent Server	24 hours
	NBS Transaction Data		Transient key NBS generates NBE Translates [NBR569, NBR570]	NBTDC		
NBMCN	NBS: MAC NBE to Campus	Triple DES	Transient key NBE generates [NBR569, NBR570]	NBMCN	1	24 hours
NBPO	NBS: PIN Block encryption (Outlet)	DES	PIN Pad encrypts NBS Authorisation Agent decrypts/translates3	NBPO (derived using DUKPT)	1 per PIN Pad	Current transaction

[46] *This convention is a guideline and not an enforced rule.*

NBPC	NBS: PIN Block encryption (Campus)	Triple DES	Self-authenticating transient key4 KMA/NBS Agent generates NBE decrypts [NBR558]	NBPC	1 per NBS Agent Server	24 hours
NBLE	NBS-NBE link encryption	Not known	Hardware2 link encryption/decryption on the dedicated comms link between the Campus and the NBE site [NBR573]	NBLE	1	N/a
NBTDO	NBS Transaction Data	Red Pike	Counter application encrypts selected transaction data NBS Agent decrypts	NBTDO	1	1 month
NBTDC	NBS Transaction Data	Triple DES	Transient key. KMA/NBS Agent generates NBE translates	NBTDC	1 per NBS Agent Server	24 hours
NBZMK			Key Encryption Key (KEK) held by Horizon & NBE. Used to encrypt NBS Keys in messages interchanged between Horizon and NBE	ZMK	2	6-12 months

Table 27 – Protection Domains

Notes:

1. Proposed use of DSA gives the ability for Counter NBS application to use existing Pathway Crypto software
2. E.g. Zergo Rambutan or Racal Datacryptor
3. The decryption/encryption between the NBPO and NBPC domains are carried out as a single translation, so that the PIN Blocks do not appear in clear except in the HSM [NBR577]
4. These keys are encrypted under the current *Zone Master Key* (ZMK) and included in the message itself. The keys are transient in that new keys could be used for each message. However, for efficiency reasons, each key will be used over a period of time up to its lifetime.

Note also that keys used for PIN encryption (NBPO) is not used for any other purpose. [NBR578]

13.4.4 NBS Messages Flows and Security

The NBS Financial Transaction Data Flows (the RAC Model) is shown in Figure 5. There are security issues surrounding the [R], [A], [C] and [D] message flows (in both directions) between the Counters and the Campus (the *NBS Authorisation Agent* and *NBS Confirmation Harvester Agents*) and between the Campus and the NBE. [NBR564]

For the Counter-Campus flow the security requirement is for:

- Authentication
- Integrity
- Non-repudiation

For the Campus-NBE flow, the requirement is for:

- Authentication
- Integrity

The Crypto API provides interfaces that enable the relevant application components to sign, verify, encrypt and decrypt message portions.

13.4.4.1 Keys Used in Message Transfers

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.

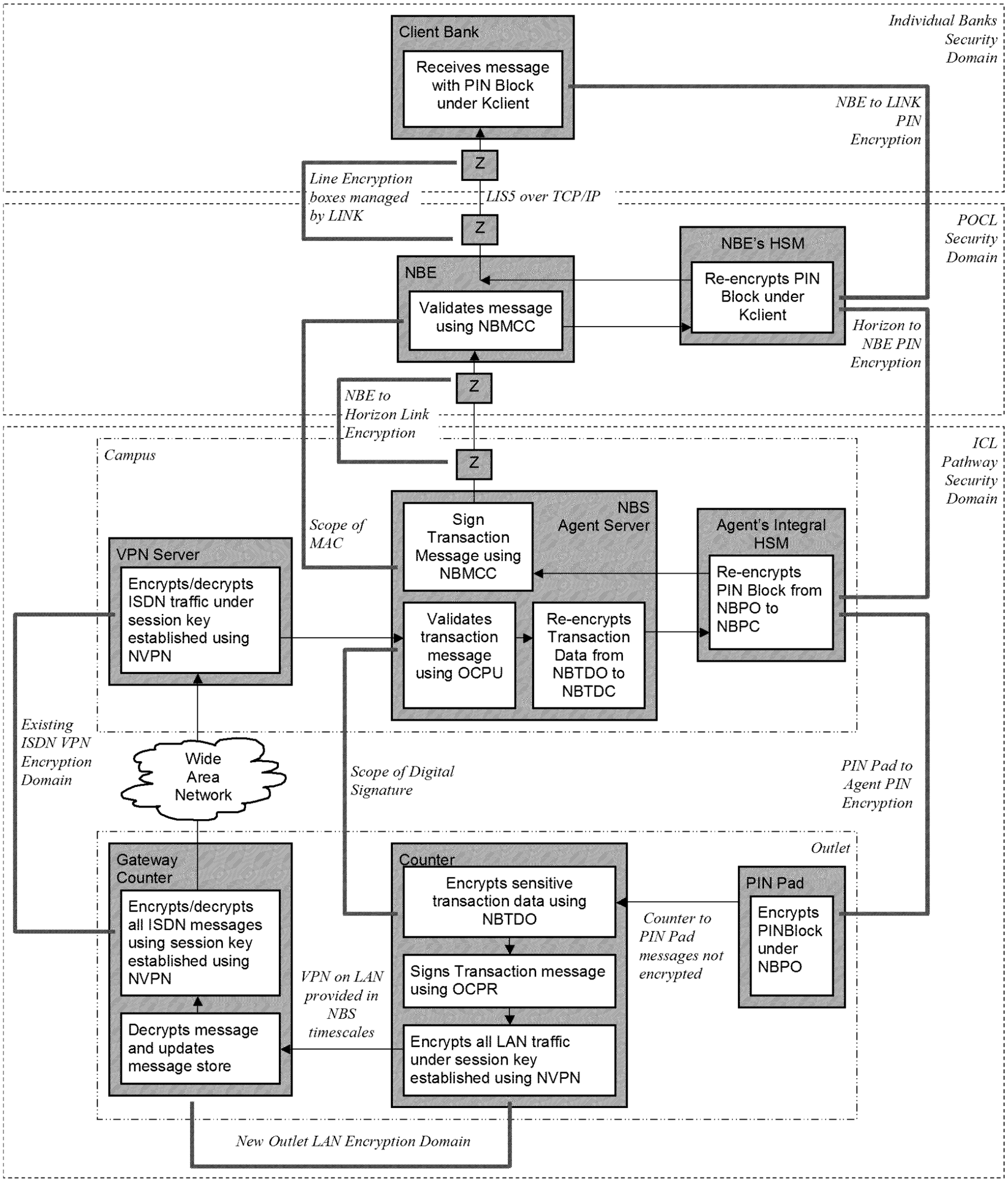

Individual Banks Security Domain
Client Bank
Receives message with PIN Block under Kclient
NBE to LINK PIN Encryption
Z
Line Encryption boxes managed by LINK
LIS5 over TCP/IP
Z
POCL Security Domain
NBE's HSM
Re-encrypts PIN Block under Kclient
NBE
Validates message using NBMCC
Horizon to NBE PIN Encryption
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 38 – 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.

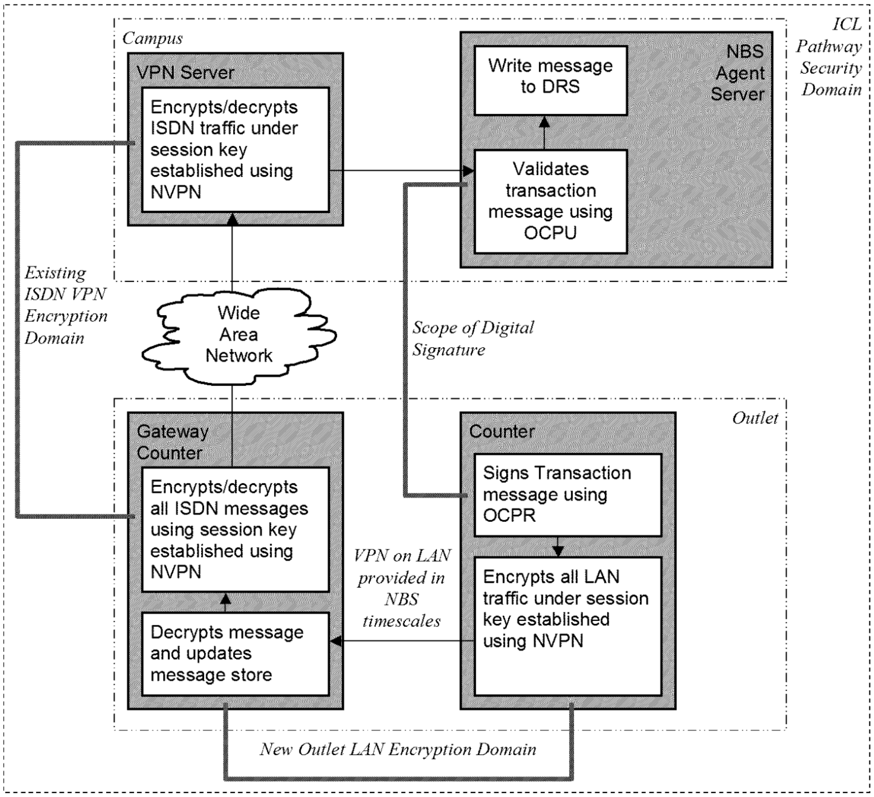

Campus
ICL Pathway Security Domain
VPN Server
Encrypts/decrypts ISDN traffic under session key established using NVPN
NBS Agent Server
Write message to DRS
Validates transaction message using OCPU
Existing ISDN VPN Encryption Domain
Wide Area Network
Scope of Digital Signature
Outlet
Gateway Counter
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 39 – 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.

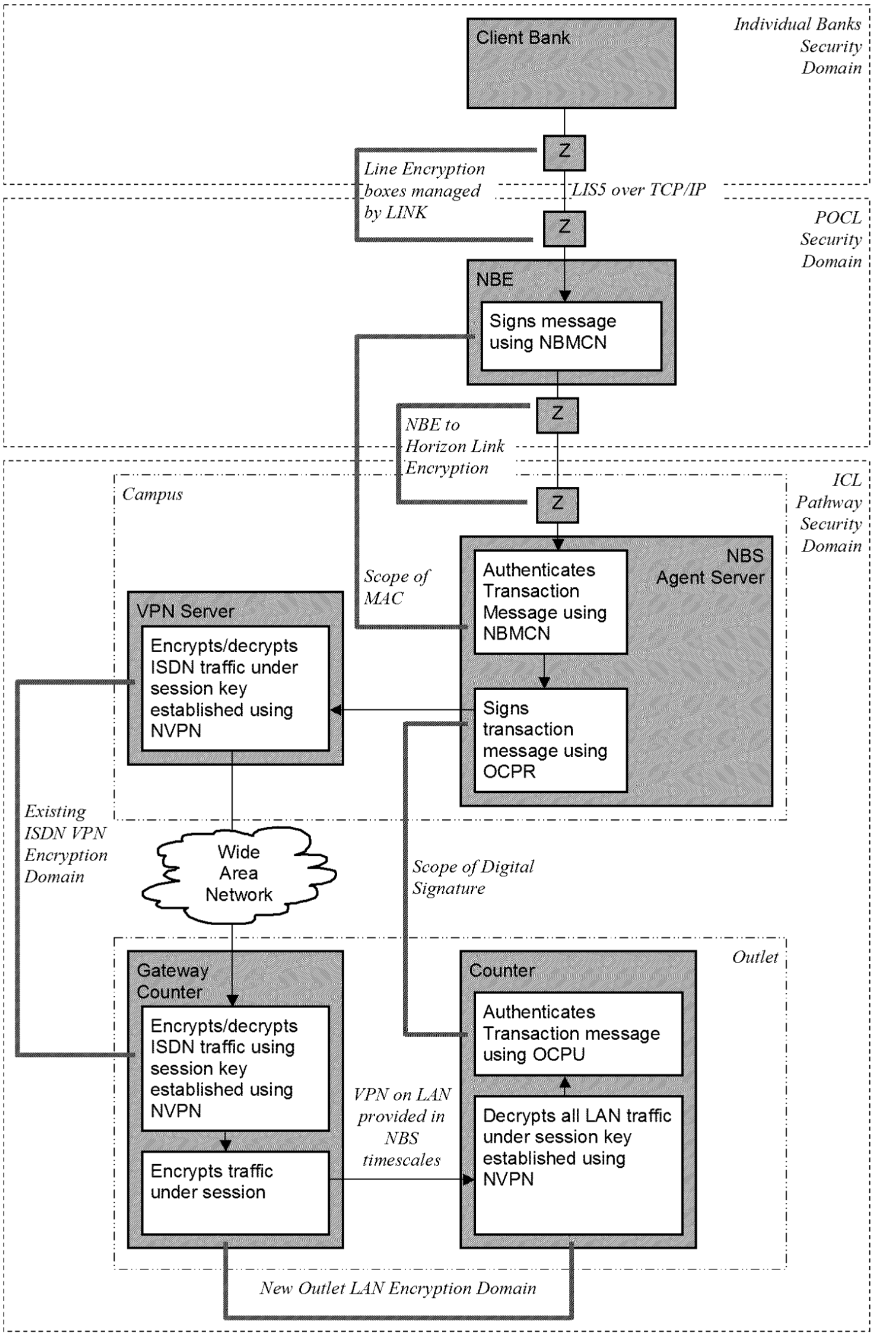

Individual Banks Security Domain
Client Bank
Z
Line Encryption boxes managed by LINK
LIS5 over TCP/IP
Z
POCL Security Domain
NBE
Signs message using NBMCN
Z
NBE to Horizon Link Encryption
Z
ICL Pathway Security Domain
Campus
NBS Agent Server
Authenticates Transaction Message using NBMCN
Scope of MAC
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 40 – Use of keys in [A] Messages

E3.4.5 Encryption of Working Keys

Working Keys are the keys used by the HSM to translate PIN values and for other purposes. They will be encrypted as specified in [ISO 8732]. Each working key will be represented as a 128-bit string with odd parity prior to encryption. The ZMK used to encrypt the Working Key may be modified by a variant prior to use. [NBR501, NBR582]

13.4.6 HSM Key Management

The Compaq Atalla HSM cards will need to be initialised with their first set of keys before deployment.

Keys are generated using the Atalla *Secure Configuration Terminal* (SCT). This is directly connected (via RS232) to a bespoke free-standing NT workstation[47], the HSM Key Generation Workstation (see Section 11.4.2) onto which is loaded the Atalla key loading software tools. Each Atalla card is installed in this workstation in turn, and its initial keys established. It is then removed and installed on the target platform (NBS Agent Servers or KMA Workstation).

None of this process requires any bespoke Horizon software to be developed.

13.4.7 Platforms and Connections

Figure 38 and Figure 39 show the principal platforms involved in the security architecture.

The Platform Types in the existing Horizon system are:

- Counter PC
- KMA Server
- KMA Workstation
- Audit Server

For NBS the following new Platform Types are defined:

- NBS Agent Servers
- Network Banking Engine (NBE)
- PIN Pad and HSM Key Generation Workstations
- PIN Pad Key Priming Platforms (if needed, proposal below uses Counter PCs for this).

It is assumed that the NBS Agent Servers support a Riposte service and that this can be used for key distribution.

13.4.8 NT Domains

The Horizon NT Domain Structure needs to be enhanced to include the new platform types identified above. The design principles applied to this update are:

- Maximise security configuration applied to the NBS Agent Servers
- Maximise reuse of existing security configuration
- Minimise disruption to the existing NT Domain structure
- Minimise changes to operational management and support processes

With these aims in mind, the following NT Domain structure changes are proposed:

- Introduce a new Resource Domain dedicated to contain the new NBS Agent Server platforms. This domain will span both Bootle and Wigan Campuses
- Set up a one-way trusting trust relationship with the existing PWYDCS Master Account authentication domain

[47] *Located in the Pathway Secure Area*

- Configure access to the NBS Agent Server platforms for a subset of the existing Horizon secure roles

13.4.8.1 New Resource Domain

The name of this new domain will be PWYPUB. It will contain the following servers:

- 1 x Primary Domain Controller located in Bootle
- 1 x Backup Domain Controller located in Wigan
- 12 x NBS Agent Servers, six each in Bootle and Wigan

All servers in this Domain will run the WebTrends vulnerability analysis software, with reports fed to a server in the Pathway Secure Area.

13.4.8.2 Trust Relationships

The new Resource Domain must trust the PWYDCS Master Authentication Domain, which holds the Horizon Human User Secure Roles.

Connections between the existing Correspondence Servers and Generic Agent Servers located in the BOPSS and WOPSS Resource Domains and the new NBS-Agent Servers will be via Riposte. The same is true for connections between the NBS Agent Servers and the KMA Server located in the PWYKMS Authentication Domain. No trust relationships are required between the new Resource Domain and PWYKMS, BOPSS and WOPSS to support Riposte message transfer connections.

Maestro will access the NBS Agent Servers to control the scheduling of the Agents. The Agents themselves connect to Oracle on the DRS Host, and have *Remote Procedure Call* (RPC) links into Riposte on the Correspondence Servers. No additional trust relationships are needed to support these access routes.

13.4.9 Security Policy

The Pathway Security Policy ([SECPOL]) describes:

- The general Pathway NBS security philosophy
- Standards for security and metrics to determine how these standards are being met
- What is to be protected – software, hardware, data etc.
- Who (i.e. which unit) is responsible for protecting these items
- How the items are to be protected

The full Community Security Policy is defined in [NBSCSRS], to which the Security Architecture specified in this document conforms. The Pathway Security Policy will be updated to reflect the requirements of NBS. [NBR556]

13.4.10 Other Protection Domains

13.4.10.1 Audit Server

The proposals of Section 13.4.3 above assume that no new cryptographic functionality is required on the Audit Servers. This precludes offering a function on the Audit Server allowing the auditor to view or select on the in-clear sensitive transaction data that is protected in transit through the system in the NBTDO protection domain. The key management for that protection domain as described above is not appropriate for data to be held encrypted in long-term storage for future decryption.

A facility to give auditors access to the sensitive transaction data would require:

- A securely managed data-encryption key for use on the Audit Servers
- Application-controlled encryption/decryption of the sensitive data (field-level or file-level)
- Application-controlled re-encryption of *all* audit data when the data-encryption key is changed

13.5 AUDIT

This Section describes the changes required to the Horizon Audit system as a result of the new data that requires retention for Audit purposes, and the change to the length of time for which certain categories of Audit data are retained.

Note that many existing Horizon data flows, including all Riposte messages, are already captured automatically for audit purposes, and these facilities will be retained and can be exploited for NBS data. [NBR453]

Wherever an additional interface is created, or additional data flows across an existing interface that is already captured for audit purposes, the minimum changes required are as follows.

Component	Description of Change
Audit Data Catalogue	Documentation of new Audit Data
Audit Configuration	Gathering & processing Audit Data
Audit Sizing Model	Update for increased data volumes

Table 28 – Basic Changes Required for Audit

13.5.1 Horizon to NBE Interface

The interface to the NBE is deemed a Horizon boundary and all data crossing the boundary must be retained for audit purposes. This interface uses TCP/IP via a Sockets interface. This provides no appropriate audit facilities, and hence the message traffic across this interface will be captured for Audit purposes by the NBS Agents.

13.5.1.1 [R]/[A] Interface

For [R] and [A] messages, a time-stamped copy of the messages will be written as a pair to the Correspondence Server message store and hence will be collected for audit purposes. [NBR016, NBR441, NBR536]

13.5.1.2 [C4] and [D] Interfaces

Files of [C4] and [D] messages received from the NBE are archived nightly to the Audit Server to provide data for audit purposes. [NBR016, NBR441]

13.5.2 DRS to PO Ltd Interface

13.5.2.1 Settlement Support Interface

The interface whereby the DRS sends settlement data to PO Ltd is a Horizon boundary and is thus subject to audit data capture. It is expected that this interface will utilise a new or existing FTMS services that can be configured to support the collection of Audit Data. [NBR016, NBR441]

13.5.2.2 Additional TIP Data

Data transferred to TIP via FTMS is already gathered for audit purposes. No additional changes are required.

13.5.2.3 Additional RDS Data

Data transferred to or from RDS via FTMS is already gathered for audit purposes. No additional changes are required. [NBR045, NBR202]

13.5.3 Extension of Audit Archive Retention Period to Seven years

NBS transaction data must be retained for seven years. This requirement has significant implications for the audit system. Holding audit data for seven years imposes a significant additional data storage requirement. In addition, it is necessary to capture the supporting systems management data that verifies that the Horizon system was performing correctly at the point of capture of the data.

The current audit system stores checksum information on file content in an Audit Checksum database. The current database will not support the increase in file volumes and will require replacement. The new database will be built using SQL Server. [NBR260, NBR315, NBR542, NBR544]

13.5.4 Performance & Usability Enhancements

This section details the changes required for the Audit system such that the current performance is not degraded by the additional loadings and that an increase in retrieval requests capacity may be considered subject to adequate Resourcing.

NBS requirements specify that PO Ltd may request data relating to an NBS transaction at any point during the seven-year period for which such data may be retained. During the first 90 days after the transaction was committed, this data may be retrieved from the DRS. After this, it may be retrieved from the Audit Server. There are contractual limits on the number of queries that may be requested; see [CAN01]

One of the major limitations on the number of retrievals that can be serviced is the extraction process itself and the architecture of the Audit Server and Audit Workstation.

There are two stages to the retrieval process.

- Data files are retrieved from DLT and placed into directories on the Audit Server
- Relevant records are extracted from files on the Audit Workstation, analysed and written to CD

For non-Riposte files, the transition from the first to the second stage is usually achieved by "dragging" the files across the network. However, for Riposte Journals it is necessary to filter out the required Outlet FAD code(s) and date range(s) by generating a pseudo Correspondence Server message store. This work has to take place on the Audit Server, and it is not possible to run more than one such filter exercise concurrently.

This restriction is affecting the throughput of retrieval requests, and these are taking considerably longer than originally anticipated.

The current Audit Server and Workstation architecture is as follows.

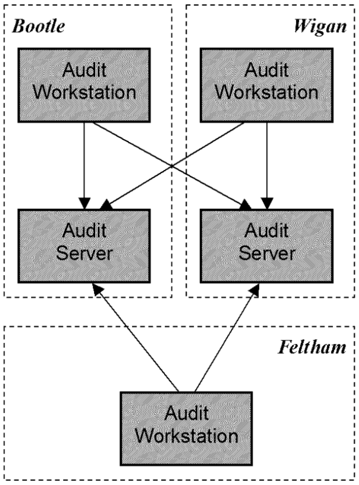


Figure 41 – Audit Workstation & Server Architecture

The workstations at Wigan and Bootle exist for resilience purposes and anticipated use by North based audit staff. In reality, these have never been used in anger and one could be moved to Feltham to provide a dual capability. However, the need to run the filtering activities on the Audit Server mitigates against any real benefit being derived from this arrangement, and hence changes are proposed to this as described below.

The current Archive and Storage implementation of the audit solution is a balance between the cost of storage and the frequency with which data has to be retrieved. Based upon the agreed number of retrievals, a solution based upon DLTs was implemented.

Since then two further categories of retrieval request have emerged.

- Retrievals in support of internal support requests, usually made by BSU or SSC. SSC requests have diminished greatly since they introduced their own rolling six-month support data store. BSU requests are exceptional and only occur when they cannot source information from the Data Warehouse.
- PO Ltd Security Investigations. This group require data to support their investigations and ultimately prosecutions for fraud. Originally they did not express any requirements for access to audit data so were not taken into account. Historically, they were to obtain their data from the Fraud Risk Management Service (FRMS), a BA service that disappeared when BA withdrew from the Horizon contract. They are now the main requesters for audit data and have stated, but not substantiated, a continuing need for ~500 retrievals per year.

The debate surrounding these latter requirements has been escalated back to the Contract and both sets of solicitors have been involved. Following meetings in May 2000 and March 2001, a letter has been sent to PO Ltd accepting that Pathway will perform 50 retrievals per rolling 12-month period. Although accepted at the March meeting, attempts to get agreement to CCN759, which would change Requirement 699 to reflect this, have been rejected. The situation remains unresolved, though it is expected that the NBE requirements for increased data retention and increased numbers of retrievals per annum will be reflected in changes to [CA].

13.5.4.1 TMS Data Storage

Riposte (TMS) Data is currently stored in a series of files per Correspondence Server per day. Each file contains a configurable number of messages. Retrieval operations extract the entire file before filtering it for the required Outlets. With the increase in retrieval volumes, this will become impractical.

The proposed change will store this data in a considerably larger number of files, each holding data for an average of 450 Outlets. Non-Outlet related data will be held in an additional volume. This change to the storage mechanism (introduction of a tape silo) will ensure that there is no degradation of current retrieval times and provide considerable ‘future proofing’. [NBR057]

13.5.4.2 Extractor File Selection

The additional data volumes for NBS transactions and the increase in retention time will seriously degrade the performance of the file selection process in the Audit Extractor. Changes have been identified that will improve the current performance, thus allowing for the increased volumes. [NBR057]

13.5.4.3 Extractor File Retrieval

The additional data volumes for NBS transactions and the increase in retention time will seriously degrade the performance of the file retrieval process in the Audit Extractor.

In addition, the handling of tapes for data retrieval is currently a manual process.

The additional number of DLT tapes within the system due to increased volume and retention period dictates that the manual handling is no longer a viable solution and automated ‘near line’ DLT storage is required in the form of tape silos.

The performance improvement will be met by migrating to a later version of Legato (with improved index and tape handling performance) as described in Section 11.3.2.6, by changes to the Audi Extractor for tape recognition and identification, by changes to the mechanism for seal verification on retrieval, and by removal of the manual tape handling. [NBR057, NBR444, NBR542]

13.5.4.4 Data Extraction – Multithreading

The current Audit extraction implementation only permits a single user connection to each Campus at any time. This effectively limits the concurrency of data retrievals to two, and thus the overall number that can be achieved to the current limit of 50 per annum.

To increase this limit, changes will be required to the Audit Architecture to remove the restrictions on the concurrency of retrievals. The changes will comprise:

- Enabling multithreading between the Extractor Client and Server
- Removal of locking restrictions on access to the checksum database
- Enabling filtering on the Audit Workstations instead of the Audit Server
- Changing filestore mapping to be exclusive to an RFI

[NBR057, NBR542, NBR546]

13.5.4.5 Audit Extractor Usability Issues

There are currently several identified usability issues with the Audit Extractor. While these are containable with the current limit of 50 retrievals per annum, any increase in this limit dictates that they should be resolved to enable an efficient service to be provided.

The current issues that require addressing are as follows.

- Inadequate user notification of errors, requiring Help Desk support for even the simplest problem of an incorrectly entered FAD code
- No facilities to cancel file selection, retrieval or status checking once invoked
- Inadequate facilities for file management on completion of an RFI
- No reporting of the files used and the seal status for an RFI (possibly required for prosecution purposes)
- Inadequate facilities for maintaining the file selection list and identifying files not required for the RFI

[NBR260, NBR315]

13.5.4.6 Extractor Activity Logging

There is a requirement, for prosecution support purposes, to provide a log of the activities undertaken in processing an RFI, Currently this is a manual logging process which will not support any increase in volume of retrieval requests above the current limit of 50 per annum.

This can be achieved automatically by logging user interaction with the Audit Extractor and providing a report on completion of the RFI. [NBR260, NBR315, NBR445]

13.5.4.7 TMS Attribute Grammar Catalogue

R-Query is the utility used in the extraction process to interrogate the pseudo Correspondence Server generated on the Audit Server following retrieval from the DLT. The tool provides parameter driven filtering based on the Riposte attribute grammar and export facilities to MS Excel or MS Access.

NBS will introduce new attribute grammar to the Horizon system that must be interpretable by both Pathway and PO Ltd audit staff.

TMS records contain a huge amount of detail whose meaning is defined through the attributes associated with it. Partial catalogues for applications exist in isolation but there is a need to consolidate these into a single Attribute Grammar Catalogue with a searchable interface. Without this, it is difficult to determine which attributes are the appropriate ones for filtering and almost impossible to decipher a TMS record to determine what the content actually means. This is particularly so for casual users. [NBR260, NBR315]

13.5.4.8 Increase in Retrieval Requests

The sections above identify performance and usability enhancements required to *support* an increase in retrieval volumes. There are no requirements for changes to the Audit Retrieval service to provide any additional retrieval or search facilities at this Release. However, without the changes identified above, the current retrieval limit of 50 per annum would be severely compromised by the additional data volumes and increased timeframe for data retention. With the above changes, an increase in Retrieval requests can be contemplated but the limiting factor then becomes the number of staff required to perform the labour intensive operations involved. Each user would require their own Audit Workstation to perform data retrievals, and thus this number would then dictate the number of retrieval requests that can be achieved per annum. [NBR260, NBR315]

13.5.4.9 Non-Audit Use of Audit Server

The Audit Server is used as a back-up server for a number of key servers within the Horizon system. These include the Correspondence Servers, ACDB, OCMS Server and KMA Server. This secondary usage was introduced at a time (CSR) when the Audit Server had spare capacity to support this role.

However, there are now a number of issues with this arrangement.

- Now that full data volumes are being experienced, there are pressures on the Maestro Schedule to be able to complete all Correspondence Server backups in time for the primary Audit Solution work to take place
- The number of Legato drives (six per site) was not increased to accommodate the Correspondence Server backup work
- The full impact of increases in audit data volumes on the backup activity is not known

The advent of NBS and the experience to date suggests that the use of the Audit Server for non-audit work should be reconsidered. It is noted that this problem is likely to be mitigated through the introduction of a fully automated tape silo, and hence no further action is proposed at this Release.

13.6 System Components

13.6.1 New Components

See Section 16.2.5.2.

13.6.2 Key Generation Tools and Processes

A set of associated processes is needed in order to enable generation of the following keys:

- Superkey (SKEY) for the Compaq Atalla PCI crypto co-processor (HSM)
- MFK for the crypto processor

Similar procedures are likely to be required for the following keys used in conjunction with PIN Pads.

- BDK (Base Derivation Key for The DUKPT algorithm)
- GKLK (for generating the PIN Pad BKLKs)

The key generation mechanism will minimise the amount of paper-based keys and operator typing. Where operator typing is required, check digits will be used to enable all typing to be checked.

In outline, the key generation processes will be as defined in the following sections.

13.1.1.1 Superkey (SKEY), MFK and KEK

Tool generates and displays/prints multiple parts with check digits. Operators type the parts into the Compaq card management tool (SCT) and check the check digits. Paper copies preserved.

The keys will need to be input to an SCT to confirm correctness.

13.1.1.2 DK and GKLK

It is anticipated that these will be produced as multiple parts on paper.

Chapter 14 - Resilience & Availability Strategy

14.1 GENERAL

This Chapter outlines the architectural enhancements made by Pathway to the Horizon system to meet the significant additional resilience requirements of NBS.

It does not cover the service operation and SLA management aspects of the need for increased availability. These are covered in detail in Chapter 20.

Component and Platform failures are the most likely cause of service level breaches. Components that have a high impact on the availability of NBS have been designed to be resilient to the majority of failure conditions. In addition, certain critical components are outside the Pathway Operational Domain. The major example is the NBE, where a failure will cause loss of service to all Counters.

This Chapter thus focuses on the steps taken to provide resilience at a hardware level within the overall Horizon system.

14.2 COUNTER RESILIENCE

The Counter environment will be resilient to failure in the same way as for current applications, namely: [NBR505]

- Card information can be keyed manually following a Card reader failure (though this may be prevented for some cards by means of Reference Data) [NBR486]
- All Data should be capable of being entered either via the keyboard or the touch screen, thus allowing each to back the other up [NBR484, NBR485]
- Any Printed output can be displayed on the screen, thus allowing receipts to be written manually should the Printer fail (including those used for customer signature)

There is no resilience to PIN Pad failure, other than to use an alternative Counter if there is one.

14.3 NETWORK RESILIENCE & AVAILABILITY

As discussed in Chapter 10, the ISDN network between the Campus and the Outlet will be enhanced such that some Outlets are permanently connected. This will reduce the number of situations in which a call fails due to congestion in the ISDN network.

14.3.1 Silver and Bronze Outlets

Chapter 10 discusses the options being addressed to improve the cost-effectiveness and availability of the ISDN network.

Thus, starting at BI3, Outlets will be assigned to either a *Silver* or *Bronze* levels of service, depending on the needs of the Outlet and (in some cases) the time of day. [NBR053]

14.3.1.1 Bronze Service Outlets

The Bronze service represents service and availability levels based upon metered dial-up. Outlets with this service level are not expected to be in locations where an outage would have exceptionally high impact, nor carry out a large number of NBS transactions, and hence cannot justify the cost of an upgrade to a permanently connected network.

All Outlets will be initially configured with a Bronze Service.

14.3.1.2 Silver Service Outlets

The Silver service will introduce a permanent FRIACO network connection to the Campus during scheduled hours, using the current ISDN circuit. The Counter CNIM will ensure that a connection to the Campus is made, and re-made as soon as possible should it be lost, within this period. If unable to do so, it will make a permanent dial-up connection. This reduces the response time for calls to the Campus, and avoids the risk of failing to make an ISDN call.

There are two main reasons that an Outlet will be given a Silver Service:

- They are doing enough business that they justify a permanent connection (for example they spend more than 50% of their time connected in the busy periods)
- PO Ltd wish the Outlet to be moved to Silver Service to reduce response times or improve connection availability

14.3.2 Outlet Availability

Outlet Availability will be measured at a transaction level, as the sum of "failed" transactions against the sum of the total number of transactions. Only those failures within the Pathway domain will be counted. A "failed" transaction is any NBS transaction for which an On-line request [R] has been submitted but for which no corresponding Authorisation [A] has been received (at the Counter) prior to the termination of the transaction. Thus, transactions initiated while the Off-Line Indicator is set will not count.

14.4 HORIZON SYSTEM RESILIENCE

The Horizon system is designed to provide a high level of resilience. All Outlets connected to services running within two Campuses, located at Bootle and Wigan. All services are replicated within these Campuses, and either of them is able to support the full Horizon workload. Critical components are replicated within the Campuses as well as between them. Each Campus supports two independent LANs, and major servers are connected to both. There are two independent external links to each Campus.

In the event of a site disaster, existing processes will ensure that the workload is switched in its entirety to the other Campus. These processes are regularly rehearsed.

These facilities will be used and extended as necessary to support NBS. [NBR036, NBR472]

14.5 RESILIENCE WITHIN THE HORIZON CAMPUS

The existing Campuses are populated and configured such that there is no single point of failure that can cause the NBS to fail in the event of any one component, or an entire Campus, being unavailable.

14.5.1 Agent and Correspondence Server Architecture

14.5.1.1 Correspondence Servers

The current Correspondence Server configuration contains three servers per Cluster. Two of these are in Bootle, and one in Wigan. In addition, there is a standby Correspondence Server for each Cluster at each Campus. This is invoked via the Compaq Recovery Option in the event of failure of the live server.

The enhanced resilience requirements for NBS will require a move towards a configuration of four active Correspondence Servers per Cluster. The Compaq recovery option on the existing active Correspondence Servers will be removed. The eight servers that are freed up by this (four per Campus) will then be used to provide the platforms for the additional Correspondence Servers in each Cluster.

The existing “wing” Correspondence Servers will be removed from Bootle. The Compaq disk array that is freed will be used for the new Bootle Correspondence Servers. New Compaq Disk arrays will be purchased for the new Wigan Correspondence Servers. These will need to be the same specification as the existing Bootle wing servers.

This Correspondence Server configuration should have sufficient capacity for the initial NBS workload. As the workload increases, it may be necessary to upgrade the hardware of the Correspondence Servers. During testing and initial live use of NBS, the performance of the Correspondence Servers will be monitored. It is assumed that a hardware upgrade is required to support the full NBS volumes, and is scheduled for BI4. The actual timing of this will depend on the results of live monitoring, and how well the Correspondence Servers perform during testing.

By moving to four Correspondence Servers per Riposte Cluster, the following consequential changes are also needed.

- Outlets will need to send connection requests to all four Correspondence Servers in their Cluster. This is needed to spread the workload across the Correspondence Servers and provide resilience against Correspondence Server failure. A single network address will be used per Correspondence Server (rather than the current two) to keep the number of priority messages sent by each Outlet to four.
- The work generated by the existing Generic Agent Servers will need to be spread across the Correspondence Servers in each Cluster. This gives improved harvesting performance and resilience in case of Correspondence Server failure.

14.5.1.2 Agent Servers

At present, there is a ten- to twenty-minute gap after a failure of an OBCS Stops Agent before it is restarted on the same or a different platform. This will be inadequate for NBS Agents.

The increasing number of real-time messages requires a review of the availability of the Agent processes that handle these messages.

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.

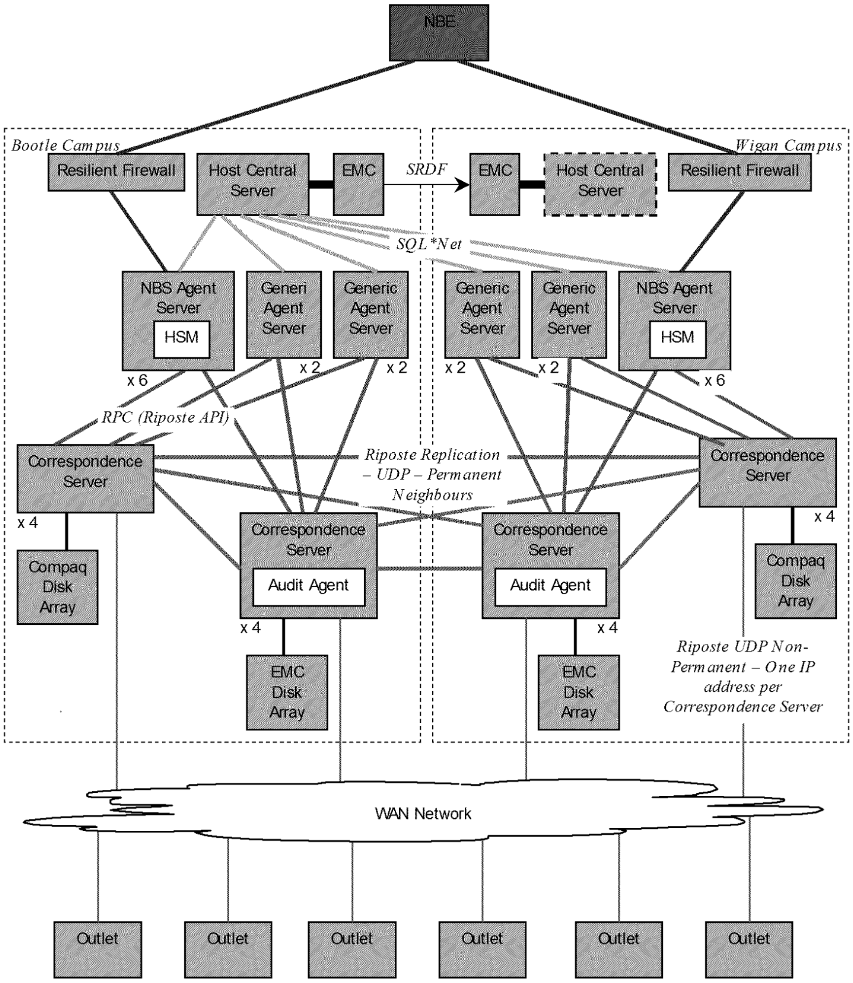


Figure 42 – Symmetric Campuses with Resilience on Disaster

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

The main advantages of this configuration are as follows.

- The Campuses are symmetric – either Campus can support the full workload in a resilience manner
- Testing is potentially easier because the two Campuses are the same
- No code change are required to the existing Generic Agent Servers, merely a configuration change to LUC
- The Generic Agent Server resilience model is improved. Loss of a Correspondence Server only causes 25% of the Agents to fail (currently loss of a Correspondence Server causes 50% of Bulk Agents to fail)

14.5.2 DRS System Resilience

The DRS database will have similar resilience characteristics to other Host applications namely:

- All data files will reside on SRDF-mirrored EMC disks. Note that the capacity of the EMC disk arrays will need to be extended.
- Harvesting will be controlled in a resilient manner by the Maestro scheduler, utilising the existing generic dynamic scheduling capabilities.
- Cold backups of the DRS database will be taken after each night's processing is complete
- Files will be sent to PO Ltd via the existing TIP FTMS Gateway

14.5.3 VPN layer

The current resilience model employed is believed to be adequate. Obviously, if the amount of traffic increases to the point where the system limits of individual servers are being reached, then more VPN servers per Cluster may be required.

14.5.4 Campus Network

The increase in real-time traffic (and for that matter general network traffic) could bring the Campuses closer to the limits of the Campus LAN, which in turn could decrease the reliability of the network. The resilience model makes it important that the Horizon system retains the ability to run the complete workload, including NBS, even after the loss of a single Campus, or of a critical Campus platform, or of the inter-Campus network.

14.1.5 NBE Resilience

Although the NBE is outside the Pathway operational domain, its resilience architecture has ramifications for the way in which the Pathway domain operates.

IBM will provide a duplexed NBE system at its Warwick site, providing a main and standby system within the same site. A single "Virtual IP Address" (VIPA) will be used and will be switched between the two systems if necessary, so that NBS Agent processes do not need to be aware of any failover from one system to the other.

IBM will also provide a Disaster Recovery (DR) system at its Greenford site. This is a single S/390 server which can be made available within 30 minutes or so of a disaster occurring at Warwick. VIPA mechanisms operate only within the same Sysplex, and hence should the DR site be brought into use, Pathway's NBS Agent Servers will need to be reconfigured to connect to it.

Chapter 15 - Performance and Scalability Strategy

15.1 GENERAL

This Chapter describes the approach taken to meet the performance and scalability requirements imposed by the NBS, without affecting the existing performance SLAs for the Horizon service.

The Performance and Scalability strategy will follow the principles set out in [PERFSTRAT], which will require updating. The revised strategy, as outlined in this Chapter, will ensure that the Horizon infrastructure can support a high level of on-line demand *whilst being* Scalable *and* Manageable

With many new services, the customer demand can only be estimated within limits and therefore the workload estimates may contain significant over or under estimates for:

- Total demand
- The demand in each time period as the service is rolled-out and becomes established
- Demand over the day, week, month or year.

The main drivers considered in shaping the approach were:

- *Uncertainty* – accept it, recognise potential consequences, deal with it
- *Stability* – promote it, avoid unnecessary service disruption
- *Technology Advances* – exploit them, grow with demand, avoid premature lock-in
- *Timescales* – be pre-emptive, plan options in advance, don't constrain business
- *Costs* – consider them (capital and running costs).

Hence, the strategic principles underpinning the approach are:

- Adopt an intrinsically scaleable architecture
- Reinforce scalability through design
- Select hardware specifically with scalability in mind
- Exploit the time over which rollout of POCA cards occurs to increase the understanding of the demand and the capacity requirements
- When defining and installing capacity:
    - Recognise unknowns
    - Focus on the near future
    - Establish a safe infrastructure baseline
    - Exploit scalability to grow with demand over time
- Performance is an ongoing programme of work involving:
    - Performance and capacity modelling
    - Performance measurement
    - Live system monitoring
    - Capacity management

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

15.2 SLAs

15.2.1 Service Measures

NBS will be subject to a set of SLAs covering:

- Request and Authorisation transmission time measures
- NBS availability measures
- Data Reconciliation Service measures
- Banking Transaction processing times

The exact measurements, the periods during which they apply, and any mitigations, are described in [CAN08] and are summarised here.

15.2.1.1 Request and Authorisation Transmission Times

This is the response time within the Pathway domain for on-line transactions i.e. the [R]/[A] message pair. Separate measures will be maintained for different Outlet-to-Campus network types, i.e. permanent connections and contended (dial-up) connections. Satellite links are included in this latter category

The network type for SLA purposes is determined by the normal network type for that Outlet. If an Outlet that normally has a fixed-up network connection but has to use the 'dial-around' then all transactions will be included in the fixed-up connection category for SLA calculations.

Transactions attempted whilst the Off-line Service Indicator (see Chapter 20) is activated will be abandoned by the Counter application before an [R] message is generated, and hence will be excluded from SLA calculation

The [R] and [A] transmission times require the system to gather response time information at the following points.

- *Counter* – For each NBS Transaction the system will record the time that elapses between the [R] being generated and the and the corresponding [A] being received back at that Counter Position (T_1)
- *NBS Authorisation Agent* - For each NBS Transaction the system will record the time that elapses between the NBS Authorisation Agent generating each [R2] for routing to the NBE, and the corresponding [A2] being received back from the NBE by the Agent (T_2)

The difference between the two times ($T_1 – T_2$) is the elapsed time in the Pathway domain i.e. the Pathway response time SLA. The Data Warehouse will also report T_1 but this is not an Pathway SLA.

In both cases, because the system clock may be reset during a transaction, the times will be measured using the same mechanism used for OBCS Foreign Encashment transactions.

A *Maximum System Wait Period* (MSWP) will be implemented at the Counter. If a response is not received before the MSWP is exceeded, then the transaction will be timed out and will be excluded from SLA calculations.

A similar timeout period will apply at the *NBS Authorisation Agent*. If this is triggered, a declined [A] will be generated which can be identified by the NBS Counter Application and the Data Warehouse as an NBS Authorisation Agent timeout.

Transactions that exceed the MSWP at the:

- *NBS Authorisation Agent* interface will be counted as successful transactions within the Pathway domain and are included in the calculation of the Request and Authorisation transmission time measure
- *Counter interface* will be counted failed transactions within the Pathway domain and are not included in the calculation of the Request and Authorisation transmission time measure

15.2.1.1.1 Service Boundaries

The service boundary between the NBS Authorisation Agent and the NBE is at the last *measurable* point within NBS because the system must be able to collect and store both performance and availability data at the service boundary.

Because of the requirement for measurability, this is not the same as the service boundary, which lies at the interface between the Pathway operational domain and the PO Ltd operational domain i.e., the domain in which the NBE is located.

15.2.1.1.2 Benchmark Times

For NBS the contractual clauses covering Counter transaction times are documented in [CAN08]. This specifies that Pathway and PO Ltd shall Agree target times for the Counter Processing Time components of each NBS transaction and each variant (PIN vs. Signature). These times shall start from the point at which the initial data is captured at the Counter (card swipe or committal of manual input). Methods of measuring these processing times are under discussion. Video benchmarks have been used in the past.

- The targets agreed between PO Ltd and Pathway will for each NBS and EFTPoS transaction type will include system components only i.e. those components of the dialogue that take place within the Counter system. For existing workloads, system components are added to manual components and network components in the *Pre-determined Administrative Data System* (PADS) model to construct the achieved time for a transaction.
- The Counter transaction times will not form part of the monthly Service Review reporting process and will not be subject to quarterly review (TRT & MAT). Transaction times will only be reported by the Request and Authorisation transmission time measure.
- The Counter transaction times will be measured according to the processes defined in [CTRBM].
- Only the system components prior to the generation of a Request [R] and after receipt at the Counter Position of the corresponding Authorisation [A] are included in the (unmeasurable) Counter transaction time.
- Pathway will investigate measurement techniques other than the Video Benchmark which is not flexible enough to support the demands of the new services.

Any changes to existing services required to support NBS, or that are requested by PO Ltd, that would cause any of the existing Benchmark Times to increase when re-measured, will be subject to CCN to change the Benchmark Time.

15.2.1.1.3 SLA Monitoring Points

There is a need to include extra monitoring points at a number of points within the infrastructure. Information gathered at these points needs to be sent to the Data Warehouse. The volumes of data generated need to be taken into account in system sizings.

SLA response time information and Availability figures are listed in [CAN08], and the implication for the Horizon system are documented in [SRS]. SLAs are assessed according to the domains through which they flow. Pathway is responsible for the response times for that portion of the end-to-end message flow that is within its domain.

Within the end-to-end NBS solution, Pathway's contribution to the overall response time for an [R]/[A] pair is as shown in the diagram below. Also shown are the points at which it is possible to measure time stamps (or time delays) in such a way that Pathway's contribution to the total round trip time can be fairly attributed. Note that time stamps are generated at the last measurable point within the component that handles the transaction. In practice, this means that measurements of messages sent to, or received from the NBE are made as follows:

- For messages sent to the NBE, immediately preceding the call to TCP/IP to pass the message to the NBE
- For messages received from the NBE, immediately after the TCP/IP call returns with the message from the NBE

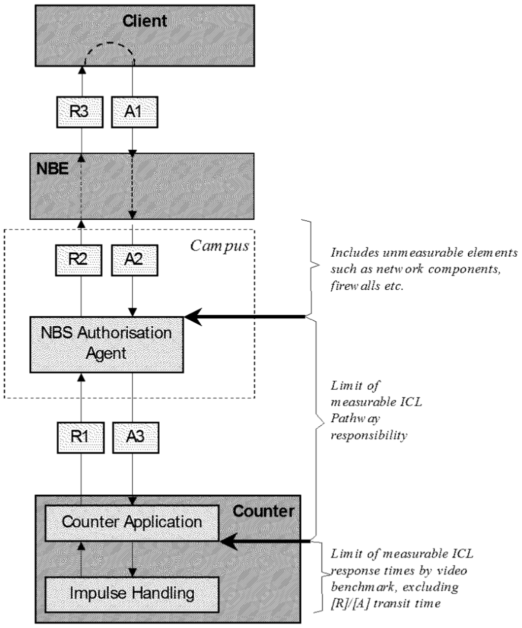

Client
R3
A1
NBE
Campus
R2
A2
NBS Authorisation Agent
R1
A3
Counter
Counter Application
Impulse Handling
Includes unmeasurable elements such as network components, firewalls etc.
Limit of measurable ICL Pathway responsibility
Limit of measurable ICL response times by video benchmark, excluding [R]/[A] transit time

Figure 43 – Limits of Pathway's SLA Measurements

Note that there are no SLA measurements associated with the passing of [C0] messages to the NBE, as there is no return message to indicate that such a message has been received.

15.2.1.2 NBS Availability

[CAN08] defines “Availability" as the percentage of all Requests written to the local message store at a Counter for which a corresponding Authorisation indicating no failure has occurred in the POCL Service Infrastructure is received at that Counter Position before the MCWP has expired.

The relevant figures will be calculated by the MIS. Different targets are used for Fixed Connection Outlets (99.00%) and Dialled Connection Outlets (97.00%)

15.2.1.3 Data Reconciliation Service Measures

Targets are defined in [CAN08] for the times taken to resolve Customer Critical Exceptions, counting time within MSU Days only. Relevant reports will be produced by the MIS, taking input from MSU progress metrics.

15.2.2 System Sizing

To ensure that it is able to meet the workloads specified in [SRSVOLS], the enhancements to the Horizon system will be sized such that:

- The demand in the peak second determines the network capacity required (even if this level of demand only exists for a few minutes per day)
- The demand in the peak day determines the disc and processing capacity required to support overnight data processing requirements

15.3 MANAGING CAPACITY

Pathway has to be able to deliver flexible capacity (within limits) that will meet the changing demands and enable it to be delivered as close to the time when it will be required as possible.

As part of NBS, Pathway will deliver a *Capacity Management Service* (CMS) targeted with pro-actively managing the infrastructure (in collaboration with PO Ltd) in order to match the installed capacity with the expected business demand.

Capacity is managed as an ongoing programme of work and is not bound by a particular Release. The capacity of the infrastructure that is implemented at a particular point in time depends on the following.

- Projected business demand for the new and existing services which should take into consideration:
    - Unpredictable public reaction/behaviour to new services
    - Seasonal variations for certain functionality
    - The impact on existing services of the change in the customer base brought about by the payment of benefits through bank accounts
- The service levels delivered by the enhanced Outlet-to-Campus network services
- The performance of new software components e.g.:

  - New Counter applications
  - WebRiposte on the Correspondence Servers
  - New Agents e.g. the *NBS Authorisation Agent*
  - DRS applications

- The level of risk that Pathway and PO Ltd wish to take (headroom)

In effect, there is a set of unknowns that must be allowed for when projecting the infrastructure capacity to meet the demand. Some of these unknowns will be resolved by:

- Technical or volume and stress testing (see Chapter 19)
- Monitoring of the live service
- Review of the actual demand versus the expected demand

The projected volumes for the following services have been documented in [SRSVOLS].

- Horizon services (based on volume projections from the live service)
- NBS services (using volumes supplied by PO Ltd [SRSVOLS])
- EFTPoS services (using volumes supplied by PO Ltd and documented in the EFTPoS SRS [EFTPoS]

That document will provide the baseline for the volumes to be supported in month by month starting from the point when the new services (NBS and EFTPoS) are introduced.

The capacity that Pathway will configure initially will:

- Be capable of supporting (at least) the 40% of the projected full roll-out volumes for the new services

- Depend on cost and in particular the running cost:

  - For those infrastructure components where there is a significant difference between the running cost of 100% capacity and incrementally rolling out capacity, Pathway will endeavour to roll out capacity just ahead of demand

  - For those infrastructure components e.g. Platforms where additional capacity is not required initially, Pathway may delay the installation of additional capacity. This will enable Pathway to exploit the technological advances that occur in the intervening period

Starting from this baseline, which is documented in [SRSVOLS], Pathway and PO Ltd will review and re-baseline the volumes every three-months and Pathway will update the capacity plan accordingly, so that if addition capacity is required, it can be installed progressively ahead of demand.

The capacity planning process will work on the assumption that there is a six month lead time to plan and implement any changes to the infrastructure so changes must be approved at least six months ahead of capacity being required.

15.3.1 Performance Engineering

Performance Engineering embraces a set of disciplines used by Pathway that are integrated into the overall development and production processes. Performance Engineering refers to the performance related activities within the following domains.

- Requirements
- Design
- Development and
- Production

The objective is to ensure that performance and scalability are built into the system from the outset. Performance modelling, performance measurement, live system Monitoring and capacity management are treated as separate activities in their own right.

Performance is a non-functional quality attribute that is designed into the system. All components of the system must be capable of delivering the throughput and response targets within resource budgets.

These measures are derived from the NBS and EFTPoS Requirements Catalogues ([SOR] and [EFTPoS]) and the PO Ltd volumetrics (see [SRSVOLS]).

Design documentation includes coverage of the critical performance characteristics, so that Development has the necessary guidelines to build a performant product meeting the performance targets and resource budgets set for it.

During the course of design and development, prototypes, including large-scale technical evaluation, are used to improve performance understanding and provide early design feedback.

15.3.1.1 Requirements

The performance engineering process starts with the requirements by ensuring that the business requirements are:

- Understood
- Fully documented
- Achievable

The consolidated set of business requirements is documented in [SRSVOLS].

From the business requirements, Pathway will derive the system requirements i.e. the peak performance that each component must support.

Each component of the system will be evaluated against each system requirement. This will include an evaluation of:

- Feasible options
- Cost and
- Risk, including service quality.

15.3.1.2 Performance and Capacity Modelling

Although the Horizon system is innovative and complex, the modular architecture allows the problem domain to be broken down into its component parts relatively easily and without undue compromise. However, the new services bring with them a new style of working i.e. On-line.

To support the capacity management process, Pathway will construct a series of models covering for example:

- The volumetrics for all services
- The peak load the service must be capable of supporting to deliver the business requirements within the service requirements (SLAs)
- The peak load that each component must support to deliver the transaction
- The load on the system against the predicted load.

The set of models will form an integral part of both the Development and the Production processes i.e. will be used during the requirements, design, development, testing and live running phases.

In many cases, point models, using simple tools, can be used to good effect. However to model dynamic real-time interaction e.g. on the Outlet-to-Campus network, complex analytical, dynamic, and simulation models, using sophisticated tools, will be required.

One of the principal objectives of performance and capacity modelling is to develop a greater understanding of the workloads demanded of the system over time, and the capacity of the system to satisfy those workloads over time. This incremental refinement or calibration is an ongoing process, capturing an ever-improving understanding of the performance characteristics of the system and the workloads to which it is subject.

The demand on the infrastructure created by different services is not uniform over:

- 5 minutes
- An hour
- A day
- A week
- A month

and so a set of profiles has been generated by Pathway which will be used to model the demand on each infrastructure component or set of components and determine where the peaks occur. In conjunction with the service level required, theseprofiles will drive the amount of capacity that needs to be installed to process the peak workload and meet the SLAs.

Some of the workload is expected to be very peaky e.g. the pattern of benefits encashments as seen below:

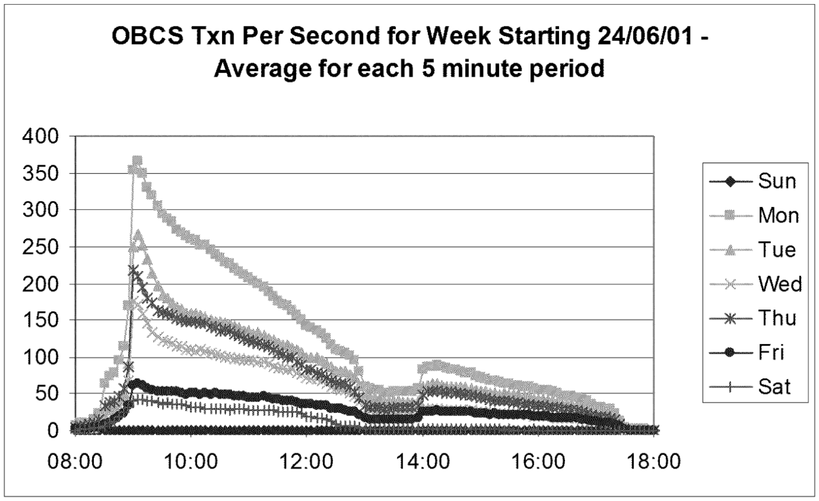


Figure 44 – Rate of OBCS Transactions

The peak is very short-lived and therefore the capacity required to support this peak might only be used for a short time each day. If PO Ltd can find a way to change customer behaviour, e.g. opening Outlets earlier or later, then this will have the effect of flattening the peak and reducing the capacity and therefore the cost of delivering the same volume of business.

This is not to say that there is only one peak. Different peaks affect different parts of the system. The infrastructure defined in [SDSINF] will be configured to support the peak business volumes in the peak:

- *Second* - the peak load that the Outlet to Campus network, WAN, routers, VPN servers, Correspondence Servers and Agents must support i.e. all resources supporting real-time transactions
- *Hour* - the peak periodic reconciliation flow
- *Day* - the peak End-of-Day and harvesting, loading and reconciliation volumes including the Host disk and processing capacity required to support overnight data processing requirements
- *Two Days* - the Host database sizes i.e. the data storage should be capable of holding two peak days data concurrently
- *Week* - End-of-Week volumes
- *Month* - the Data Warehouse volumes

The infrastructure including the Outlet to Campus network shall, were possible, be implemented progressively ahead of demand.

The Performance and Capacity Modelling activity will provide input into the Capacity Management Service.

15.3.1.3 Performance Measurement

Performance measurement is part of the Development process and aims to verify many of the assumptions made in the Performance and Capacity Models. For the new services, performance measurement will form part of the systems testing and volume & integrity testing phases of the programme (see Chapter 18). In addition, ad-hoc Technical Testing may be performed to investigate:

- The performance characteristics of new software or components as early as possible in the programme
- Limits and bottlenecks that may inhibit scalability

The resulting performance data will be used to further improve understanding of the performance characteristics of the system and to refine the capacity projections and models accordingly. Where significant changes in understanding are brought about, further modelling and evaluation work may be required to address any issues arising.

15.3.1.4 Live System Monitoring

Once in live running, the performance characteristics of the services need to be monitored on a regular basis including:

- Monitor the behaviour of the systems and services to ensure that they are behaving and growing as would be expected.
- Monitor the actual business volumetrics and the consequent system workloads and verify any assumptions, in particular the incidence of peaks, seasonal variations, etc.

Performance monitoring of the live system is a key input into the Performance and Capacity Modelling process and should collect data about:

- *Demand* – The number of transactions, messages, etc processed by a component
- *Response* – The elapsed time within and between components
- *Reliability* – The number of failures e.g. timeouts that occur in a component or at component interface
- *Resources* – The amount of cpu, memory, disk, network bandwidth, etc used to process the demand
- *Scalability* – Are the resources per unit of demand constant as the demand increases

Live systems monitoring aims to verify many of the assumptions made in the Performance and Capacity Modelling process, and to further validate the performance of the solution against the projected workloads.

15.3.1.4.1 Athene Performance Monitoring and Reporting Service

Pathway has installed the Metron Athene product to monitor the resources used and report on the demand on a component and the resources used to process that demand. For the new services the Athene service will be extended to:

- Monitor and report on new platforms
- Monitor and report on new application where performance metrics are built into the application e.g. the NBS Authorisation Agents
- Report on the on-line characteristics of the new services

15.3.1.4.2 Data Warehouse

Reports will be produced by the MIS covering the following areas.

- *Response times*
  - Overall analysis of response times by time slot over the working day
  - Specific Outlet reports allowing slow responding Outlets to be identified and investigated
- *Timeouts* – analysis of timeouts both at the *NBS Authorisation Agent* interface and the Counter

These will be input into the Performance and Capacity planning models.

15.3.1.4.3 Counter Network Information Monitoring Service (CNIM)

The monitoring of networks will be extended to cover:

- The enhanced Outlet-to-Campus network
- Network links between the Campus and the NBE.

New or enhanced monitoring tools will be implemented as part of the Service Management upgrade (see Chapter 20) and these tools will provide detailed data about the traffic in the network components into the CMS.

Chapter 16 - Application Development

16.1 GENERAL

This Chapter discusses the developments needed to support NBS, and summarises the application development processes and tools used.

16.2 PATHWAY DEVELOPMENTS

The developments that are to be undertaken by Pathway are as follows. There are no changes to existing development processes unless stated.

16.2.1 Application Architecture Changes

16.2.1.1 Counter Application

Counter Applications are developed using Visual Basic V5.0.

New *Operation Launch* Impulse to handle magnetic card swipes and cause entry to the application (see Section 5.4.2.1.6) including:

- Magnetic Token Validation Function (5.4.2.1.4)
- Magnetic Token Manual Entry (5.4.2.1.5)

New *NBS Counter Application* (BI3), including

- Reference Data definitions for each transaction type
- Host components that are used by NBCA
  - *Initialise* (see Section 5.4.3.1.1)
  - *RequestReply* (5.4.3.1.2)
  - *Output* (5.4.3.1.3)
  - *Input* (5.4.3.1.4)
  - *Finalise* (5.4.3.1.5)

New *NBS Counter Recovery application* (see Section 5.4.3.4). (BI3)

16.2.1.2 Counter Drivers

New *PIN Pad Driver* (see Section 13.4.2.1.4) (BI2)

16.2.1.3 Agent Processes

New NBS Agent processes (all at BI3). These are largely developed using C.

- *NBS Authorisation Agent* (see Section 5.7.2)
- *NBS Expedited Confirmation Agent* (see Section 5.7.3)
- *NBS Confirmation Harvester Agent* (see Section 5.7.4)

Other Agent changes:

- Enhancements to *TPS Harvester Agent* to handle additional fields in [C] messages (see Section 5.10.2)
- *KMA Agents* change to reflect the database upgrade to SQL Server 2000
- *Audit Agent* changes to break down audit files into smaller chunks for improved retrieval performance

16.2.1.4 Agent-Like Processes

EoD File MAC Checker process (see Section 5.8) to run on the *NBE Gateway Server - Local*

16.2.1.5 FTMS Configurations

New *FTMS NBE Configurations Local* and *Remote* to run on the NBE Gateway Servers (see Section 5.8)

16.2.1.6 EPOSS

Potential enhanced *EPOSS Counter Application* to cover settlement of NBS transactions and receipt printing (see Section 5.4.4.1)

16.2.1.7 Automated Payment Service (APS)

Enhanced *APS Counter Application* to handle POCA card receipt (see Section 5.4.4.2) and to remove logging of receipt messages to the message store (BI3)

16.2.1.8 Order Book Control Service (OBCS)

Enhanced *OBCS Counter Application* to ensure that Foreign Transactions continue to operate correctly in the new network paradigm (see Section 5.4.4.3). (BI3)

16.2.1.9 Transaction Processing Service (TPS)

These are at BI3

- Enhancements to *TPS Host Application* to handle the additional attributes required by NBS messages (see Section 5.10.3)
- Enhancements to *TPS Database* to permit a View for DRS (see Section 9.5.1.1)

16.2.1.10 Management Information Service (MIS)

Enhancements to the MIS to calculate new and revised SLAs as described in Section 5.11. (BI3)

Additional data feed from OMDB. (BI3)

- Outlet network type, which is needed for SLA calculations where Outlets with different network types have different SLAs

16.2.2 Reference Data Management Centre

Enhance *Reference Data Management Centre* (RDMC) and its associated RDMC Database as follows (BI3)

- Receive additional data across an enhanced Type A Data Interface and to validate

that data

- Introduce a new view into the RDMC Database for DRS
- Reference Data Production and Enrichment Access Database System to support the additional data required for NBS

Enhance *Reference Data Distribution Service* (RDDS) as follows.

- Make the additional data available to other Host systems, specifically TPS and the Data Warehouse

Pathway will develop the mechanisms needed to support a new, chargeable, Bank Take On Service, which will be used under the direction of PO Ltd. for validation of PO Ltd. Reference Data involving the Pathway domain, the NBE, and if relevant the Bank. The Service will cover the introduction of a new Bank, NBE Routing ID, NB Token, Bank Issuer Scheme or other PO Ltd. Reference Data at the direction of PO Ltd. [NBR411]

16.2.3 Data Reconciliation Service (DRS)

The DRS is introduced as described in Chapter 9, using Oracle 8i as its base (BI3). It includes the following components.

- NBS Data Reconciliation Service (DRS) Host Application (see Section 9.5.1.1). Development will use the Oracle 8i development tool set and SQLJ (Java with embedded SQL), Pro*C (C with embedded SQL) and PL/SQL. Coding and debugging will use Microsoft Developer Studio across Net8 (SQL*net) from Microsoft Windows NT 4 portable to IBM Sequent Dynix.
- DRS Database (see Section 9.5.1.1) Design and Schema will be captured using Oracle Designer.
- DRS Workstation Application (see Section 9.5.1.2). Development will use the Oracle 8i development tool set. Design will be captured using Oracle Designer/Developer. Development will be in Oracle Forms, SQLJ (Java with embedded SQL), Pro*C (C with embedded SQL) and PL/SQL. Coding and debugging will use Oracle Forms Development across Net8 (SQL*net) from Microsoft Windows NT 4.

16.2.4 Network Infrastructure

Introduction of the Counter Network Information Monitor (CNIM) to implement the Outlet's network connection type and report on the network status for interested applications, and to implement call reversal as required for Software Distribution. See Section 10.4 (BI2, enhanced for FRIACO services at BI3)

16.2.5 Systems Management

16.2.5.1 SYSMAN

Enhance the *Operational Management Database* (OMDB) and associated Web pages for the following (BI3).

- To accept an enhanced data feed from the ACDB listing the network type of an Outlet, and display Outlet network information (see Section 12.6.1.4 and 12.9.2)
- Feed this information to the Data Warehouse
- To add PIN Pad details to the Counter hardware inventory (see Section 12.6.2)

Enhance *Service Management Data Base* (SMDB), which mirrors some of the data held in the OMDB for use by support staff, as follows (BI3).

- Accept and display new Outlet connection types (see Section 12.9.8)
- Reference Data delivery to Counters

Enhance *Auto-Targeting Engine* (ATE) to support ISDN call reversal. See Section 12.6.1.4 (BI3)

Enhance *Software Distribution – Counter* component to handle PIN Pad key distribution, change of master keys and *Base Derivation Key* (BDK), PIN Pad location tracking, Health Check reporting (battery low) (see Section 12.6.2 and 12.8.4)

New *BMC Patrol Knowledge Module for DRS* (see Section 9.5.1.1)

Enhance Sentry monitoring for Agent and Correspondence Server platforms (see Section 12.8.1) (BI3)

Enhance *Counter Diagnostics* component, as described in Chapter 20 (BI3)

16.2.5.2 Auto-Configuration Database (ACDB)

Enhanced *Auto Configuration Data Base* (including Counter Downloader):

- To support the modified ACFs for FRIACO networks and Riposte Cluster changes
- To feed CHAP information to the Radius Servers (see Section 10.5.2.3.4 and 12.9.2.1)
- To feed modified Outlet routing information to the NMS

Enhance *Counter Downloader* to support the modified ACFs for FRIACO networks and Riposte Cluster changes

Enhance *AutoConfig ISDN Router Configuration Script Generator* to use configuration information provided by ACDB to generate modified Router configuration scripts.

16.2.5.3 Outlet Change Management Service (OCMS)

Enhance *OCMS* to specify and initiate the configuration changes for new network types, as described in Section 0. (BI3)

16.2.5.4 Network Router Script Generation

Enhance *AutoConfig ISDN Router Configuration Script Generator* to accept revised routing information and generate the scripts for new Router types.

16.2.6 Security

16.2.6.1 Key Management

Upgrade *KMA Database* to SQL Server 2000 (see Section 11.3.2.6.3.1). (BI2)

Enhanced *KMS Application* to remove workarounds introduced following the decision that this would be implemented on SQL Server 6.5, rather than any later version, and that are now unwanted following the upgrade to V2000 (see Section 11.3.2.6.3.1). (BI2)

Corresponding enhancements to the KMA Workstation and KMS Admin Workstation applications. (BI2)

KMA Workstation application is enhanced to import ZMKs and manage the installation and synchronisation between the NBS Agent Servers and the NBE. The ZMK is used to support MAC signing.

Enhance KMA Database for new protection domains. (BI3)

Enhance KMS Application for new protection domains, and to deliver keys to new platforms (*NBS Agent Servers* and *NBE Gateway Servers* - *Local*). (BI3)

16.2.6.2 Crypto API Library

The Crypto API library is enhanced (if required) as follows (BI3).

- Support the Request/Reply interface in the Counter so that encryption, signing and verifying can be done at this point (see Section 5.4.3.1.2)
- Support of MAC generation and verification
- Support of PIN Block translation within the NBS Agent Server, using the HSM
- Support of *Digital Encryption Service* (DES) encryption (using the HSM)
- Support for new NBS Agent Servers as recipients of CAPUs
- Enhancement of the Automatic Channel to handle ZMKs (via enhancements to the KMRx service)
- Performance improvements to support caching of 5,000 keys to support NBS Authorisation Agent throughput

16.2.6.3 Other New Key Handling Enhancements

- Code to handle manual key generation for HSMs
- Session key management code for NBPC domain to LINK standards
- PIN Pad key management

16.2.6.4 Audit Handling

Enhancements to Audit catalogue for increased use of audit data and improved performance. (BI3)

- Enhancements to *Audit Checksum database* (see Section 13.5.3), including porting this to SQL Server
- Enhancements to Audit Sealer and Hoarder to handle revised checksum database
- Enhancements to TMS data storage (see Section 13.5.4.1)
- Introduction of Tape silo for audit storage, and development of appropriate procedures (se Section 13.5.4.3)

16.2.7 Common File Set

Enhancements to the Common File Set to include components of WebRiposte, Internet Explorer 5.5, NT 4.0 SP6a and others. See Section 11.3.2.4.4.2. (BI2)

16.1.8 NT Secure Build

Enhancements to the NT Secure Build to include the new NBS Agent Servers domain (PWYPUB), and other improvements to the access control and audit policies. See Section 11.3.2.4.4.3. (BI3)

Chapter 17 - Documentation

17.1 GENERAL

This Chapter provides an initial list of the documentation (other than this SDS) that will be needed to support the development. Further documents may be found necessary as the development proceeds.

17.2 REQUIREMENTS SUMMARY

Many existing documents will need amending to reflect the introduction of NBS. These documents include Contract Controlled and Contract Referenced Documents. A number of Working documents, for example those at the process, procedural and operational levels, will also need to be updated. Many of the changes will be minor. However, some new interface documents will need to be created to describe and manage the flow of data and services across the new interface.

Operations Manuals will be updated as necessary to reflect the NBS.

In addition, documents defining the Acceptance processes and Service Introduction will need to be jointly agreed as *Contract Controlled Documents* (CCDs).

17.3 CONTRACT CONTROLLED DOCUMENTS

The list below covers candidates for Contract Controlled and Contract Referenced Documents, The table gives the latest version of those documents from which revised NBS versions will be derived. [NBR551]

Pathway Reference	SDS Reference	Document Title	Version	Notes
BP/DES/003	[CHD]	Counter Hardware Design Specification	7.1	
BP/IFS/007		Application Interface Specification Reference Data to Pathway	4.1	[NBR045]
BP/IFS/010		Application Interface Specification - Reference Data to Pathway for CSR+	4.6	[NBR045]
BP/IFS/011		Reference Data System - Application Interface Specification Reference Data to Pathway Type B Data for CSR+	4.3a	[NBR045] (PO Ltd responsibility)
BP/IFS/012		AIS Type B Reference Data (PO Ltd Ref. RDP/AIS/009)	1.0B	[NBR045]
CR/FSP/004	[SADD]	Service Architecture Design Document	6.0	
CR/FSP/006		Audit Trail Functional Specification	5.0	
CS/IFS/003		ICL Pathway/POCL Interface Agreement for Operational Business Change – Outlet	3.0	[NBR045]

CS/PDN/015		Service Descriptions for Outlet Change	3.0	
CS/PRD/058	[OBC]	ICL Pathway / POCL Interface Agreement for Operational Business Change – Product	5.0	New OBC procedures for NBS Reference Data [NBR045]
CS/PRO/090		CSR+ Access Control and User Administration Processes and Procedures Description	6.0	[NBR026]
CS/PRO/092		CSR+ Horizon System Help Desk: Processes and Procedures Description	3.0	[NBR026]
CS/PRO/093		PPD: Introduction of New Release	3.0	
CS/PRO/095		CSR+ Electronic Point of Sale Service: Processes and Procedures Description	4.0	[NBR026]
CS/PRO/097		CSR+ Operating Environment: Processes and Procedures Description	5.0	[NBR026]
CS/PRP/001	[CTRBM]	Counter Transaction Performance Measurement and Benchmarking	2.0	
CS/REQ/006		Requirements for Operational Change Management System	3.0	
CS/SIP/002		Business Continuity Framework	5.0	
CS/SPE/011	[DRSREP]	Network Banking End to End Reconciliation Reporting	1.0	
NB/PRO/002	[RECIM]	Network Banking Reconciliation and Incident Management	2.0	
NB/SPE/003	[CNTRDLG]	Network Banking: Counter Dialogue & Activity Flows	New	
PA/PER/031	[NSBV]	Horizon New Service Business Volumes	New	
PA/STR/003		Pathway Release Policy	5.0	
RD/CSD/001		Reference Data Business Rules & Values	1.0	(PO Ltd responsibility)
RS/FSP/001	[SFS]	Security Functional Specification	4.0	
RS/POL/002	[SECPOL]	Pathway Security Policy	6.0	
SD/DES/005	[REPREC]	Horizon OPS Reports and Receipts	10.0	[NBR032]
SD/STD/001	[STYLE]	Horizon OPS Style Guide	8.0	To reflect use of PIN Pads
TD/ARC/029		TMS Architecture Specification	(0.8)	Note that update is required before NBS Acceptance
TD/ARC/030	[OPSARCH]	OPS Architecture Specification	1.0	Describes the Counter environment at CSR+ NBS will introduce changes at the Counter in the areas of WebRiposte. New PO Ltd Reference Data objects, PIN Pad support. Note that update is required before NBS Acceptance
TD/STD/004	[GENAPI]	Generalised API for OPS/TMS	1.0	PIN Pad APIs and others
TI/IFS/001	[TIPAIS]	Pathway to TIP Application Interface Specification	6.0a	
New		Testing and Integration Strategy for Network Banking	New	
New		Pathway Network Banking Release Contents Description	New	[NBR074]

New		PO Ltd NBS Configuration Data AIS	New	
New		RDP/OLA/010 – RDS OLA	New	
New		Security Incident Management	New	
New		Network Banking: Approach to Measurement of Target times	New	
New		Network Banking Management of Prosecution Support	New	

Table 29 – Contract Controlled Documents to be Added or Modified

17.4 INTERFACE SPECIFICATIONS

New AIS/TIS documents will be required, with the intention that they become CCDs. These will include details of the backup and recovery processes appropriate to their interfaces. [NBR037]

Reference	Tag	Title	Version	Notes
NB/IFS/008	[NBEAIS]	Post Office Limited - Network Banking Engine - NBE - Horizon Application Interface Specification	2.0c	[NBR050, NBR050], NBR050]
NB/IFS/009	[NBETIS]	The Post Office - Network Banking Engine - Technical Interface Specification - Horizon to NBE	1.04	
New		Campus to PO Ltd Settlement Host (Settlement Data)		

Table 30 – AIS/TIS Documents

Other Interface specifications, internal to Pathway, include the following.

Reference	Tag	Title	Version	Notes
DW/IFS/001	[DWTPSAIS]	Data Warehouse to TPS Interface Specification	1.12	
DW/IFS/005	[DWRDAIS]	Data Warehouse To Reference Data System Interface	1.4	
New	[DRSRDAIS]	RDDS/DRS Interface Specification	New	

Table 31 – Internal AIS/TIS Documents

17.5 WORKING DOCUMENTS

The following shared Working Documents, which will not be contractual, may need to be created or updated.

Pathway Reference		Document Title	Version	Notes
AD/PDN/001		Pathway Agents: Operational Overview for CSR+	2.0	Needs to cover new Agent types
CS/IFS/007	[HSHDIFS]	ICL Pathway/POCL Interface Agreement for NBCS and HSH Interface	2.0	
CS/IFS/008	[PMIFS]	ICL Pathway / POCL Interface Agreement for the Problem Management Interface	(0.3)	

CS/IFS/009		ICL Pathway / OSD Interface Agreement for the Problem Management Interface	(0.3)	PVCS
CS/POL/005		Service Management Framework		[Withdrawn]
CS/PRO/111	[TPSREC]	TPS Reconciliation & Incident Management	1.0	
IA/MAN/005	[AUDM]	Horizon System Audit Manual for CSR+	1.0	
NB/IFS/003	[CNTRRD]	Network Banking Counter Reference Data Interface	New	
NB/SDS/008	[NBSMIS]	Network Banking MIS Reports Design	New	
NB/SPE/009 ?	[NBRDBRV]	Network Banking Reference Data Business Rules and Values	New	
PA/PER/015	[PERFSTRAT]	Performance and Scalability Strategy	2.0	
RD/DAT/001	[RDMCDM]	RDMC Data Model		
RS/POL/003	[ACP]	Access Control Policy	3.0	
SD/DOC/009	[OPSMESS]	Horizon OPS Desktop Messages and Help Text: CSR+	4.0	
SD/SPE/016	[OPSMENU]	Horizon OPS Menu Hierarchy	17.0	Covers Menu trees and screen layouts
TD/ARC/001	[TED]	Technical Environment Description	4.7	Overall description of the Horizon architecture
New		Network Banking Audit Trail Specification	New	
New		Logical Reference Data Model – PO Ltd Reference Data	New	

Table 32 – Working Documents to be Added or Modified

17.6 DESIGN DOCUMENTATION

17.6.1 High Level Designs

17.6.1.1 New HLDs

The following Documents will be produced.

- NBS Counter HLD

  This will cover the following:

  - NBCA
  - EPOSS Integration
  - Reconciliation
  - Recovery
  - Generic Transactions

- NBS Agent HLD

  This will describe the Agents defined in Section 5.7 and cover:

  - Database design
  - Host Processing
  - Interface to TPS

- NBS Reference Data HLD
- Network Infrastructure HLD (including DMZ)

17.6.1.2 Revised HLDs

A number of existing HLDs will need to be updated to cover enhancements described in this Document. They include the following.

Reference	Tag	Document
Security		
IA/PRO/003		Conducting Audit Extractions at CSR+
PA/PRO/032		Pathway Sensitive Material Handling Process
RS/DES/010		Key Management High Level Design
TBD		Key Management System Low Level Designs
RS/DES/018		Key Management Application Design
RS/REQ/009		Key Management Requirements for Crypto Code
RS/DES/051		NT Domain Structure Design for CSR+
RS/DES/052		NT Domain Names
RS/DES/053		NT Trust Relationships
RS/DES/054		NT Server Names
RS/DES/062		Implementation Build Guide for NT Platforms
RS/MAN/003		User Guide For KMA Helpdesk Application
RS/MAN/006		KMS User Guide for CSR+
RS/MAN/007		Guide for OSD Local Operations and Key Custodians
RS/MAN/010		SecurID Token User Guide and Responsibilities
RS/PRO/013		Horizon Security Pass Procedure
RS/PRO/014		Pathway SecurID Token and Pin Management Process
RS/PRO/032		Security Event Management
RS/PRO/034		Horizon Security Passes Audit Procedure
RS/PRO/036		Cryptographic Key Handling Procedure For Remote Key Custodians CSR/CSR+
RS/PRO/037		Key Management Process Guide
RS/PRO/038		KMS Sensitive Material Handling Processes
RS/PRO/039		KMS User Roles Authorisation Process
RS/PRO/040		Application for Access to the Live Network
RS/PRO/042		Production of System Information for Evidential Purposes
RS/PRO/044		Physical Security Procedures: A0 Secure Area
SB/SDU/009		Windows NT 4.0 Generic File Security
TPS		
AD/DES/041		TPS Agents for CSR+ High Level Design
AD/DES/047		TPS Agent Tables and Mappings for CSR+
TI/DES/001		TPS Host Technical Specification
Data Warehouse		
		Data Warehouse HLD
DW/IFS/028		CSR+ Inward Data Delivery Measurement AIS
Network		
TD/DES/059		Network HLD
Resilience		
		Agent & Correspondence Server Resilience
Systems Management		
		Counter Process Control HLD
Reference Data		
RDP/TEC/951		Reference Data Business Rules and Values
RD/CSD/002		Reference Data Business Rules & Values
RD/DES/046		RDMC High Level Physical Design
RD/DES/047		RDDS High Level Physical Design
		Definition of Reference Data Collections
Build		
CSM/ION/018		Common File Set Baseline Delivery for CI4
Platform Design Documents		
SD/DES/011	[PDHOST]	Physical Design for Host Central Server [CSR]

SD/DES/147		Platform Physical Design Specification for Data Warehouse
New		Physical Design Document for NBS Agent Server
New		Physical Design Document for Cisco Syslog Server
New		Physical Design Document for Cisco Secure Server
New		Physical Design Document for RADIUS Server
New		Physical Design Document for HSM Key Management Workstation
New		Physical Design Document for Support Terminal Server
New		Physical Design Document for Vulnerability Detection Server
New		Physical Design Document for NBE Gateway Server – Local [& remote]

Table 33 – Design Documents to be changed

17.7 MIGRATION STRATEGY

A Migration Strategy document is required for these Releases, followed by a Migration High Level Design document. Issues to be addressed include:

- Do the Campus before the Outlets
- Try to do the Campus servers via Tivoli
- Outlet upgrades will require at least one reboot. Conceptually, SP6a and IE5 will require a reboot each. If possible, this will be reduced to a single reboot.

17.8 SUPPORT GUIDES

- OBC for PO Ltd Reference Data
- OBC for Changes to NBS Configuration Data
- Procedures for Reference Data maintenance through Enrichment, specifically RD/PRD/002
- Procedures for end to end reconciliation processes [NBR041]

17.9 PPDS

Pathway will develop clear and unambiguous processes and procedures to support NBS Transactions. [NBR463]

These are to be documented in the *Processes and Procedures Documents* (PPDs) [NBR026, NBR500]

Chapter 18 Acceptance and Integration Testing

18.1 GENERAL

This Section briefly describes the strategic approach to be adopted by Pathway for the integration and testing of NBS and the related infrastructure. It does not set out to describe in detail the individual testing processes, but rather it concentrates on highlighting the specific facets of the NBS that will require particular attention. In this respect, it refers to, rather than describes, those processes that have become well established and agreed over time on the Horizon Programme, selecting the appropriate processes for the NBS, and indicating where modifications to the existing approach are to be considered.

It sets out the established testing life cycle, the testing required to validate the new infrastructure needed to support NBS, and the proposed strategy for testing the NBS release.

It proposes a number of changes and additions to this established approach. These will be expanded in CCDs, under the Change Control process, to identify the implications on the underlying testing and integration processes. Such CCDs will form the agreed testing strategy for this system [NBR062].

18.2 REQUIREMENTS SUMMARY

Two aspects of NBS will cause a significant impact on the normal Pathway validation and testing strategy for new Releases.

- The decision to include the WebRiposte facilities in the Counter architecture
- The possibility that the interface to LINK may need special certification. This can take up to six months.

The first of these will cause a significant change to the overall Counter infrastructure, and in particular will pose a number of interesting migration problems, similar in complexity to those successfully overcome at CSR+.

The second raises many issues to do with liability for security breaches, financial reconciliation and performance measurement that are discussed elsewhere in this note. The conclusion in each case is that sophisticated, detailed and thorough testing is needed to ensure that any such issues are resolved before the relevant service is introduced into the live Horizon estate.

18.2.1 Acceptance Process

The Acceptance Specification shall comprise a combination of “Specification Conformance Testing” criteria (relative to the functional characteristics of the system) and an “Operational Conformance Checklist” (relative to the Service Description). [NBR059]

These criteria may cover the following.

18.2.1.1 Technical Tests

Scripted tests against which the Service is formally tested to check that the actual result conforms with the expected result.

18.2.1.2 Demonstration

This applies particularly to trial situations where the test processes have not been scripted.

18.2.1.3 Document Review

The examination of documents that Pathway are required to produce (e.g. PPDs).

In addition, there are criteria which are examined by:

18.2.1.4 Endorsement

This applies to those situations which are not readily testable by the preceding methods, but which PO Ltd accept (although may be caveated against subsequent experience).

An example is where Pathway will ensure that the HSHD staff are trained to deal with NBS calls, another being the requirement that Pathway is able to provide suitable evidence to support prosecutions. [NBR547]

18.2.1.5 Current Contract

Many of the NBS characteristics are extensions of the current contractual requirements. PO Ltd has already accepted that Pathway conforms with these contractual obligations, and a separate demonstration is unnecessary unless the introduction of NBS significantly effects some charateristic.

These, when taken together, represent the criteria against which the Release Authorisation Board recommend acceptance of the system.

The NBS shall be deemed to have been accepted in the event that the Release Authorisation Board recommend that the NBS be fully rolled out on the successful completion of the live Pilot(s).

On acceptance of the principle of this approach, Pathway will prepare a draft Acceptance Specification.

18.3 TESTING LIFECYCLE

The purpose of the testing lifecycle is to confirm the release is fit for the live environment, and that the risks of going live are known and assessed. [NBR473]

At a high level the established testing lifecycle for the introduction of substantial new components is as follows:

- Technical Evaluation – informs design stage
- Code Review
- Unit Test
    - Module Test
    - Link Test
- Product Integration Test
- System Test [NBR477]
- Direct Interface Test – for systems with external interfaces
- Integration Test
    - Conformance Testing
    - Volume and Integrity Test
    - Release Test
- Regression Testing (Tivoli and infrastructure – in case of implementation failure)
- PO Ltd Driven Testing
- Live Pilot

These are carried out as considered necessary by Pathway under Pathway control. All of these lifecycle stages apply for the introduction of NBS; these testing principles have been established and documented over the past five years.

18.3.1 Infrastructure Changes

The introduction of NBS requires major infrastructure changes. Most prominent is the adoption of WebRiposte. These in turn require more recent versions of Tivoli and other underlying Counter software. The relevant stages for each and the tests that Pathway will carry out in respect of them are listed below.

18.3.1.1 Tivoli

- Product acceptance test to verify the completeness of the third party deliverable
- Product integration test to mount the update correctly on the test rigs and to establish the correct configuration
- Conformance test to confirm non-regression of the Systems Management facility, with particular attention to performance for high volume distribution
- Limited release test to validate and rehearse the migration and implementation method
- Repeat conformance test following update of Counter infrastructure to confirm compatibility and non-regression

18.3.1.2 Counter Infrastructure Update

- Technical evaluation to confirm correct selection of necessary component updates to achieve inter-compatibility
- Product integration test to mount the updates correctly on the test rigs and to establish the correct configuration
- Conformance test (including limited business scenario based testing) to confirm non-regression, with particular attention to secure build validation
- Limited release test to validate and rehearse the migration and implementation method
- Repeat conformance testing following introduction of WebRiposte to confirm compatibility and non-regression

18.3.1.3 WebRiposte

- Technical evaluation to confirm understanding of the new product and to determine migration implications
- Product acceptance test, with particular attention to non-regression (e.g. using sample system test regression packs), new facilities (most likely requiring the construction of a test harness to enable each interface to be exposed to test)
- Product integration test to mount the update correctly on the tests rigs and to confirm the correct configuration
- Extensive conformance test to confirm both non-regression and new facilities, with particular attention to performance, security, data integrity, and recovery, and with limited business scenario based testing, to confirm non-regression
- Limited release test to validate and rehearse the migration and implementation method

In planning the testing for these infrastructure changes, it is important to note that each requires testing in combination with the next to confirm forward compatibility. This can be seen in the duplication of activities described above. Pathway will use reasonable endeavours to plan the overall testing sequence so as to eliminate these duplications and so effectively reduce the testing cost and time required.

Note that the above list is not exhaustive. Other infrastructure changes are also required and need to be validated, such as changes to the systems supporting OBC (e.g. OCMS and ACDB).

18.3.2 NBS Applications

18.3.2.1 Context

The testing strategy for the NBS release is predicated on the following: [NBR550]

1. The NBE will be operated by IBM for PO Ltd, and responsibility and liability for correct working and availability will be entirely outside of Pathway except in respect of end-to-end response times for authorisations and compliance with the agreed interface specification(s)
2. Pathway will be responsible for integration of the NBS and associated additional infrastructure with the existing Horizon infrastructure such that existing service levels are protected, including aspects of security, performance, availability, integrity, recovery as described in [SRS]

3. Pathway will be responsible for confirming functional conformance of the whole Outlet system with the stated business requirements

18.3.2.2 The TMS

TMS is used by, rather than being a part of, NBS. It is an infrastructure product. No separate specific testing of TMS is required beyond that described in the entry above on Infrastructure Changes and the entry below on Integration Test.

18.3.2.3 The Campus Systems

These are all exclusively Pathway deliverables, and they employ existing techniques and technologies familiar to Horizon. As such all stages of the established test lifecycle apply. Pathway will continue to observe good practice but reserves the right to change its approach if it believes an alternative approach is more appropriate in the prevailing circumstances.

18.3.2.4 The Network Banking Engine

This system lies outside Pathway scope except for the communications interfaces with Campus systems, as described in [NBETIS]. A dummy agent will be used to simulate responses from the NBE for unit test, system test, and conformance testing. It is expected that for direct interface test, and PO Ltd driven testing, an appropriate NBE will be made available.

PO Ltd together with IBM are responsible for providing access to the NBE.

It is expected that the ‘actual’ NBE, together with a responder test service at the FI or LINK, will be incorporated in a End to End test and a high volume trial to confirm response time performance and throughput capability. Pathway will review their involvement in that Test Strategy, when it is available. [NBR499]

18.3.2.5 The FI Systems

These systems lie outside Pathway scope.

18.3.2.6 The PO Back End Systems

These systems lie outside Pathway scope except for interface with Campus systems. These are predominantly batch interfaces and require no special provision for testing the Campus systems in isolation.

PO Ltd is responsible for making available appropriate test systems for direct interface test, PO Ltd driven testing. It is further expected that a full capability test system will be made available for high volume trials to confirm response time performance and throughput capacity.

18.3.2.7 Direct Interface Test

Each agreed external interface will be subject to direct interface testing, to start the process of validating the AIS/TIS for the interface concerned (see [NBEAIS] and [NBETIS]). This is a well-established process on Horizon [NBR478].

With NBS, the only special case worthy of additional explanation is the interface with the NBE, because it involves On-line interactions. The Campus systems involved will have, as already described, previously been subject to testing using a dummy Agent to simulate the possible NBE responses and so to pre-validate those systems against the agreed AIS/TIS.

PO Ltd is responsible for ensuring that the NBE will have been pre-validated to reduce the risk of abortive attempts to conduct direct interface testing. Pathway shall have the entitlement to recover additional costs if abortive attempts occur as a result. In planning the direct interface testing, the implications of a On-line interface need to be taken into account. In general, until they have become stable and reliable, it is advisable to schedule short frequent testing slots, and to gear up development support teams to provide rapid resolution of problems in the intervening periods.

This is in contrast to batch interfaces where typically a number of larger tests can be run in the same test slot, finding a whole series of problems, and leaving a longer intervening period for resolution before the next slot is scheduled.

18.3.2.8 Conformance Test

This builds on the conformance testing performed for the infrastructure changes, described above. It is directed at a number of separate validation objectives including reconciliation, performance, integrity, systems management, and business scenario based integration tests.

18.3.2.8.1 Security

The NBS Application, in conjunction with the Horizon Systems, will be subject to security testing to confirm that the introduction of the new systems has not compromised security. [NBR474]

In this respect the secure build configuration for each platform affected will be re-confirmed. In addition specific sample tests will be performed to confirm non-regression for the supplementary security provisions, including filestore encryption, digital signatures, and Key Management. (This testing is likely to be extensive.)

18.3.2.8.2 Performance

Appropriate performance modelling and measurement will be performed to confirm that the introduction of the new systems has not compromised the agreed Service Levels with respect to the performance of the existing Horizon infrastructure and services, as described in the Codified Agreement, in accordance with [PERFSTRAT]. [NBR489]

In addition, appropriate and agreed performance modelling and measurement will be performed to confirm that the infrastructure required for NBS, in the context of the Horizon environment, is capable of supporting the projected business workloads, or is proven to be scaleable to do so. [NBR475]

18.3.2.8.3 Integrity

The NBS Application, in conjunction with the relevant parts of the existing Horizon infrastructure, will be subject to integrity testing to confirm that the introduction of the new systems has not compromised the required levels of system integrity, with particular regard to resilience, and recovery. In this respect, specific sample tests will be performed to confirm non-regression in each of the recognised failure scenarios.

In addition, a disaster recovery rehearsal can be performed, under PO Ltd overall management (i.e. including NBE failover) simulating loss of a Pathway Campus and subsequent recovery to full capability. (This testing is likely to be extensive.) [NBR476]

18.3.2.8.4 Systems Management

No additional systems management tests will be required for the introduction of the new system beyond those already performed for the Infrastructure Changes, described above. However, the running of the business scenario based testing, and the release test (see below) involve the use of all these facilities in managing the test rigs, so they are indirectly validated by usage throughout.

18.3.2.8.5 Business Scenarios

Wherever practicable, the above Conformance Tests will be designed and planned to be run in the context of long business scenarios, integrating the whole Pathway system set, from Outlet Systems through to Host Systems, and using the ancillary systems (such as systems management, audit and archive, in the day to day running of the test environments. (Where it is not practicable, then separate point tests will be performed.)

18.3.2.9 End to End Interface Test

It is expected that the PO Ltd Testing Strategy will build upon the earlier PET/UCT Testing performed by Pathway and run End to End in the context of the whole Horizon system in conjunction with all external interfaces – 'Day In The Life Of' style – designing the scenarios such that business data flows end to end, and back where appropriate. In this way, the operational aspects of the AIS/TIS will be validated, and not just the functional conformance. PO Ltd is responsible for ensuring all external systems make suitable test environments available (and operate them) for these tests.

18.3.2.10 Acceptance Testing

Pathway will prepare an Acceptance Specification for the NBS, in conformance with [CA] as amended and with certain CCDs.

The Acceptance Specification shall comprise a combination of "Specification Conformance Testing" criteria (relative to the functional characteristics of the system) and an "Operational Conformance Checklist" (relative to the Service Description). [NBR059]

These criteria will cover the following.

18.3.2.10.1 Technical Tests

Scripted tests against which the Service is formally tested to check that the actual results conform with the expected results.

18.3.2.10.2 Demonstration

This applies particularly to trial situations where the test processes have not been scripted.

18.1.1.10.3 Document Review

The examination of documents that Pathway are required to produce (e.g. *Process and Procedures Documents* (PPDs))

In addition, there are criteria which are examined by:

18.1.1.10.4 Endorsement

This applies to those situations which are not readily testable by the preceding methods, but which PO Ltd. accepts (although may be caveated against subsequent experience).

An example is where Pathway will ensure that the HSHD staff are trained to deal with NBS calls. Another is the requirement that Pathway is able to provide suitable evidence in accordance with [PACE].

18.1.1.11 Release Test

The migration/implementation of the NBS release will be iteratively rehearsed on large scale test rigs, in co-operation with suitable test harnesses simulating all external systems to confirm the viability of the release as a whole.

PO Ltd is responsible for the involvement of the NBE, and the use of all pertinent operational and user procedures intended for use with the system.

18.1.1.12 Subsequent FI and Product Take-on

Following Live implementation, when a new Client FI or product is planned and agreed to be introduced, and where there is, in Pathway's opinion, no significant change to the application (etc.) required, then it is proposed that the existing fast track verification process be adopted as is currently employed for AP Client take-on. Revisions will be required to tailor it for the OBC process for NBS, and a study will be needed to carry out these revisions.

Where changes to applications (etc.) are required which, in the opinion of Pathway are significant, then the established test lifecycle will be adopted as described above.

18.1.1.13 PO Ltd Driven Testing

In the past on Horizon a number of different forms of joint testing and PO Ltd driven testing have been performed, with varying degrees of success. A post implementation review of this testing for the CSR+ release made some recommendations for lessons to be learned in this area. A study will need to be carried out to determine and agree the most appropriate way forward in this area.

18.1.1.14 Live Pilot

In the past on Horizon, each major release has made use of a live trial period in which the number of Outlets exposed to the new system was restricted and the system behaviour closely monitored, prior to rolling the system out across the whole country.

Chapter 19 - Service Introduction Strategy

19.1 GENERAL

This Chapter covers the processes involved in bringing the NBS into use, including the infrastructure enhancements needed to support it, once they have completed testing & integration.

19.2 REQUIREMENTS SUMMARY

The single most important requirement for NBS is that the service should be available during 2002 and contain the functionality required to support both private banking and customers of the POCA.

The Programme Plan is thus designed to implement the NBS capability through the smallest possible number of Releases, with minimal disruption to operational service, and with appropriate and thorough testing.

This is best achieved by a single functionality Release (BI3). Pathway notes the requirement that the system shall be able to revert to any earlier version of NBS without disruption to the operational service. However, no NBS Release is planned other than the BI3 Release described in this SDS. [NBR498, NBR502]

19.2.1 Service Introduction Planning

The introduction of NBS requires:

- Infrastructure upgrades and software release
- Certification
- Pilot(s)
- Service Launch

The timescales for each of these activities will be discussed with PO Ltd. [NBR412]

19.2.1.1 Infrastructure Upgrades and Software Release

The infrastructure upgrades require both physical hardware and network upgrades, and upgrades to the software installed throughout the Pathway domain. Much of this must be applied prior to the implementation of NBS, though some (required as the workload increases) can be applied later.

19.2.1.1.1 Installation of PIN Pads

The infrastructure shall be designed and implemented to support PIN Pads, although the roll out of PIN Pads is not part of this SDS.

19.2.1.2 Certification

The Service will need to be fully accredited by LINK and by the FIs before a live service can be authorised. It is the responsibility of PO Ltd to organise this phase, which must be initiated during the PO Ltd driven testing phase and continued through the live Pilot phase, if required.

Pathway is dependent on PO Ltd to document what the requirements are concerning the Certification process and the dependencies on Pathway.

19.2.1.3 Pilot(s)

Pathway recommends that only one or two FIs be involved with the Pilot phase, so reducing the need for the initial take on of PO Ltd Reference Data. However, live Reference Data will have formed the basis for the latter stages of testing, and this will have established synchronisation between Horizon and the NBE. [NBR414]

Pathway recommends that the following Pilots be adopted.

- Pilot of 10 Outlets with one or two FIs for a minimum period of two weeks
- Pilot of 300 Outlets, with one or two FIs for a period of 2 months (rising to take on additional FIs in later stages of Pilot)
- Full roll out of Service to all Outlets (Service Launch), subject to authorisation by the Release Authorisation Board.

19.2.1.4 Service Launch

Launching NBS is the responsibility of PO Ltd, and Pathway wishes to discuss and understand the impact this will have at the earliest opportunity.

Service Launch will require PO Ltd to:

- Train the Counter staff
- Advertise the Service (this could potentially be a national advertising campaign)
- Coordinate the Launch with the FIs
- Roll out the POCA bankcards

19.3 MIGRATION STRATEGY

19.3.1 Objectives of the Migration Strategy

The strategy has been developed with the following objectives.

- The single most important objective is to introduce the NBS service with full software functionality within PO Ltd's timescales
- To this end, only a single functionality Release is planned.
- The functionality in this Release will be no more than it is possible to provide within the timescale.
- Non-software enhancements (such as to the Network) that are required to support full rollout volumes can be provided once the initial service is available, so long as this can be done without disrupting the provision of the NBS (or any other) service

19.3.2 Release Schedule

Currently two major Releases are planned:

- BI2 –Infrastructure upgrades. These are introduced in several stages at the Campuses, and two stages at the Counters, because of the complexity of the total upgrade requirements.
- BI3 – Application Introduction. This is the single functionality Release described above

In addition to these, a range of post BI3 – Service Improvements will be needed to support full rollout volumes. These include network upgrades prior to full rollout and introduction of the POCA.

The order in which the required upgrades are applied is important and has a significant impact on Pathway's Programme plans. The scope of the changes identified in this document is such that every platform in the Horizon system is affected in one way or another. A number of issues arise when planning the migration of the estate to the Releases proposed.

19.3.2.1 Counter Releases

The most important consideration is the Counter population, where any upgrades must be applied remotely. If a particular upgrade becomes too large or too complex, there is a likelihood that it will fail in a significant number of Outlets. Splitting the required upgrades into a large number of small steps will, however, increase the complexity of the overall testing and impact on the total time required to implement the necessary upgrades.

Some of the upgrades are extremely complex and high risk. In every case, upgrades implemented via Tivoli are transmitted with a regression capability that can be used to remove the upgrade should this prove necessary. The design and complexity of the regression capability obviously depends on the complexity of the upgrade, and the regression capabilities (if any) provided by the component's supplier. It has been necessary at times to go beyond published upgrade support guidelines (for example for IE) to ensure a regressible upgrade. The following is a guideline to the risk level of a Tivoli initiated upgrade.

Risk	Description	Mitigation
High	The upgrade has a complex regression script, and has the potential, if it goes wrong or is incomplete, to leave the Counter in a state where a hardware swap out is required	▪ Early exposure of the upgrade and regression issues ▪ More thorough than usual testing of the upgrade process itself ▪ Don't do any other high- or medium-risk upgrades in the same SIP
Medium	There is a regression route, but If the upgrade goes wrong and does not regress properly, it will require Help Desk intervention to get the Counter back to a working state	Thorough testing of both the upgrade and regression route
Low	No particular difficulties if the upgrade is missed, incomplete or fails	Normal *Pathway Testing Unit (*PTU) testing

Table 34 – Tivoli Upgrade Risk Levels

As at CSR+, migration testing for NBS will test not just the "straight through" paths, but all the failure conditions that could arise following, for example, a power failure at a critical point in an Outlet upgrade.

19.3.2.2 Campus Migration

At the Campuses, it is assumed that the same version of a product is used throughout the estate. There are clear benefits to this, including a greatly simplified support situation. However, as indicated in Chapter 11, there may be cases where for some reason or other it is not possible to make such an "across the board" upgrade. For example, the DRS service will run on an Oracle 8i database while some other Host applications (LFS, OBCS, APS) remain on Oracle 7.3.4.5.

With Campus systems, there is a choice between an upgrade and a rebuild. The preferred route is to upgrade, and all Campus platforms can be upgraded via Tivoli. Only when there are too many fixes is the system re-baselined by PIT.

19.3.3 BI2 – Major Infrastructure Upgrades

For technical reasons, discussed below, it is proposed that the remaining infrastructure upgrades required before NBS can be brought into use are carried out in one Campus and two Outlet upgrades.

Note: [SRS] states that BI2 will upgrade the infrastructure to support full rollout volumes. This is not in fact proposed. Instead, the hardware capacity at the Campus will be enhanced in this way, but the network and some other workload-dependent aspects, that can be enhanced in isolation from the rest of the Horizon system, will be left until after BI3.

19.3.3.1 Timescale

BI2 will be introduced in a number of stages commencing in March 2002.

19.3.3.2 BI2_CA – Campus Correspondence Server Changes

The migration to four Correspondence Servers in a Cluster is complex, particularly when other changes such as Service Pack upgrades are taking place. It needs to be carried out before the main software upgrades. It needs to include the following activities.

- Split off the existing Compaq recovery Option Correspondence Servers. This will need to be done on a Sunday. It will then allow new Correspondence Servers to be added (upgrade of Wing at Bootle to 450 MHz / 550 MHz systems, provision of a wing at Wigan – requires new Compaq Disks)
- Change the Counter Call Scheduler to make inward calls to replace the existing outward calls. Changes to Maestro and Counter Call Scheduler configuration (Reference Data change only) to remove the Correspondence Server outward call windows (Outlets will dial in instead)
- Buy and install Compaq disk arrays for Wigan. Build and install extra Correspondence Servers per Riposte Cluster. This can be done during the week

- Change Maestro to start managing the new Correspondence Servers for archiving and index rebuilds
- Remove the Wing Correspondence Server. This can be done during the week once the new servers at Bootle have been built
- Upgrade in a migration weekend to the new version of commodity products including Riposte and NT4 SP6a on Generic Agent Servers and Correspondence Servers.
- Change the routing to the Correspondence Servers to have only one network address used for Counter traffic
- Make ACDB changes to the neighbour definitions used by the Gateway PC in the Outlet
- Change Tivoli to start populating Outlet neighbour definitions in the new Correspondence Servers.
- Configure half the Generic Agent Servers to use the new Correspondence Servers. This has to be done after the Counters have started using the new Correspondence Servers, to avoid errors

19.3.3.2.1 VPN Servers

Replacements of the existing VPN servers by more powerful and smaller processors. These will have been built in advance with a full BI2 baseline, and then exchanged for the existing VPN Servers. There is no need to upgrade the existing servers.

During this upgrade care must be given to ensure a network path is always available for Riposte and Tivoli traffic through the VPN servers.

19.3.3.3 BI2_CB – Campus Software Changes

Once the Correspondence Server changes are complete, the Campus software changes will be done during a single weekend. Bootle will be done on the Saturday, with Wigan on the Sunday. These will be handled in a single Campus upgrade prior to any Outlet upgrades. This migration will include the following stages.

19.3.3.3.1 Campus NT Servers and Workstations

All NT platforms will be upgraded as follows.

- Upgrade to NT 4.0 SP6a
- Upgrade to Internet Explorer 5.5 SP1 where relevant
- Upgrade to Riposte Message Service V6.2.nn (“WebRiposte”) where relevant (e.g. Correspondence Servers)
- Legato

19.3.3.3.2 ACDB and OCMS Servers

- Upgrade to SQL Server V2000

19.3.3.3.3 SecurID Server

- Upgrade to ACE/Server V4.1

19.3.3.3.4 KMA Servers

The KMA Servers will be upgraded to SQL Server V2000. Special care will need to be taken with this upgrade. There are two KMA Servers, one at each Campus, one live and one a “hot standby”. Their databases are kept in step via the EMC Disk array and SRDF features. Thus, the upgrade will involve taking both databases out of operation for around 16 hours.

During this upgrade, no unattended reboot will be possible, and if a Post Master loses his PIN he will have to wait until the upgrade is complete before he can get back on line.

This upgrade will affect:

- Help desk applications
- Agent Server code
- ISD processes
- Security scripts
- KMA security model

It will be done as part of the migration weekend as the system can be taken out for a few hours to do the upgrade.

An upgrade is required to the EMC Disk Array (shared with Host Central Servers) and of EMC driver software. This will be done as part of the Host disk change (see below). It must be done after the software upgrade, due to the service pack dependencies.

The KMA Server will also be upgraded to support VPN on the LAN in Outlets.

19.3.3.4 BI2_CC – Campus Host, Data Warehouse and EMC Changes

Once the estate has been migrated to NT 4 SP6a and IE5, the EMC cabinets and Host Central Server upgrade can be done. This dependency exists because the version of the EMC control software (on the KMA server) needed to drive the new EMC Cabinets is not certified on SP3, and hence the upgrade needs to be carried out after the upgrade of the KMA Server to SP6a. It will take at least one weekend.

The upgrade to the new EMC cabinet can be done at any time prior to BI3, and will be a significant migration in itself. It is recommended that this is done early, before free floor space becomes an issue in the Campuses. EMC professional services will be employed to assist with the EMC Array migration exercise. Their experience in carrying out migrations from one EMC array to another will significantly reduce the associated risk.

The upgrade to the new processor (and Dynix version) on the Host Central Servers and Data Warehouse Servers can be done at any time prior to BI4, subject to testing constraints. This, too, will take at least a weekend. It is sensible to keep the Host Central Server and Data Warehouse Server hardware in step with each other.

19.3.3.5 BI2_OA – Outlet Internet Explorer and Service Pack Upgrade

This Increment carries out the Counter upgrade to NT4 SP6a and IE5.5 SPn. These both constitute High Risk upgrades, but it is believed that they can reasonably be introduced together, subject to detailed and early validation of the migration path.

Also at this stage, changes are made to the configuration of Correspondence Server Neighbours on the Gateway PC, to exploit the move from two to four Correspondence Servers per Cluster.

This upgrade introduces no new business functionality, and should not be visible to Outlet staff.

This upgrade will be designed such that it is done on a Counter-by-Counter basis, not a whole Outlet at a time. This is important because if an Outlet-wide upgrade is required, it cannot start until all Counters are available (i.e. logged out). Equally importantly, if one Counter fails to upgrade and needs to be regressed, this should not cause the entire Outlet to be regressed.

Note that a Counter reboot will be necessary on all Counters, using the unattended reboot functionality introduced at S10.

Note that the introduction of PIN Pads is likely to require a Counter reboot to install the appropriate drivers, and so if the drivers are available and validated it is sensible to introduce them at this point.

19.3.3.6 BI2_OB – Outlet Wide Software Changes

Once BI2_OA has been completed, a second change to the Outlets is required. This will introduce the following enhancements.

- Introduction of VPN on the LAN
- Introduction of WebRiposte

This change will be Outlet wide and will need to be implemented or regressed autonomously across all Counters in an Outlet.

Note that this upgrade introduces no new business functionality, and should not be visible to the Outlet staff.

19.3.3.6.1 VPN on the LAN

VPN on the LAN is a complex and high-risk operation and ideally should not be done at the same time as any other significant upgrade. However, adding it to the release of WebRiposte and associated changes does not increase this risk significantly, but does greatly simplify the testing and migration timescales.

This upgrade is scheduled to be done *after* the upgrade to SP6a, so that it does not need to be validated on both SP3 and SP6a.

A reboot is required on each Counter to activate VPN on the LAN. This will use the unattended reboot functionality introduced at S10.

19.3.3.6.2 Introduction of WebRiposte

WebRiposte, like any other upgrade to the Riposte Message Store, *will* require that all Counters within an Outlet are upgraded at the same time. All Counters in an Outlet must be at the same Riposte version.

19.3.3.7 Link to NBE

At this stage, it is possible to introduce the links needed to support access to the NBE, and the associated Campus infrastructure, as described in Chapter 10.

19.3.3.8 Network Enhancements for Enhanced Tivoli Software Distribution

The *Outward Call Routers* are introduced so that the ATE has the capability to dial out to Outlets to force an inward call for software distribution purposes.

19.3.4 BI3 – Introduction of NBS Application

BI3 introduces the NBS and DRS applications, and associated enhancements (such as to RDMC).

This upgrade is visible to Outlet staff in that it introduces the new NBS application. It should be preceded by a period of training for both Outlet and Help Desk staff.

At the Campus, a number of changes are made including the following.

- Introduce the DRS application running on the Host Central Servers.
- Upgrade Generic Agent Servers
- Install NBS Agent Servers. The software that runs on them (NBS Authorisation Agents and EoD File MAC Checker) are introduced at BI3
- Generate and distribute keys used for NBS, including those required by the NBS Agent Servers
- Other Agent processes change at BI3, including the TPS Harvester Agent
- MIS and Audit functionality is introduced to support NBS
- Service management and support enhancements are introduced

The NBS Counter application is distributed via Tivoli, and is introduced by the targeted distribution of “trigger” objects, first as a pilot in some 300 Outlets, but followed shortly thereafter by rollout to all live Outlets.

Other Counter developments are introduced as part of the same package. These include EPOSS developments, to incorporate NBS transactions

19.3.4.1.1 Reference Data Management Service (RDMS)

The RDMC and RDDS applications and databases are upgraded to Oracle 8i. Note that the DRS, when it is introduced at BI3, will also run on Oracle 8i

19.3.4.1.2 Host Applications

The DRS service can be installed prior to BI3, and is introduced by Maestro schedule changes It needs to run along side the existing Host applications for most of the day. In the early evening slot when harvesting takes place, the DRS application will be configured to have a low resource usage. To avoid impacting the existing Host services significantly, it may be worth considering restricting the number of processors that the DRS application and database can be run on (to say two).

The prior upgrade to the existing Host Central Server should provide sufficient free capacity for the DRS application. However, this needs to be proved by performance testing.

19.3.5 Network Migration Strategy

Once NBS is in place, it becomes possible to switch selected Outlets from dial-up ISDN communication to permanent network connections. At the Counter, this is done by changing the number dialled by the Outlet’s Gateway PC, and by making a number of other configuration changes to Riposte and the ISDN card. These will be initiated by ACF and changes are made to ACDB at BI3 to support this.

However, before this can take effect, it is necessary to introduce the FRIACO service. Chapter 10 describes the modifications to the ISDN network needed to support the increased load associated with NBS and EFTPoS. This Section discusses the stages necessary to implement that enhanced network. They may be made in parallel with the BI3 migration described above, and early stages can in fact precede the introduction of BI3.

The following assumptions are in addition to the points covered in Chapter 10.

- FRIACO telephone numbers will be in two sets, Wigan facing and Bootle facing, thus on completion of the migration exercise, half of the Outlets will point at Wigan as Prime and the other half will point at Bootle as Prime. Secondary numbers will be the other Campus's FRIACO Numbers
- The Energis ISDN *Closed User Group* (CUG) for Pathway remains fully operational throughout the migration exercise
- Separate telephone numbers are provided for Horizon and YG
- The CHAP "wait for reply" timer, as introduced into the Eicon driver for the SATELAN solution, will remain. CHAP handshakes may fail due to timing problems as the CHAP negotiation is no longer point to point but disappears into the network cloud to find a Radius server for authentication
- Outbound traffic from Tivoli to the Outlets will be via the default ISDN route, at phase I, unless the VPN layer has been notified by the Summary and LAR Router layers that another route exists via the FRIACO Routers
- Outbound traffic from Riposte to the Outlets will be triggered

The migration consists of a number of stages, each of which moves a block of 1,000 Outlets from the voice network to FRIACO

19.4 TRAINING

PO Ltd is responsible for training Outlet and other PO Ltd staff, including the development and production of appropriate training material.

Pathway will train its own staff, including those in the HSHD, and shall develop and produce any material deemed appropriate. [NBR272]

Pathway will not provide Training Mode for NBS (or similar functionality) to enable Outlet staff to familiarise themselves with NBS functionality.

Pathway is concerned that the introduction of a new Service will lead to a severe escalation in the number of Advice and Guidance calls attributable to NBS. PO Ltd shall be responsible for the cost of all Advice and Guidance calls to the HSHD in respect of NBS for 3 months after the introduction of the NBS into an Outlet.

19.5 TRIALS

As is normal with any release, there will be a trial period, during which a relatively small number of Outlets (typically 200 to 300) are migrated to the new release. These are generally run for at least a week before the changes are made to the rest of the system. There are a number of reasons for doing this including:

- Final proving that the service is fit for release to the whole estate
- Confirmation that manual procedures are correct and work in practice
- Early experience of any operational issues, before they cause significant service outages

At BI3, it is expected that the pilot period will last longer than usual. This is because NBS is a significant change to the working practices of the Outlet and the working of the NBE and reconciliation needs to be proved in the live environment.

19.6 COUNTER SPARES

The policy of Counter spares needs careful consideration.. The following spares baselines are proposed:

- Post BI2OA – Needed because of the time taken to migrate to NT4.0 SP6a and IE5 if this were done as a "catch up"

It is not believed that a Spares baseline is required for BI2OB. The introduction of VPN on the LAN involves very little new software. The Spares build from BI2OA should include the ability to join an encrypted LAN if it finds one. The introduction of WebRiposte can be carried out in "catch up" mode.

It is not currently clear if a spare is needed after BI3. This will be dependent on the amount of change in BI3.

Chapter 20 - Service Operation and Management

20.1 GENERAL

The operations, service management and support processes provided by Pathway are well established and have supported the rollout and delivery of the Horizon system for a number of years. The introduction of the NBS brings with it changes to the requirements placed on these teams that will change the way their processes operate and the tools that they will use.

NBS introduces a number of characteristics that the current solution is not designed to support. These significantly affect the operation and management of the service, in particular the architectural issues and processes that ensure that high levels of availability are established and maintained.

This Chapter covers the changes in the support processes and tools that are required to allow Pathway to meet the support requirements of NBS. Some of the requirements described in this chapter are documented in the [SOR], while others are derived from the requirements of Pathway support and operations organisations.

The requirements are described from the point of view of the:

- Postmaster
- Support teams
- Operational and network management teams
- CS Service management

The Pathway requirements for NBS focus on meeting the SLAs for NBS availability and the Outlet time to fix when the NBS is not available at an Outlet. Many of the changes are concerned with identifying the cause of common problems as early as possible in the support process, and putting in place rectification actions. [NBR054, NBR534]

This Chapter does not cover the support and operational requirements for other new services e.g.:

- EFTPoS
- Talexus
- Your Guide

These will be considered separately.

20.2 SERVICE MANAGEMENT

Service management, in the context of this document, is concerned with the ability of Pathway to manage the Horizon solution following the inclusion of the NBS. The service management requirements generated are internal to Pathway. They are derived PO Ltd's requirement as defined in [SOR], and Pathway's continuing need to meet the SLAs defined by [CA].

20.2.1 Service Failure Types

Component failures, including network failures, are the most likely cause of service level breach. The design of the Horizon solution, including the addition of the NBS, takes into account the possibility of component failure and the consequential impact on the ability to operate the service.

20.2.1.1 High impact Failures

These affect many Outlets. Examples include:

- Failure of the NBE
- Failure of some Campus systems e.g. the NBS Authorisation Agent

Components that have a high impact on the ability to offer the NBS have been designed to be resilient to the majority of failure conditions, however it is not possible to totally eliminate failure. The Horizon system is a *high availability* system not a *non-stop* system.

The failure of certain components outside the Pathway operational domain, for example the NBE, can cause loss of service to all Counter positions. These failures are not under the control of Pathway. However, Pathway must ensure that it protects the Pathway operational domain and the Pathway SLAs in the event of such failures.

20.2.1.2 Low impact Failures

These affect only one Outlet. Examples include:

- Failure of the Outlet LAN
- Failure of the Outlet to Campus network link

At present, the effect of a failure of the Outlet to Campus network would not stop the Counter Clerk from serving customers, and in all likelihood would go almost unnoticed by the Clerk, with service level agreement breaches applying only if the failure lasts longer than a couple of days.

However, NBS is totally dependant on the availability of the network connection to the Horizon Campus. The impact of a WAN failure is low, in that it will affect one Outlet per ISDN line failure, but the cost of protecting the network connection is high, especially given the number of connections (approximately 18,000).

20.2.2 Service Management

Service management is concerned with the day-to-day management of the Horizon system. Pathway must manage the system to ensure that SLAs are not breached. There are two aspects to this:

- Monitoring, alerting and informing on service failure
- Resolution of an issue highlighted by the monitoring

NBS has a number of aspects that generate new service management requirements:

- The on-line service – [R]/[A] message flow
- [C] message delivery – the near-time delivery of confirmation messages to the

NBE

- Reconciliation – the new DRS host application

- Reference Data – software delivery by Reference Data
- Increased MIS reporting associated with NBS Reconciliation and Reference Data delivery

20.2.3 Assumptions

- The Pathway *Horizon System Help Desk* (HSHD) will operate as the first line support with regard to the availability of the NBS at the Outlet, and will log all operational incidents [NBR504]
- Delivery of [C] messages will under normal circumstances be via a second connection to the Campus, and thus one or more [C] messages may be marooned at an Outlet following a failure in the network infrastructure. Marooned [C] messages will either be harvested once the communications fault is fixed, or retrieved as a consequence of any data recovery actions carried out at the Outlet – i.e. utilising the Day D laptop solution
- It is not possible to staff up the HSHD to support the volume of calls in all failure scenarios, for example failure of the NBE could result in calls from the majority of Outlets
- In the majority of circumstances, Postmasters will not call the HSHD following a failure of a central system if they are informed about the failure including the estimated time to fix
- Long-term failures of central components are unacceptable where they affect the availability of NBS at the Counter
- Metrics gathered by Pathway from the Pathway domain will be acceptable when measuring the network supplier's performance against contractual SLAs
- The current Host alerting mechanisms will be suitable for alerting of failures of DRS

20.2.4 Non-functional Requirements

20.2.4.1 Resilience and Availability

The mechanisms by which the monitoring information is delivered to the relevant support units must be:

- *Reliable* – the integrity of the information being delivered must not be in question. Operation support will use this information to initiate recovery actions and to inform the Counter Clerks of expected recovery times, and accurate information is vital to both of these
- *Resilient* – no single point of failure should cause long-term unavailability of information. If an outage does occur, it must either be recovered automatically or reported to the relevant support unit allowing manual recovery to be initiated. It is important that a lack of information is not mistaken for 'NBS operating successfully'. Long-term in this case is defined as over one hour.

20.2.4.2 Performance and Scalability

Information on the failure of components involved in the delivery of the NBS on-line service must be delivered to the interested parties, including the HSHD, within two minutes of the failure. This will permit the Help Desk(s) to put in place actions to reduce the possibility of large numbers of calls from Outlets.

Information on failures of DRS must be delivered within a timescale that allows recovery in time to meet the DRS SLAs.

Network quality of service information is, under non-failure conditions, delivered from the Outlet to the Campus daily, so that CS has access to the previous day's information. This is generated by the *Counter Network Information Monitor* (NIM; see Section 10.4) and returned to the Campus by Tivoli.

Reports on the Outlets and Counter positions that have not received urgent Reference Data are reported to the Reference Data team by 08:00 on the day of delivery. Urgent data is data that is sent the night before it is required. Failure to deliver non-urgent Reference Data is highlighted under a separate report by 08:00 on the day delivery was attempted.

Network monitoring will not itself generate additional calls, with the exception of attempting calls on a regular basis following previously detected outage. Any monitoring process will not adversely affect the performance of Horizon Counter positions.

20.2.4.3 Supportability

All system error codes, messages and prompts displayed on the screen should be written to the Counter NT event log in a time-stamped message. Note that user error messages such as "The amount must be between £10 and £100, in multiples of £5", will not be recorded in the event log.

20.2.4.4 Security

Sensitive data will be obscured before being displayed, and encrypted before being logged. Information will be pushed out from the Campus into the DMZ. There will be no unsecured access to Campus systems as a result of the developments documented in this Chapter.

Sensitive information made available outside the Campus will be protected, only being accessible by authenticated users.

20.2.4.5 Usability

Information displayed to the Counter Clerk that is to be relayed to support units will be:

- Simple in content – no complicated technical phrases
- Short – include the minimum information, for example, error code, date/time and transaction ID
- Printable – the Clerk will be given the opportunity to print the error information to the locally connected slip printer

Information made available to support units from the Campus on the health of various systems will be clear and unambiguous, allowing them to react quickly to a fault that will result in loss of service to a large number of Outlets.

Recovery tools for use in failure situations will provide immediate feed back on their success, or failure, to complete the required recovery action.

20.2.5 Changes to Service Management for NBS

20.2.5.1 Monitoring and Alerting of Components of the On-line Service

Those systems that affect the on-line NBS are monitored for failure, including failure of the resilience built into the systems. When designing the characteristics of the monitoring, a number of factors must be considered:

- Where has the fault occurred? Is it Outlet centric, or at the Campus and beyond?
- Is the failure persistent, or is it temporary or intermittent?
- What action is required from the Postmaster following a failure?

Failure handling should inform the Postmaster as to whether to raise a Help Desk call. The failure scenarios that require a call to be raised include:

- Failure within the particular Outlet– Outlet LAN, Gateway PC, Counter PC, failure of the Outlet to Campus network. These failures are Outlet centric and as such only affect the particular Outlet
- Campus failures resulting in the loss of the NBS at the Campus will result in loss of service to a significant proportion of the estate, and in these circumstances, it is not sensible for Postmasters to raise Help Desk calls. Failures in this category include:
    - Failure of the NBE
    - Failure of the Campus infrastructure – especially long term outage where the resilience mechanisms have failed to provide the necessary protection

  The service offered by the Campus infrastructure will be closely monitored and alerts will be raised on any failures that result in loss of service. The alert will allow the Help Desk to prepare for a possible influx of calls from Postmasters. Details of the actions taken by the Help Desk on central systems failure are included in Section 20.2.6.

The following table lists each error condition that can be distinguished by the NBS Counter application along with the proposed rectification actions.

Failure condition	Fault identification	Message to the Postmaster
Outlet LAN or Gateway PC outage	Check carried out during NBS Counter application initialisation phase. A visual Off-line Indicator displayed on all Counters within the Outlet	"The Network Banking service is currently unavailable from this Counter. If you have not done so already please call the Help Desk and quote the following error code: *n*."
Outlet to Campus network Outage – temporary	The CNIM service, running on the Gateway PC, will respond, indirectly via the Riposte Message Store, to the NBS request, sent by the Counter application, indicating there is a temporary network outage	"The Network Banking service is temporarily unavailable please retry in 5 minutes. Please do not call the Help Desk"
Outlet to Campus network Outage – permanent	Two mechanisms by which permanent faults can be identified: 1 One of the checks carried out during the NBS Counter application initialisation phase will examine the state of a network status object. The state of the object will be updated dependant on the status of the network connection to the Campus. 2 The CNIM service, running on the Gateway PC, will respond,	"The Network Banking service is currently unavailable from this Outlet. If you have not done so already please call the Help Desk and quote the following error code: *n*."

	3 indirectly via the CCS, to the NBS request, sent by the Counter application, indicating there is a permanent network outage	
Acknowledgement Agent outage	The NBS Counter application will timeout following the failure to receive the acknowledgement [A] message while the Off-line Indicator is not set	“The Network Banking service request has failed. Please retry immediately. Please do not call the Help Desk.”
NBE outage – slow response – some NBS transaction are succeeding	The NBS Acknowledgement Agent will respond to the NBS Counter application with a ‘timed out’ acknowledgement message.	“The Network Banking service request has failed. Please retry. Please do not call the Help Desk.”
NBE outage – recovery time unknown	The NBS Acknowledgement Agent will respond to the NBS Counter application with a ‘NBE failed’ acknowledgement message.	“The Network Banking service is temporarily unavailable. Please retry in 30 minutes. We are aware of the fault and are fixing it. Please do not call the Help Desk.”
NBE outage – recovery time known	All instances of the NBS Acknowledgement Agent will be updated with the time service will be resumed. The Agent will respond to NBS requests with a ‘NBE failed” acknowledgement message which includes the service resumption time.	“The Network Banking service is currently unavailable. Please retry after date/time. We are aware of the fault. Please do not call the Help Desk”

Table 35 – Outlet NBS Failure Conditions

20.2.5.1.1 Outlet Centric Failures

20.2.5.1.1.1 Failure Detection

In the case of long-term Outlet centric failures, it is expected the Postmaster will raise a call alerting Pathway to the failure. Where the Postmaster does not raise a call the current Campus monitoring will alert the second line support unit to the following three failure conditions:

- Outlet to Campus network
- Gateway Counter PC
- Outlet LAN

20.2.5.1.1.2 Fault Diagnosis

Help desk calls raised due to permanent faults in the Outlet infrastructure i.e. faults that stop the NBS operating, need to be resolved within the timeframe of the SLA. The NBS Counter application must determine the fault that is causing access to the NBS to fail. It will be able to diagnose certain faults locally; others will require feedback from other infrastructure components located within the Outlet.

The *Network Banking Counter Application* (NBCA) will display either a request for a retry, or an error code, following a transaction failure. An error code may be accompanied by a message requesting the Postmaster to retry the transaction or, if the failure is classed as permanent, to raise a Help Desk call quoting the error code. As the telephone used for the Help Desk call may not be adjacent to the Counter, the application will provide the Postmaster with an option to print the error message/code to the locally connected tally roll printer. The error code will help pinpoint the cause of fault and will allow the Help Desk agent to efficiently route the call to the relevant support unit.

Outlet centric faults will be detected as follows:

Outlet LAN & Gateway PC Faults

At initialisation, the NBS Counter application will check it can see the Gateway PC over the Outlet LAN. This will involve a Riposte level check to ensure that messages are flowing between the Counter and Gateway PC. If the check fails, an appropriate error code will be displayed.

Outlet to Campus Network Faults

Communication between the Counter application and the Campus is handled through components of the Outlet infrastructure, specifically Riposte and the CNIM. These need to provide feedback to the Counter application following a detected fault.

Detecting network related faults is complex. There are two aspects to it:

- *Monitoring at the network transport level*. This is done by the Counter Network Information Monitor (CNIM) and allows a reasonable accurate diagnosis of the fault, i.e. is it permanent or temporary
- *Monitoring at the Riposte messaging level.* This detects failures where the communications line is brought up successfully but no Riposte messages flow

20.2.5.1.1.3 *Enhancements to Counter Infrastructure and Application Components*

On-line Service Persistent Object

A new Riposte Local[48] Persistent Object will be created to assist in the management of on-line applications. This Persistent Object will allow Gateway PCs to inform on-line applications on other Counters of the status of the Outlet to Campus network. This Object will have two main purposes:

- To inhibit access to the online applications, for example NBS
- To help determine the reason behind a failed online transaction where no acknowledgement message is received

Counter Network Information Monitor Service (CNIM)

This new service runs on the Gateway PC and permanently traces all Level 2 (link level) communications activity on the Outlet to Campus ISDN line. This trace is examined to determine the nature of any faults. Its functions are described in Section 10.4. The design includes the creation of two trace files:

- Full trace of all ISDN activities
- Call digest including a single record per call which includes information about the call, for example any error code that was returned

Off-line Indicator

A visible indication of service unavailability will be provided for users of all on-line applications.

The on-line service may be unavailable at a Counter as indicated by the state of an on-line service persistent object that is maintained by the CCS, as described in Section 5.4.5.3. The Off-line Indicator will either be provided by:

[48] *Using a local persistent object limits the possible consequential index rebuild load on the Correspondence Server*

- An enhancement to the Riposte Counter infrastructure or
- A 'busy.exe' style application – a small window will display an icon indicating the on-line service is not available at that Counter. The window will only be displayed if any of the above conditions are true. The window will have the always-on-top property, and will be placed on the desktop in a location where it will not hide other desktop icons or information. Once online service is resumed, the application window will be hidden. [NBR236]

The exact nature of the Off-line Indicator will be documented in [CNTRDLG].

The Off-line Indicator will be "unset" when the Outlet successfully communicates with the Campus, and an appropriate message will be displayed on all Counters within the Outlet at an appropriate time.

Network Quality of Service Information

Network quality of service records will be generated on the Gateway PC from the ISDN trace generated by the CNIM. The *TMS Outlet Monitor Agent* running in the Campus will be extended to harvest these messages and write them into the OMDB. These records will be replicated to the SMDB using currently available mechanisms. Once on the SMDB, the records will be made available to Pathway Customer Services via three mechanisms:

- Web pages displaying standard reports generated in advance. The contents of these reports will be subject to review with the users once the network supplier service levels agreements are understood in more detail.
- Web pages allowing the quality of service records to be searched using pre defined queries. For example: list all Outlets that have suffered from more than three faults per day over the last two weeks
- Read only database access using a standard reporting package – Business Objects, Crystal Reports or SQL access. The reporting packages will be employed by expert users to ascertain network failure trends using the harvested quality of service records.

20.2.5.1.2 Failures at the Campus and Beyond

Components in the Campus and beyond have been designed to be resilient to the majority of failure scenarios. This is necessary because of the impact of a failure on the NBS. Complete breakdown of the resilience mechanisms will deny access to the NBS at a significant proportion of the estate. The proportion affected will depend on the component that failed, for example:

- Failure of the NBE will affect every Outlet
- Failure of a single NBS Authorisation Agent will affect 25% of Outlets

In these circumstances, it is important the Postmaster is dissuaded from calling the help desk, as the Help Desk would be swamped and the time to respond to a call would be well outside the SLA. To manage the number of calls initiated when a significant failure occurs, it is important that the error message displayed gives some indication of for how long the NBS will be unavailable.

To minimise the impact of Campus component failure, it is vital that failures are reported to the relevant support unit within two minutes. This will require close monitoring of all relevant components. These include:

- Post Office access layer
- Summary Router layer
- Access Routers
- VPN servers
- Logical Campus Routers
- Correspondence Servers
- NBS Agent Servers
- DMZ Router
- Firewall
- NBS Router

Components outside the Horizon Campus are outside Pathway operational domain. However, because of the effect that a failure of one of these components will have on the availability of the service at the Counter, it is important that Pathway receives notification of failures within two minutes. This information needs to be made available to both first and second line support.

20.2.5.1.2.1 NBS Resilience – An Overview

The current solution has been designed to be highly resilient to failure of any single component. In many cases, it is resilient to multiple component failures. For example, within the VPN layer, connections to eight servers need to fail before an Outlet is denied access to the Campus.

- The Outlet has multiple phone numbers by which it can contact the Campus. Each phone number addresses a different system within the Post Office Access Layer. Failure of a component in this layer will result in some Outlets dialling a different phone number than usual and being directed to a working Router within the Access Layer.
- The Riposte Message Service sends each on-line request to all four Correspondence Servers within the Outlet's Cluster. The route to each Correspondence Server is via completely separate components within the Access Layer and the Correspondence Server layer. Therefore, failure of single components within each of these layers will not affect the ability of the Counter to send a request to a Correspondence Server

Once the message arrives at a Correspondence Server, it is replicated to all other Correspondence Servers within the same Cluster. The active NBS Authorisation Agent will be connected to one of the Correspondence Servers within the Cluster, and therefore will receive the on-line service request. This request is forwarded via the NBS Authorisation Agent to the NBE. Once the message is passed across the Horizon/PO Ltd service boundary, it is the responsibility of the NBE. Failure to receive a response from the NBE will result in the NBS Authorisation Agent sending a failed acknowledgement message back to the NBS Counter application.

Due to restrictions in the NBS Authorisation Agent to NBE interface, the approach to Agent resilience within the Agent layer is less robust than that adopted by other layers of the architecture. All failures of the NBS Agent Server will be subject to a period where no service is offered. This is a consequence of there being a single Agent instance active at one time for that Cluster. Another Agent instance runs as a hot standby, but there will be a period during failover between the two Agent instances when no service is offered.

The network connection between the NBE and the NBS Authorisation Agent will be designed to be resilient to any single points of failure.

The objective of the resilience design has been to minimise service downtime. The effect of not doing so at the Campus will be that large numbers of Outlets will be denied access to the NBS. It has not been possible to totally eliminate failure – the cost of doing this would be excessive and probably not possible within the restrictive timescales available. As a consequence, it is necessary to provide on-line monitoring of all components involved in the on-line NBS transactions, with status information being fed directly to:

- Second line support, to allow manual recovery actions to be initiated immediately
- The HSHD, to allow them to prepare for a potential influx of calls from the Outlets
- The NBS Counter application, to enable it to be able to report where the failure occurred and prompt the Postmaster in a way that will dissuade them from making a call to the HSHD – there is no fall back in the event of failure of the on-line service.

20.2.5.1.2.2 On-line Service Monitoring

The SMC second line support unit currently monitors the well being of Campus components through the Tivoli Event Management service. With the introduction of an on-line service, the Campus monitoring paradigm needs to change. Each component involved in the on-line service should be monitored closely as to its ability to deliver the service it has been designed to provide. The rules of how this information will be collected are:

- Regularly – the non receipt of information should be classified as a fault with an alert being raised
- From multiple perspectives:
  - A health check of the platform itself, for example, are the relevant services running, are any performance Counters indicating abnormal conditions.
  - A health check from the perspective of adjacent layers within the architecture.
- These monitoring services must be protected from overload conditions in other parts of the Horizon management solution (i.e. the transport systems used must be partitioned from other management streams by either using discrete routes or expedited channels within the existing streams)

The systems that require monitoring are:

- Routers within the Post Office access layer
- Routers within the summary layer
- Access Routers
- VPN servers
- Logical Campus Routers
- Correspondence Servers
- NBS Agent Servers
- DMZ Routers
- Firewalls
- NBS Router

These systems fall into two categories:

- Commodity networking components: Summary Routers, Access Routers, logical Campus Routers, DMZ Routers, firewalls and NBS Routers
- Pathway specific systems: VPN Servers, Correspondence Servers and Agent Servers.

The commodity networking components are managed by the ISD networking team. They will continue to manage these systems. Additional monitoring will be required; however it is expected this requirement can be met using industry standard network management technology. The specification, configuration and management of this software remains the responsibility of the ISD network management team.

The Pathway specific systems will require bespoke monitoring to provide the necessary system information. Monitoring information needs to be provided to Second Line Support and in some cases the HSHD.

20.2.5.1.2.3 *Platforms*

This sub-section discusses the monitoring requirements of each platform type.

VPN servers

These are grouped together in Clusters. Failure of a single server should not affect the ability of a Counter to communicate with Campus systems. Loss of both servers within a Cluster could cause loss of service for some applications where the communication is to a single subnet within a Campus. However, this is not the case with NBS where the request for service is sent to all four Correspondence Servers within a Cluster. Four VPN clusters are thus used, and eight VPN servers would have to fail before there was a total loss of service at an Outlet.

Failure of a cluster during a NBS transaction could cause individual transaction to fail. This does not stop further transactions from working.

Correspondence Servers

Correspondence servers are grouped together in four Clusters of four servers. Each Cluster supports around 4,500 Outlets. Messages received by one server are immediately forwarded to the other Correspondence Servers within its Cluster. Loss of a single Correspondence Server will, at most, cause a transient loss of service. The actual duration of the failure is dependant on how long the NBS Authorisation Agent takes to fail over to use a different Correspondence Server. It is expected this will be less than five seconds. Failure of a Correspondence Server will affect any transactions that were in progress at the time of the failure; however further messages from an affected Outlet will be successful.

Correspondence server failure is an important event that requires urgent investigation, as for the period of the outage there will be a reduction in the number of copies of the message store, and the other Correspondence Servers within the Cluster may be subject to an increased load.

NBS Agent Servers

Failure of the Agent will cause loss of service to 25% of the Counter estate, i.e. all Outlets being serviced by the Cluster to which the Agent is connected. The hot standby Agent ensures that the total failure time is minimised, but there will be a loss of service at Outlets whilst the hot standby Agent determines that the active Agent is unavailable and takes over processing.

For this reason, a great deal of thought has gone into the resilience of this Agent. Each NBS Authorisation Agent is specific to a particular Cluster, and will make two connections to the Cluster's Riposte Message Service, each to a separate Correspondence Server via a different network route. Failover between the two message services will be measured in seconds.

The network connection to the NBE will be protected by the use of fully resilient network connections. Failover of any network component between the NBS Authorisation Agent and the NBE must be within 10 seconds.

20.2.5.1.2.4 *Failures Beyond the Pathway Domain*

Failure of the NBE will affect every Horizon Outlet. The NBE is not within the Pathway domain and therefore Pathway cannot influence its availability. Failures of the NBE should be reported within two minutes of the failure occurring. Failures must be reported into the Pathway domain automatically and made available to the HSHD via the SMDB. Details of the actions taken are included in Section 20.2.6.

The processes and procedures for managing such failures will be the subject of a joint agreement between Pathway and PO Ltd (see Section 20.5).

20.2.5.1.2.5 *Broadcast Message*

Due to the nature of some faults, it may not be possible for the Counter application to respond appropriately. In these cases, it may be necessary for the Outlets to be kept informed through the Broadcast Message function. This tool allows a message to be sent to all Outlets.

To ensure the message is sent within an acceptable time, a new fast track process will be developed, which will allow a message to be constructed, approved and sent within 30 minutes. Pre-formatted messages will be defined and agreed with PO Ltd covering all known error conditions where Message Broadcast may be used. The message will arrive at the Counter the next time it communicates with the Correspondence Server layer. This could be some time. However, it will be received by any Outlet that attempts an NBS transaction

20.2.5.1.3 Changes to the NBS Counter Application

There are various points during the execution of the NBS Counter application where faults can be detected:

- At application initialisation
- Following the receipt of, or failure to receive, a response from the NBS Authorisation Agent

20.2.5.1.3.1 *Transaction Initialisation*

The Counter application will start by carrying out a number of checks before the Clerk is asked to input any information These checks will ensure there are no local reasons why the NBS transaction should not continue. [NBR263]

These checks will include:

- Can the Counter position running the transaction communicate with the Gateway PC?
- Is access to on-line applications current inhibited? The on-line service Persistent Object supported by the CCS (see Section 5.4.5.3) will be examined to determine the status of the network. Access will only be inhibited on permanent faults.

20.2.5.2 Confirmation Message Delivery

[C] messages include details of the outcome of any NBS transaction.

The FIs operate under the assumption that the transaction will have been successfully completed. Only the [C2] message can change that. It is therefore important that [C2] messages, indicating a different transaction outcome to the original request, reach the NBE in good time to enable it to issue an [E] (Reversal) message to the FI.

[C0] messages are written at the Outlet immediately the [A] is received, or when the wait for the [A] times out. If the connection was dialled, it will thus still be open at the time the [C0] was written, and hence the message will be immediately replicated to the Campus. It is harvested by the *NBS Expedited Confirmation Agent* and should arrive at the NBE within a few seconds of being written. Reasons that could prevent this immediate delivery of the [C2] messages include:

- Failure of the link to the Outlet (either at that point, or earlier such that the [R] was sent but the [A] was not received)
- Failure of the NBS Agent Server or NBS Authorisation Agent

To minimise the impact of a large number of lost [C2] messages it is vital that the infrastructure services that move [C]s between the various hosts (Riposte Message Service to Agent to NBE) are monitored for any failure, are recovered as soon as a failure is detected, where possible automatically.

The changes necessary to accomplish this are described in Section 5.7.

20.2.5.3 Reconciliation

The DRS application running on the Host Central Server carries out a number of activities:

- The receipt of NBS transaction from the various system that are to be reconciled
- The reconciliation process
- The generation of various reconciliation reports for Pathway Customer Services and PO Ltd

Each activity has its own service management requirements. These are described in Chapter 9

20.2.5.3.1 Transaction Gathering – Messages to be Reconciled

DRS receives data feeds from three sources:

- The message store
- The TPS host application
- The NBE

Long-term failure of any of these data feeds will result in a large number of reconciliation incidents being raised. All components involved in the transfer of these messages should be monitored to ensure they are running. In addition, various checks should be put in place to ensure each data flow is making the necessary progress to ensure the reconciliation process has time to complete within the timescales set by the various SLAs. It is envisaged the reconciliation process will need to be completed by 8:00 am, at which point the MSU will act on the reports generated.

20.2.5.1.2 The Reconciliation Process

A number of tasks will make up the reconciliation process; all must be monitored for both failure and lack of progress, alerts being raised in either case. Once an alert is raised, the relevant support unit should be called out to investigate and rectify any faults, ensuring the processes complete in time so as not to cause a breach in service levels agreements.

20.2.5.1.3 Report Generation and Delivery

Reports are generated for both PO Ltd and the MSU. Ltd reports will be delivered to the PO Ltd TIP Remote Gateway. MSU reports will be delivered to a location can be accessed from CS PCs in Bracknell. The progress of the delivery of reports should be monitored, with alerts being raised if progress is delayed such that service levels may be breached.

20.2.6 Risks and Issues

Failure to implement the developments defined in this Section will results in:

- Over loading of the HSHD during central systems failures. This will result in the breach of SLAs as well as portraying a poor system image to the Counter Clerks
- The inability to measure the QoS provided by the network supplier
- Failure to meet the PO Ltd requirement to inhibit access to the NBA during Outlet to Campus communications failures
- Failure, by 2nd line support, to notice central systems failure, which will cause loss of service to a large proportion of the Outlet estate, within a timely manner, therefore causing SLA breaches and portraying a general poor system image to Counter Clerks

20.3 FIRST LINE SUPPORT

First line support covers the support services provided by the Horizon System Help Desk (HSHD) [NBR046, NBR248, NBR452, NBR545]

- Level 1 (Advice & Guidance) calls [NBR047]
- Level 2 (Training) calls

The introduction of NBS will cause a change to both the number of calls from the Postmasters, and the priority of the calls, regarding lack of NBS at the Outlets. Calls could concern the failure of a single Outlet, or multiple Outlets where there is a failure in the Horizon Campus or the NBE.

To an individual Postmaster and to Customers in the Outlet, the importance and impact of both of these is the same – no NBS. The impact on the HSHD is quite different. The changes to the service provided by the HSHD must be focussed on ensuring that the service is:

- Re-instated as soon as possible and
- The Postmaster is informed (where possible) how long the service will be unavailable.

As described above, the Counter Clerk will be informed via an on-screen display when the NBS is not available at that Counter. In addition, new facilities will be introduced to monitor the failures of the NBS within an Outlet and report failures to the Counter clerk. Both of these should have the impact of avoiding a large number of calls to the HSHD.

However, any failure in an on-line service with no fallback will cause an increase in Help Desk calls. Postmasters will be unable pay any benefits whilst access to the service is denied. Certain failure scenarios can result in loss of service to a significant proportion of the Horizon network, for example failure of the NBE will result in loss of service to all Counters. Between 09:00 and 10:00 Monday to Thursday, it is estimated that all open Outlets will attempt to use the NBS at least once.

If all Postmasters affected by a NBE failure lasting five minutes were to phone the HSHD, then it would be overloaded trying to answer calls from a large proportion of the estate as can be seen in the graph below:

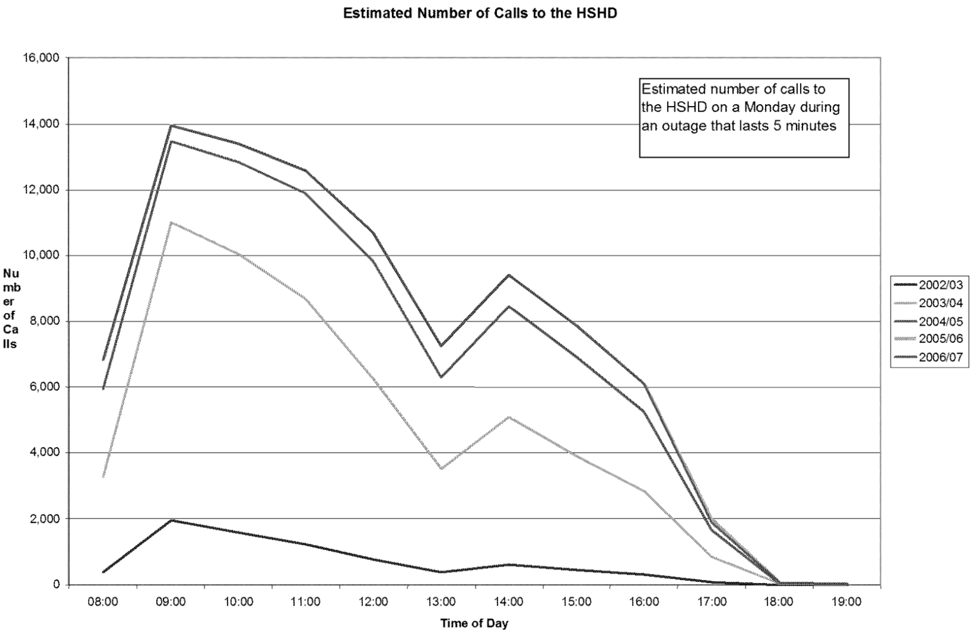


Figure 45 – Frequency of Help Desk Calls

Postmasters are currently not adversely affected when a central component fails. The only on-line service offered by Horizon is OBCS foreign encashments, and failure of these is supported by a fall back process that does not normally require a call to the Help Desk. OBCS foreign encashments are only used when a claimant uses an Outlet they have not been to before. They are also discouraged by Business Rules restricting the number that can be carried out in a year.

20.4 SECOND LINE SUPPORT

Second line support covers the support services provided by:

- Hit Teams
- SMC

Second line support handles calls that are not Level 1 or Level 2.

For NBS the main difference will be:

- Most of the problems currently picked up by the 'Day D' team will be the subject of calls from the Postmaster because the NBS is not available at that Outlet
- There will be more higher priority calls associated with the NBS not being available at an Outlet
- The response provided by Pathway will have to be in-line with the requirements of an on-line service, in particular the process for identifying and rectifying faults related to the Gateway PC or the Outlet to Campus network will have to be more responsive
- New processes will be introduced for informing Postmasters when the NBS is available following a major outage i.e. a failure in the Pathway Campus or in the NBE that results in the NBS being unavailable in a significant number of Outlets. This process will use Message Broadcast functionality (see Section 20.2.5.1.2.5). Standard (pre-formatted) messages will be used whenever possible and the messages will be sent to a standard set of Outlets depending on which platform/component has failed.
- SLAs covering the availability and response time for the end-to-end NBS will be introduced (see also [SRS] chapter 7).
- Selected SMC staff are provided with the ability to conduct remote support activities on Counter PCs using the Campus-to-Outlet ISDN lines. Such activity is only conducted for legitimate maintenance and diagnostic functions for the duration of the intended purpose. The link to the Outlet is protected by VPN. [NBR572]

20.5 THIRD LINE SUPPORT

Third line support covers the support services provided by the third line support team

Third line support handles calls that cannot be resolved by first or second line support.

For NBS, the main difference will be:

- There will be more high priority calls associated with NBS not being available at an Outlet that have not been either solved by second line or transferred elsewhere.
- The response provided by Pathway will have to be in-line with the requirement of an on-line service.

New processes and tools will be introduced to fulfil the additional security and auditability requirements of supporting NBS e.g. access to Counters will be via a terminal server type interface supported by the new Support Terminal Servers.

Third line, as the leading support unit, has additional responsibilities to produce support documentation and training for the other support units including *Field Service Managers* FSMs).

20.1.1 Capacity Management Service

An outline of the proposed Capacity Management Service (CMS) is included in Section 15.2.2. This would be an additional service to that provided for Horizon and therefore would be chargeable to PO Ltd.

Chapter 21 - Conformance to Requirements

21.1 SOR General Requirements

This Section provides a table that includes cross-references between the PO Ltd requirements as defined in [SOR] and modified by Pathway comments, and the outline solution described in this SDS. It omits requirements that are specifically stated in [SRS] to be Excluded.

In the table:

- Unshaded entries represent requirements for which Pathway is solely responsible
- Shaded entries represent requirements which Pathway shares responsibility with another party
- ESF indicates an Existing System Feature, which has been established and accepted at CSR+. [ESF] indicates Part ESF, in that this requirement is already partially covered by the existing system.

These are derived from the Versions of [SOR], as reflected in and with the Status as given in [SRS], specified in Section 0.3. The table will be updated if any later version of [SOR] is agreed and baselined between Pathway and PO Ltd.

NBR	Particulars	Status	Location
NBR001	The following transactions shall be initiated at the Counter by presentation of a magnetic stripe Token within Serve Customer mode 1) Cash Withdrawal 2) Withdraw all funds 3) Balance Enquiry 4) Cash Withdrawal With Balance 5) Cash Deposit 6) Change of PIN The magnetic token is not required to initiate the following transactions 7) Account Opening 8) Customer Enquiries 9) Customer Complaints *Pathway Comment: "Withdraw all funds" is now called "Withdraw Limit". This applies throughout the Document*	Yes Transactions 7, 8 and 9 are outside Horizon system.	3.2, 6.3.2.1
NBR002	For Clients utilising a direct interface from the NBE, the service shall support On-line Cash Deposit transactions for which no verification is required	Yes	3.2, 3.3.2.2.1, 3.3.3
NBR003	The service shall support On-line Cash Withdrawal transactions	Yes	3.2, 3.3.2.2.1
NBR004	The service shall support On-line Balance Enquiry transactions	Yes	3.2, 3.3.2.2.1
NBR006	The IIN (Issuer identifier number) recorded on the Token shall be used to determine the transactions supported for that Token	Yes	8.7.1.3, 6.3.2.1
NBR007	The Counter application will check that the IIN is supported, "from date" is valid (if applicable), "expiry date" is valid (if applicable) and LUHN on PAN is valid and will accept or reject the Token, and prompt the Clerk to advise the customer that it has been rejected *Pathway Comment: Issue Number will also be checked if applicable*	Yes	6.3.2.2
NBR008	The Counter application will allow clerk to decline the transaction (e.g.	Yes	6.3.2.4.1,

	suspicious circumstances) once it has commenced e.g. once the Request [R] has been issued. If the Clerk declines to undertake the transaction, and no Request [R] is issued, there is no record of an attempted transaction. If an [R] request has been issued, a response code will be captured within the [C] confirmation, indicating why the transaction has been declined. This will not be displayed to the clerk.		
NBR009	The Counter application will always seek to go on-line when processing an NBS transaction.	Yes	6.3.2.5
NBR010	The Counter application shall only proceed where positive authorisation is given by the on-line connection to the Client bank and by the clerk I.e. a visual manual check will be undertaken before going On-line for authorisation	Yes	6.3.2.5, 6.3.2.7
NBR011	The Counter application shall not support Off-line working. i.e. the Counter application must receive an [A] authorisation before continuing with the transaction.	Yes	3.3.3
NBR012	The Counter application shall not support fallback working, i.e. fallback is where an attempt to go on-line is made and if this fails revert to local processing.	Yes	3.3.3
NBR013	The system shall recover transactions lost through a Counter system failure Pathway Comment: Recovery process is documented in [CNTRDLG]	Yes	3.4.4, 5.4.3.4
NBR014	The Clerk may be requested to retain the Token by the Client Bank, and indicate if they have complied, as part of the [C] confirmation.	Yes	3.3.2.3.3, 6.3.2.2
NBR016	All transactions must be fully auditable, including abandoned transactions (I.e. after a [R] Request has been generated) Pathway Comment: Recovery process is documented in [CNTRDLG]	Yes [ESF]	13.2.3.1, 13.5.1.1, 13.5.1.2, 13.5.2.1
NBR017	The value and volume of withdrawals, deposits and balance enquiries must be reflected in the Cash Account. *Pathway Comment: See* NBR018 & NBR464	Yes	3.4.1.10, 5.4.4.1.1
NBR018	NBS transactions map to a Product, dependent upon the IIN and the transaction type, and will be mapped to the appropriate Cash Account line as defined in Reference Data *Pathway Comment: See* NBR017 & NBR464	Yes	3.4.1.10, 5.4.4.1.4
NBR019	Any one Token may be keyed or swiped multiple times within a Horizon customer session	Yes	6.3.2.1
NBR020	The system shall support the RAC (Request, Authorisation, Confirmation) model of End to End transaction flows	Yes	3.3.2.2, 0
NBR021	The Confirmation [C] message generated at the end of a customer session may be replicated in the normal Horizon fashion. (i.e. the [C] message can be transmitted along with other EPOSS transactions in the next scheduled replication.)	Yes	3.3.2.2.2, 5.4.5.3
NBR022	The NBS Application shall use WebRiposte *Pathway Comment: Pathway understands that the obligation to use WebRiposte ha been removed. If WebRiposte is used, this will only be to use the uprated Message Server. No new facilities will be used.*	Yes[49]	4.2.2, 5.2, 5.4 passim
NBR023	NBS transactions at the Counter shall be generic and shall be driven by Reference Data (i.e. the Counter application is Client-independent with the context being set by the IIN and NBE routing ID) *Pathway Comment: [SRS] qualifies this: "NBE will convert communication dialogues with individual banking clients into single set of transactions, which will support Counter dialogues with all banking clients*	Yes	3.2, 5.4.2.1
NBR024	New Clients will be treated as an extension to the range of Tokens supported at the Counter i.e. new IIN specific Reference Data may be for either an existing Client or a new Client	Yes[50]	3.4.1.6, 8.7.1.3

[49] *This will exclude web-based services, and the associated WebRiposte Framework and Asset Manager products*

[50] *Within the operational constraints of settlement/reconciliation reporting processing schedules within the DRS*

	Where a new Client is supported by an existing interface this shall be the only system data change required. Where a new interface is required, then data to map the IIN to the NBE routing identifier shall also be required, and may be done via a change to the NBE interface to state the newly supported value of the NBE routing identifier.		
NBR025	The Operational Business Change (OBC) will be used to introduce changes to NBS as required through Post Office Reference Data	Yes	8.1
NBR026	Pathway shall update Process & Procedure Documents	Yes [ESF]	17.3, 17.9
NBR028	The Counter application shall conform to the Horizon Style Guide. This must also be support via an integrated context sensitive help facility on data entry fields at key points in the transaction.	Yes	6.2, 6.3.1
NBR029	Counter Receipts will be generic across banking Clients *Pathway Comment: Receipt layouts are documented in [REPREC]*	Yes	6.3.2.9
NBR030	Receipts will always be given to customer for all completed NBS transactions, (i.e. for both accepted and denied transactions) The information to be displayed on receipts will be fully defined in the Pathway Reports & Receipts document. NOTE: Transaction times will be displayed in 'HH:MM:SS' format *Pathway Comment: Office Receipts will only be printed for Cash Withdrawal Transactions where it has been approved and there is no Clerk or Customer Decline. Office Receipts will not be printed for PIN Transactions and Declined Transactions. Customer Receipts are printed for Transactions that have not been abandoned.*	Yes[51]	6.3.2.9
NBR031	The system shall support standard agreed messages from the Client within the prescribed format for printing on Counter Receipts *Pathway Comment: Message to be printed on Receipts depending on the NBE Response Code will be documented in [REPREC]*	Yes[52]	6.3.2.9
NBR032	Pathway shall update the Horizon OPS Reports and Receipts Functional Specification *Pathway Comment: Layout of receipts to be documented in [*REPREC*] and contain a heading, title, location of terminal, Client name, masked PAN [*NBR539*], expiry date, token type, IIN, swipe details, value of transaction, FAD code, CAP, balance period, stock unit, date and time (hh:mm:ss format* – NBR031*), session identifier, free text space, outcome message, balance after a successful withdrawal. See* NBR536.	Yes[53] [ESF]	6.3.2.9, 17.3
NBR033	The Counter shall support the presence of Reference Data at the Counters to minimise on-line call connections (e.g. local validation)	Yes[54]	6.3.2.2
NBR035	On start up, each Outlet node will check for consistency & prompt for any unknown outcomes of withdrawal and deposit transactions, i.e. Request [R] no Confirmation [C]. E.g. Following a system failure, on re-start the system shall determine if there are any deposit or withdrawal requests [R] with no matching confirmations[C], the Clerk must be prompted to define the outcome – did the transaction complete or not – and this will be recorded in a recovery [C] message. *Pathway Comment: As per recovery model documented in [CNTRDLG]*	Yes	3.4.4, 5.4.3.4
NBR036	NBS transactions shall be supported at resilient Data Centres, e.g. for Pathway, the current Campuses at Wigan and Bootle.	Yes ESF	14.3.2
NBR037	Each system and interface shall provide robust Back-up & Recovery processes and procedures	Yes[55]	3.4.4, 17.4

[51] *PPDs will include appropriate procedures.*

[52] *Pathway will support the transfer of such receipt text from NBE to Counter application*

[53] *Dependencies on IBM and PO Ltd*

[54] *Pathway will distribute the Reference Data and make it accessible to the Counter application*

[55] *For those interfaces under Pathway control*

	The processes for each interface will be defined within the relevant AIS and TIS		
NBR038	The Request [R] & Authorisation [A] messages shall be supported in real time (i.e. via an immediate on-line connection)	Yes	3.3.2.2.2, 0
NBR040	An End to End (E2E) Reconciliation function is to be provided	Yes	3.3.2.4, Chapter 9 passim
NBR041	End to End (E2E) Reconciliation procedures (i.e. definition of manual processes) are to be provided	Yes	17.8
NBR042	At any reconciliation point, all reconciliation exceptions are to be highlighted and resolved	Yes	9.5.1.2
NBR045	Pathway to enhance the current interface to RDS to support NBS transactions. The current TIS and AIS will be updated to reflect the enhancements	Yes	8.7.1.2, 17.3
NBR046	Horizon System Help Desk (HSHD) to support NBS (excludes customer queries and Token management) *Pathway Comment: HSHD not required to provide advice on NBS usage at Counter. Advice limited to menu navigation only*	Yes [ESF]	20.2.6
NBR047	Pathway HSHD to provide 1st line support for NBA Service for Horizon originated calls, with handover to NBE support functions as appropriate.	Yes	20.2.6
NBR048	Each domain will have its own System Management Service to support NBS. Where domains interact, a Service Management process will be defined. *Pathway Comment: System management service, process and scope needs to be defined where Pathway domain interacts with PO systems and NBE.*	Yes [ESF]	Chapter 12
NBR049	Pathway to enhance Software distribution facility to support NBS (to enable controlled targeted release). (Note that this could enable pilot operation)	Yes[56] [ESF]	No enhancements required
NBR050	Pathway to agree TMS/NBE interface with NBE supplier and PO Ltd. This will be detailed in both an AIS and TIS *Pathway Comment: See [*NBEAIS*] and [*NBETIS*]*	Yes	3.4.1.9, 17.4
NBR051	MIS to support SLA monitoring, charging and trend analysis is required	Yes[57]	5.11
NBR053	NBS shall be available at all Counter positions as specified by PO Ltd, subject to limits set in [CA] Schedule A12. On-line availability of the NBA service at Outlets shall be: * Outlets with Dial Up communications links – 97% (e.g. Outlets served by ISDN) * Outlets with Fixed communications lines – 99.5% (e.g. satellite links) These times shall be calculated as monthly averages for the periods an Outlet is open within the PO Ltd Core Day. Agreed maintenance activities on the system and failures of elements that fall outside of Pathway's remit shall not count towards downtime calculations.	Discuss – subject to resolution of communications infrastructure [58]	14.3.1
NBR054	The Time to Repair failures shall be in line with [CA] Schedule G10 for those elements of NBS that fall wholly within Pathway's remit.	Yes	20.1
NBR055	On-Line Performance: 100% of each Request/Authorisation communication within the Pathway domain shall take no more than 4 seconds. This shall be measured on a daily average per Outlet basis. NB: 'daily average' needs to be confirmed by Network Banking Business Unit	No To be discussed in context of communications	

[56] *Software distribution to Outlets*

[57] *If such MIS includes information originating outside the Horizon domain, Pathway is dependent upon the third party for the provision of such information and an appropriate interface will require to be defined and supported by the third party.*

[58] *Action taken at Commercial Meeting with Keith Baines 20/6/01, to be resolved as part of the overall decisions on communications infrastructure. (See NBR055, NBR057, NBR259, NBR459)*

[59] *Action taken at Commercial Meeting with Keith Baines 20/6/01, to be resolved as part of the overall decisions on communications infrastructure. (See NBR055, NBR057, NBR259, NBR459)*

	Pathway Comments: *1) Pathway will not accept an SLA requiring 100% achievement; Pathway believes any SLA must recognise the distribution of response times and is willing to discuss achievement on this basis (as per industry standard) against the 95% target originally required. This is subject to commercial discussions.* *2) The issue of response times within the Pathway domain is subject to discussions on the communications infrastructure, and Pathway is not willing to discuss response times faster than the original 5 seconds target.* *3) Pathway does not accept that measurements should be based on a daily average per Outlet basis, which will add substantially to the reporting overheads and costs. An average monthly report for the live estate is proposed (see also* NBR053*).*	infrastructure[59] and commercial review	
NBR057	The E2E service must support projected workload volumes (including peak throughputs). *Pathway Comment: Pathway shall comply with this for those aspects of the E2E service under its control. See* NBR053	Discuss – subject to resolution of communications infrastructure [60]	2.4, 4.2.4, 13.5.4.1, 13.5.4.2, 13.5.4.3, 13.5.4.4
NBR059	Suppliers shall demonstrate that all requirements within their domain are met, by meeting agreed acceptance criteria *Pathway Comment: See* NBR259	Yes – subject to Acceptance Criteria being developed and agreed[61]	13.2.4.1, 18.2.1
NBR060	Service Level Agreements (SLAs) – to be defined.	A2A	
NBR061	Suppliers shall comply with the requirements of the Data Protection Act (DPA). 8 principles must be adhered to: - Fair & lawful processing - Limitation of use - Adequate & relevant - Accurate - Not kept longer than is necessary - Processed in accordance with the individual's rights - Secure - Not transferred to countries outside Europe without adequate protection i.e. If information is to be transferred to a country outside the EEA (European Economic Area) a contract may need to be in place so that sufficient guarantees can be obtained from the recipient in the country of destination concerning the security of the information and the data subject's rights. If the project does not comply with the above principles then it is mandatory to "Notify" the Office of the Data Protection Commissioner (ODPC).	Yes[62]	6.3.2.14.1, 13.2.1, 13.4.2.1.2
NBR062	Suppliers shall carry out an approved testing strategy comprising Component testing, Volume testing, Disaster Recovery testing and End to End (E2E) testing before NBS is implemented and participate in joint testing as directed by PO Ltd *Pathway Comment: Note that Pathway covers testing process in greater detail*	Yes	18.1

[59] *Action taken at Commercial Meeting with Keith Baines 20/6/01, to be resolved as part of the overall decisions on communications infrastructure. (See NBR055, NBR057, NBR259, NBR459)*

[60] *Pathway will comply with this for those aspects of the E2E service under its control*

[61] *Note that some requirements do not clearly delineate the specific requirements within each domain and therefore as currently documented cannot be the subject of acceptance criteria*

[62] *Pathway will only operate as a data processor*

	future development if required		
NBR066	Pathway will provide and install PIN Pads in line with the PIN Pad service definition supplied by PO Ltd	Yes	6.2
NBR070	Session Mobility is only possible once the NBS dialogue has been completed. I.e. once the [C] Confirmation has been written to the transaction stack	Yes	5.4.3.1
NBR072	Forced End Session – and other similar system behaviours, must not compromise the integrity of the RAC model. E.g. in the event of there having been an [R] generated, but no matching [C], a forced end session at the Counter must not breach integrity by orphaning the [R] with no corresponding [C]	Yes	3.4.1.12, 5.4.3.3
NBR149	Compliance with the Welsh Language Act will be via Reference Data for Outlet specific receipt header and footers, and by the Banks complying in the free text that they deliver for printing	Yes[64] [ESF]	5.4.4.1.3, 6.3.1, 6.3.2.9, 7.3.2.1
NBR150	The system will provide advice to the Clerk to communicate to the customer regarding fee charges from the Bank. The customer may then elect to abort the transaction without incurring any customer fees, or accept the transaction with the customer fees	Yes[65]	6.3.2.12
NBR151	Each transaction is separate, i.e. if a customer wishes to perform a withdrawal and a deposit, this would be via two transactions with no system relationship between them.	Yes	6.3
NBR153	The system must be capable of transacting business in Euros. *Pathway Comment: See Change Request 130, concerned with impact of Euro on existing Horizon system. PO Ltd needs to carry out a gap analysis against the banks' requirements. See also* NBR399.	Partial	3.4.1.7
NBR155	In the event of printer failure, a screen 'print preview' to support manual transcription is required. The screen preview must incorporate all details on the receipt, including the balance.	Yes	5.4.2.2.3
NBR156	It is a system decision on pay/no pay based on the authorisation from the Bank, this will not be locally adjustable, i.e. there will be no Supervisor Card override facilities.	Yes	6.3.2.5
NBR157	The receipt date and time stamp will be based on the local time at the terminal. This will be carried through any dialogue with the customer and Bank to ensure consistency. The underlying system will be based on Universal Time (UCT).	Yes [ESF]	6.3.2.9
NBR158	Transactions will be uniquely numbered as generated by the Counter application, however, these numbers will not necessarily be incremented by one each time *Pathway comment: Pathway will use a mixture of numeric and non-numeric (printable) characters*	Yes [ESF]	3.4.1.8
NBR159	The Human Computer Interface for NBS is identical to the existing Horizon application. Reporting of financial information remains the same. Customer facing HCI elements for the PIN Pad must be included in [STYLE] *Pathway Comment: [*STYLE*] will be updated to reflect the use of PIN Pads*	Yes	3.3.2.4.1, 5.4.4.1.4, 6.2, 6.3.1
NBR161	If the Counter application determines that the card is valid, it will then prompt the Clerk to perform APACS40 standard checks.	Yes[66]	6.3.2.2, 8.7.1.2.7

[63] *Pathway cannot commit to supporting future Smart Card applications until the application requirements and the Smart Card characteristics have been defined*

[64] *Pathway are required to distribute and maintain the Reference Data and provide an interface to the Counter application which will enable identification by the application that the Outlet is subject to the requirements of the Welsh language act and to support Outlet specific language variants (Welsh/English&Welsh) for headers and footers*

[65] *Pathway will support conveyance of appropriate message information between the NBE interface and the Counter application.*

[66] *Such checks need to be taken account in establishing SLAs. PO Ltd will define the checks (clarification by Keith Baines at draft schedule review, 17/10/2001)*

	Pathway Comment: PO Ltd state that the checks will not be APACS, but will be referred to as something specific to PO Ltd (title to be confirmed, in the meantime referred to as "agreed checks")		
NBR164	Where a token cannot be read electronically, the Counter application shall support manual keying of information held on the front of the card. The Clerk enters the PAN (the large digits across the centre of the token); The system matches the PAN with Reference Data held patterns to identify other fields that need to be manually input, e.g. expiry date, and other fields that must be validated NB: It may be that Reference Data identifies that 'keyed entry' is not permitted for a particular range of tokens and the Clerk needs to be advised and print details onto the receipt to this effect for the customer to take up with the issuer of the token.	Yes Not system action – Clerk must manually write on receipt	6.3.2.1, 6.3.2.2
NBR166	Multiples, minimums and maximums transaction values can be enforced by the system. Multiple and minimum transaction limits will not apply to 'Withdraw Limit' functionality	Yes[67]	6.3.2.2
NBR167	The Clerk may abandon the transaction at any point prior to generating a Request. No permanent record of such abandons is required. *Pathway Comments: Same as second part of* NBR008	Yes	6.3.2.4.1, 6.3.2.7
NBR168	Reference Data will hold details of minimum, maximum and multiple amounts against each product. Multiple and minimum transaction limits will not apply to 'Universal Banking Withdraw All' functionality however the maximum limit applied at the Outlet will be advisory, and the Bank may, or may not, utilise this parameter. *Pathway Comment: See* NBR430.	Yes	6.3.2.2
NBR173	Signature verification will take place after the Authorisation is received for withdrawals. The result of the signature verification will be captured in the [C] confirmation message.	Yes[68]	6.3.2.4.1
NBR176	Following a system failure, on re-start where the system determines there is a balance enquiry request [R] with no matching confirmation [C], it will automatically generate an 'assumed completed [C]'	Yes	3.4.4, 5.4.3.4
NBR180	All Requests [R]s and Confirmations [C]s will be presented to the NBE once, and only once for onward transmission to the Bank	Yes[69]	3.3.4.2, 5.7.4
NBR182	The Confirmation [C] will form part of the associated EPOSS transaction, i.e. a single message will be recorded at the Outlet	Yes[70]	3.4.1.10, 0, 5.4.4.1.1, 0
NBR202	Existing physical interfaces from RDS to TIP and the Horizon Campus will be used to transmit and receive Post Office Reference Data updates The TIS shall remain the same, however capacity may increase.	Yes ESF	8.4.1, 8.8.1.2, 13.5.2.3
NBR212	The Pathway Campus required to reconcile banking transactions processed [C4] by the NBE against banking transactions [C1] recorded on EPOSS and report any exceptions *Pathway Comment: See* NBR294 *and* NBR389	Yes	9.3.1.2
NBR219	Response message from LINK or partner Banks will need to be converted by the NBE to a format acceptable to Pathway	Dependency on NBE	5.4.2.2.3, 6.3.2.11
NBR221	There is a requirement for the Outlet node to store a 'Maximum System Wait Period' against each Client. This period, set in milliseconds, would prevent the Counter sitting idle if the banking request or authorisation is not received within acceptable timescales.	Partial[71]	6.3.2.5
NBR227	Internal system processes must ensure that all data successfully	Yes	9.3.1.3 et seq

[67] *Pathway will distribute via Reference Data and make it available to the Counter application*

[68] *Counter procedures will document this*

[69] *Except in exceptional circumstances; "stale" [R1]s will not be presented. See also NBR227*

[70] *A single **logical** message - in exceptional circumstances there may be two physical messages (e.g. when 2 Kb message limit broken)*

[71] *A global "Maximum System Wait Time" will be supported, common to all FIs*

	delivered is successfully processed, with any errors identified and reported. *Pathway Comment: Ensure all data received is processed by checking for complete Confirmation sets. Pathway to receive data from NBE for [R]s without matching [C]s. All errors except one will be identified by the two checks ([R] at Counter not reaching NBE and not resulting in null due to system failure).*		
NBR228	Data Integrity must be assured across all interfaces, both internal to the Post Office and external to the Post Office. Reconciliation processes must cater for error situations across all interfaces, e.g. rejected and re-sent files.	Yes [ESF]	13.4.2.2.1
NBR229	Reconciliation of all data flows, where the same data is passed to more than one place, e.g. from the Campus to NBE and TIP and report any differences.	Yes	9.3.1.3 et seq
NBR230	Reconcile the volume and value passed to TIP on the Cash Account to the volumes and values settled with the Client for each Cash Account week as defined in Reference Data. Report any differences, I.e. Cash Account not delivered to TIP, transactions on Cash Account not included in settlement and transactions settled not on Cash Account.	Yes	9.3.2.2.2
NBR232	There must be clear and unambiguous processes and procedures to support NBS Transactions. *Pathway Comment: See* NBR275	PO Ltd	n/a
NBR235	The service for all Clients is available across the Network, i.e. All the Horizon enabled Outlets are allowed to conduct Banking transactions	Yes [ESF]	8.7.1.3
NBR236	Following on-line failure, the Clerk must be advised that on-line connectivity is now available to avoid constant attempts to determine if service is back up and operational. I.e. once a 'system unavailable' message is received, the Clerk may not attempt any further NBS transactions, therefore positive notification is required. *Pathway Comment: Subject to discussions and Off-line Indicator documented in [CNTRDLG]*	Yes but notification will not be immediate	5.4.5.3, 5.4.5.4, 20.2.5.1, 20.2.5.1.1.3
NBR237	A signature slip must be produced on the Horizon tally-roll, to enable comparison of the customer signature for a balance enquiry. This signature slip must be destroyed once the comparison is made. The signature slip must only contain a subset of the key fields on the receipt so that a transaction could not be generated from the signature slip.	Yes	6.3.2.9
NBR238	For withdrawal transactions, the printed receipt must be printed twice to allow a signed copy to be retained within the Outlet and a second copy passed to the customer *Pathway Comment: An Office Receipt will only be produced for Cash Withdrawal Transactions where verification is by signature – or as set out in [CNTRDLG]*	Yes	6.3.2.9
NBR239	Every transaction must be identifiable to an individual user and stock unit (i.e. the physical compartment containing stock) within an Outlet	Yes	6.3.2.5
NBR240	The Counter application must identify that a transaction cannot be completed at the earliest possible stage, to avoid abortive activity. In particular, a transaction whose failure can be predicted without involving on-line activity must be failed immediately – e.g. if the product is not supported at that office or if a card has passed its expiry date *Pathway Comment: As set out in [CNTRDLG]*	Yes, subject to system constraints	6.3.2.2
NBR245	On-line banking deposits, withdrawals and balance enquiries must be available at Outlets 24 hours per day, 7 days per week every day of the year Clarification: The requirement is for the NBE to have a service availability of 99.985% 24 hours per day, 7 days per week. However the majority of transactions are expected to occur between 08:00-20:00 and outside of these hours the NBE must be able to handle a reduced volume (expected to be in the region of transaction full load of 40	Partial[72] ESF	11.5.4.5

[72] *Pathway cannot support the Service during periods of scheduled maintenance, such as the nightly period for software and Reference Data download, lasting typically half an hour.*

	Outlets.) *Pathway Comment: Pathway does not find this Requirement acceptable in the form stated, because NBS at the Counters is dependent upon EPOSS. Schedule F01 (para. 2.3) and Schedule F08 (para. 1.2) of [CA] express this EPOSS requirement in the form "The Contractor shall provide EPOSS at all Outlets for all the hours that they are open for business". Pathway believes this form of words for NBS meets PO Ltd's requirements and is acceptable to Pathway, subject to periods of scheduled maintenance*		
NBR248	Helpdesk processes (NBSC and HSHD) and procedures must be in place to support the Counter Clerk in support of the banking product.	Yes (HSHD)	20.3
NBR250	The method of Customer verification shall either be based on: * None - No customer verification required * Signature – i.e. the Clerk will be required to verify the customer via a signature check against the card * PIN – i.e. the Clerk will request the Customer to enter their PIN, which will be verified outside of the Pathway domain * PIN falling back to signature – where PIN will be used if a PIN Pad is available to the Counter (i.e. installed, powered, connected and working), otherwise the transaction will proceed as a signature based transaction For the avoidance of doubt, the fallback from PIN to signature will not require any additional action from the Clerk or Customer. It is a system decision such that – other then by disrupting an installed PIN Pad – there is no user selection of signature in place of PIN, where for example, a PIN has been forgotten. The method of Customer verification will be controlled by Reference Data and will be able to be separately set for each transaction type for each IIN *Pathway Comment: Pathway will assume "available" to mean "installed". PIN Pads have a long MTBF and will be replaced when faulty. It is not possible to detect differences between devices switched off deliberately (fraud risk) and not working. See also* PPR014	Partial[73]	6.3.2.4 et seq
NBR251	The system must prompt the Counter Clerk to confirm that the customer's signature is correct. If the signature is incorrect then the system must prompt the Counter Clerk to do one or more of the following, dependant on Client requirements: * Decline the transaction and retain the card * Decline the transaction and return the card to the Customer	Yes	6.3.2.4.1
NBR252	The system must provide unambiguous instructions to the Counter Clerk to retain the card if the response from the Client requires such an action.	Yes – Dependency on NBE[74]	6.3.2.11
NBR254	All completed transactions must report to the common 'transaction stack' within EPOSS, contributing to the customer sessions total (including zero value banking transactions).	Yes [ESF]	5.4.4.1.1
NBR256	Reports required for internal office accounting must be capable of production from Horizon within the current reporting regime. The ability to produce Outlet reports must be produced from the single core data captured at the time of the Serve Customer transaction. The ability to produce Outlet reports must not be dependent on availability of external systems. The following reports must be available: * Summary report by Client by Product * Transaction listing by Client by Product * Bundling summary report by Stock Unit by Product since last Transaction. Receipts may be utilised to support the balancing process if necessary *Pathway Comment: this has been clarified by Bob Booth in that all the*	Yes [ESF]	3.4.3, 0

[73] *Pathway will document Counter procedures*

[74] *Pathway will transfer such instructions from NBE to Counter application*

	reports are to be produced via the Counter printer, not the A4 printer		
NBR258	The volume and value recorded on the Cash Account shall include all transactions irrespective of outcome i.e. both successful and declined transactions will be recorded. Management information, by Outlet, product, outcome, Cash Account week is required to monitor the number of successful and declined transactions performed.	Yes	5.4.4.1.6, 5.11.1
NBR259	The system response time from the swipe of the card to the completion of the transaction must be consistent with banking standards. This is to ensure an acceptable customer experience. Clarification: The Post Office requirement is that the transaction time from swiping the card to completion of the transaction should be no more than 45 seconds. *Pathway Comment: Pathway's obligations are covered in* NBR055 *and* NBR059	No[75]	
NBR260	Access to all transactions for 3 months at individual transaction level must be available at both the Campus and NBE, to support online error resolution within defined periods: as specified within [RECIM] (for Pathway) […]. Timescales, and the method of presentation, need to be jointly agreed and defined between Consignia and Pathway/IBM. Three types of query are envisaged are follows: (a) Simple dispute enquiries, which are defined to relate to contested transactions where no system malfunction occurs. These enquiries can be satisfied by interrogation of audit records from the NBE, with no interrogation of the Horizon audit records. The volume of such queries is assumed to be 9,000 queries per annum. (b) Dispute enquiries with system malfunction, which are defined to relate to contested transactions where a system malfunction may be involved, e.g. terminal failure causing the transaction completion message to be delayed or lost. These enquiries are satisfied by interrogation of some combination of the NBE, Horizon and reconciliation records from LINK. The volume of such queries is assumed to be 900 queries per annum. (c) Prosecution support enquiries, which are defined as queries in support of criminal prosecution or civil litigation. These enquiries are satisfied by interrogation of some combination of the NBE, Horizon and reconciliation records from LINK. In addition, interrogation of supplier fault and help desk logs is required. The volume of such queries is assumed to be 250 queries per annum. *Pathway Comment: See* NBR315. *Access is for Pathway internal staff. The period of access to all transactions shall be as specified within [RECIM]*	Yes – Discussion needed on projected volumetrics	3.4.1.2, 13.2.3.1, 13.5.3, 13.5.4.5, 13.5.4.6, 13.5.4.7, 13.5.4.8
NBR261	There must be access to a daily total volume and value of transactions by Client by product by agreed posting day to enable the production of monthly invoices. This needs to be able to separately identify successful, declined and failed transactions (e.g. Customer changed mind, Client decline, system failure or system timeout) *Pathway Comment: Totals are to be by "Product" as defined in [RDSAIS] (clarification by PO Ltd – review comments for version 0.10)*	Yes	3.4.1.10, 5.11.1
NBR263	A balance enquiry will result in a zero value transaction for which the Client must be charged (i.e. a zero value transaction will be transmitted to TIP in the existing EPOSS feed)	Yes	3.4.1.10, 6.3.2.7, 6.3.2.8
NBR268	Service Level Agreements will be supported by the production of management reports covering: * response times of banks and systems * availability of component systems * availability of banks systems (downtime) * Post Office systems response times *Pathway Comments: Service Management Reports to include*	Yes – Partial	5.11.1

[75] *To be shown as an Exclusion with the caveat that Pathway accepts responsibility for components within the Pathway domain.*

	information on availability of Pathway elements according to SLAs, response time of transactions within Pathway, problems resolved and outstanding. *MIS reports may be separately agreed which report E2E service monitoring*		
NBR269	Management Information will be available to support the level of multiple transactions (i.e. on the same IIN/PAN combination within a single day) conducted in order to identify possible misuse of the system.	Yes	5.11.1
NBR272	Horizon System Helpdesk (HSHD) will need training to deal with banking enquiries and the correct procedures to follow.	Yes [ESF]	19.4
NBR275	Processes and procedures will be produced to support the end to end service.. *Pathway Comment: See* NBR232	PO Ltd	n/a
NBR276	Contingency procedures are required to ensure that availability is maintained to the level agreed with FIs and integrity of all data is maintained to support reconciliation. *Pathway Comment: PO Ltd confirm there is no agreement with the banks at the present. Any such additional requirement will be subject to Change Control*	Yes[76] – Partial	Chapter 14
NBR277	The NBE will interpret, translate and switch messages between the Post Office (Horizon), LINK (as appropriate) and Banking Domains.	NBE	n/a
NBR278	The NBE will match transactions in the LINK LREC File and report on exceptions. *Pathway comment: Data will be received from NBE notifying detected exceptions in NBE, between NBE and Clients, between LINK and banks. DRS will receive data from NBE on [R]/[A]s with a different outcome from the [A] or any later [C0]. Unmatched [A]s will be added to Transaction State Table.*	Yes[77]	9.3.1.4
NBR285	The NBE and Campus domains will interact using an assured communications protocol / medium, allowing boundaries and responsibilities to be clearly demarked between the domains	Yes – subject to agreement on NBE/Horizon AIS[78]	3.3.4, 3.4.1.9, 10.7
NBR293	The NBE will report on variances and discrepancies in the LREC figures and those in the NBE's total and by FI view of transactions. This report will contain the LINK settlement Total, the NBE calculated total, and the individual transaction records where exceptions occur (no record of the txn in one of the files or no match).This report will be made available to the Client settlement team by 08:00 the next day	NBE[79]	n/a
NBR294	The NBE will provide the Horizon Campus with its view of the day's transactions (i.e. [C4]s and exceptions) for reconciliation purposes *Pathway Comment: See* NBR212 *and* NBR389	Yes – subject to agreement on NBE/Horizon AIS	9.3.1.2
NBR315	Access to archived transactions (i.e. over 3 months old but within 7 years) must be available within 24 hours of any request Three types of query are envisaged are follows: (a) Simple dispute enquiries, which are defined to relate to contested transactions where no system malfunction occurs. These enquiries can be satisfied by interrogation of audit records from the NBE, with no interrogation of the Horizon audit records. The volume of such queries is assumed to be 1,000 queries per annum.	Yes – Partial[80] Discussion needed on impact of volumetrics and retrieval times	13.2.3.1, 13.5.3, 13.5.4.5, 13.5.4.6, 13.5.4.7, 13.5.4.8

[76] *PO Ltd to review wording of Requirement with a view to removing "to the level agreed with FIs"*

[77] *Pathway will receive such exceptions as part of the feed to the DRS; other aspects of meeting this requirement rest with the NBE supplier*

[78] *Work in progress: PO Ltd/IBM*

[79] *Assuming this is a direct interface from NBE to PO Ltd Settlement; if this reporting is intended to form part of the DRS to PO Ltd Settlement reporting further discussion will be needed about presentation of this information across AIS Interface 3*

[80] *At meeting in London (31/7/01), requirement was clarified to mean archives had to be located in 24 hours, not necessarily loaded. [RECIM] to clarify action taken to different types of enquiry and target response times.*

	(b) Dispute enquiries with system malfunction, which are defined to relate to contested transactions where a system malfunction may be involved, e.g. terminal failure causing the transaction completion message to be delayed or lost. These enquiries are satisfied by interrogation of some combination of the NBE, Horizon and reconciliation records from LINK. The volume of such queries is assumed to be 100 queries per annum. (c) Prosecution support enquiries, which are defined as queries in support of criminal prosecution or civil litigation. These enquiries are satisfied by interrogation of some combination of the NBE, Horizon and reconciliation records from LINK. In addition, interrogation of supplier fault and help desk logs is required. The volume of such queries is assumed to be 750 queries per annum. *Pathway Comment: Pathway require PO Ltd to provide volumes and types of data required. See also* NBR260 *The archive may be located within 24 hours but not necessarily electronically loaded for access (clarification by PO Ltd at meeting in London 31/7/2001)*		
NBR324	The transaction receipt must be expandable to allow for the provision of mini-statement information *Pathway Comment: Clarified by Jeanette Brown at meeting in Chesterfield (22/06/2001) that mini-statements comprise (up to) the last 12 transactions*	Yes – subject to limitations of message length	4.3.1.1, 6.3.2.9
NBR329	Multiple tokens may be keyed or swiped within a single customer session	Yes	6.3
NBR337	Receipts are required for cards that have been retained *Pathway Comment: No Office Receipts for declined Transactions, but Customer Receipts will be printed a per [CNTRDLG]*	Yes	6.3.2.2
NBR389	The NBE will match transactions provided directly to Clients not supported by LINK, and report on exceptions. This report will be transferred to the Campus. Pathway will then report Client/NBE exceptions along with other exceptions *Pathway comment: See* NBR229 *and* NBR294	Yes	9.3.1.2
NBR394	The token used to initiate a banking transaction must conform to ISO 7810	Yes [ESF]	6.3.2.1
NBR395	The token used to initiate a banking transaction must conform to ISO 7811	Yes [ESF]	6.3.2.1
NBR396	The token used to initiate a banking transaction must conform to ISO 7812	Yes [ESF]	6.3.2.1
NBR397	The token used to Initiate a banking transaction must conform to ISO 7813	Yes [ESF]	6.3.2.1
NBR399	EURO: Counter transactions will be recorded in sterling only throughout transition and up to E-day, and in Euro only on and from E-day. E-day is assumed to be 21/02/2004. This must not preclude the ability to display dual prices, along with the ability to print receipts showing both prices including the Euro logo, during the run up to E-day nor the period of dual circulation (E-day to F-day), both of which will be required.[81] *Pathway Comment: See* NBR153	Yes – subject to Change Request 130 - EPOSS and other dependencies	3.4.1.7
NBR401	Post Office Reference Data shall identify what fields from a card front shall be keyed if the card is not swiped	PO Ltd/(Yes[82])	6.3.2.1
NBR403	Reference data shall identify the Card Issuer whose card is being processed.	PO Ltd/(Yes)	6.3.2.1
NBR404	Reference data shall identify whether transactions supported for the	PO Ltd/(Yes)	6.3.2.1

[81] *The Horizon system has the capability of displaying both Sterling and Euro symbols on the screen and tally roll printer. It is assumed the display of dual prices will be in the free text area only.*

[82] *Pathway will distribute and provide access to Reference Data for the Counter application. (This also applies to NBR403 –NBR406)*

	token are valid for swipe, manual key or keyed and swiped magnetic cards.		
NBR405	Reference data shall allow the swipe to be parsed to determine the relevant fields to be processed	PO Ltd/(Yes)	6.3.2.2
NBR406	Reference data shall identify the customer verification to be undertaken for each transaction type supported	PO Ltd/(Yes)	6.3.2.4
NBR407	Reference data shall be temporal i.e. have a commencement and expiry date to allow for pre-loading and cut over of data from one version to another.	PO Ltd/(Yes)	8.1
NBR410	Reference data shall contain future fields (or fields whose values may be set to further values at a later date) such as fees, alternate verification method etc. such that the interface shall not need retesting when these features are enabled. E.g. there will be a mix of agreed fields, some of which are 'not used at this release' and others that hold values that can be added to, such as verification method may be 0-signature, 1-PIN allowing 23 to be retina etc.	PO Ltd/(Yes)	
NBR411	Reference Data shall be clearly classified and able to be implemented within agreed periods at the Counter. The introduction of a new compliant IIN shall be done within two weeks. Within 4 working days the supplier shall have produced a verification report of the supplied data and a test report of an interaction to the LINK simulator. Within 4 further working days The Post Office shall authorise it (if acceptable). A change to data associated with an existing IIN shall be undertaken within 2 working days, with a change originating from OSG by 10:00, reaching RDS by 12:00 and Pathway by 16:00. By 09:00 the following day, OSG shall authorise for release. *Pathway Comment: These incidents will be dealt as OBC activities and will be applied in the same manner as currently being provided to Horizon with any specific associated NBS impact agreement arising out of operational practice and application.*	Yes – subject to OBC process being agreed	8.8.1, 16.2.2
NBR412	The addition of a Client with a new interface will be as agreed via change control for the development and test of the interface. National Roll-out must be complete by 25 October 2002. The service provided for the following FIs must be provided by the LINK interface to meet this deadline. - RBS/NatWest Group - HSBC - Nationwide - Co-op - Abbey National - Barclays - Lloyds TSB - NAG - Halifax/BoS The service provided for the following banks must be provided by the NBE direct interface to meet this deadline. - A&L *Pathway Comment: See Section 9.1 of [SRS]* *The date for migration of the Campuses, which is the key date prior to Pilots and then National roll out, is subject to Pathway completing the implementation planning phase following production of this SDS, and as such is "subject to discussion".*	Yes[83] Roll out timescales are subject to discussion	3.4.1.6, 19.2.1 et seq
NBR413	The supplier shall clearly state any constraints on the number of IINs	Yes[84] – subject	0

[83] *Mostly outside Pathway domain, except for reconciliation settlement reporting aspects*

[84] *To be considered for Reference Data and reconciliation/settlement reporting. Other aspects such as NBE support lie outside Pathway responsibilities*

	that may be supported, or the level at which system performance will be impacted. This shall be quantified and options for moving forward identified. *Pathway Comment: Pathway require indications of volumes from PO Ltd. See* NBR414	to joint design of Reference Data and feedback on volumes	
NBR414	The supplier shall suggest optimal strategies for initial take on of Clients that may be bulked to reduce time to market and increase accuracy of the offer. *Pathway Comment: Pathway require indications of volumes from PO Ltd. See* NBR413	Yes – subject to joint design of Reference Data and feedback on volumes	19.2.1.3
NBR415	The supplier shall categorise the changes required to their systems so that changes can be evaluated as the minimum that is required and where enhancements give other benefits. *Pathway Comment: This is handled through Commercial reviews*	No	
NBR416	Introduction of new cards shall be supported by updates to procedures in OBC as normal.	Yes[85] ESF	3.2, 8.8.1
NBR417	Reference Data shall be designed with the awareness that: * EFTPoS may use the same cards * Smart cards are likely to be introduced in the future (LINK mandate the use of Smart by 2005) Any developments must not preclude the introduction of these and must make re-use feasible.	PO Ltd/(Yes)	n/a
NBR418	Reference Data should be introduced to the NBE prior to implementation at the Counter. Similarly, when Reference Data expires, it should be ceased at the Counter before being ceased at the NBE. There should be an adequate Hygiene Period, to allow for full replication across the Counter estate.	PO Ltd/(Yes[86])	n/a
NBR423	The NBE will interpret Banks Response Codes into a usable format. *Pathway Comment: It appears from [*NBEAIS*] that the NBE is not interpreting the Response Code, in which case PO Ltd must provide Pathway with the appropriate business logic associated with each Response Code, together with the text to be displayed to the Clerk and, where appropriate, printed on the receipt and/or displayed on the PIN Pad. Receipts will be printed with text depending on NBE Response Codes as documented in [*CNTRDLG*]*	IBM/PO Ltd	3.4.1.3, 6.3.2.11
NBR429	Balance Provision with / without Withdrawal. For Universal Bank customers, the Counter Clerk shall have access to the following three transaction options on the front-end Counter system 1) WITHDRAWAL WITH BALANCE 2) WITHDRAWAL OF ENTIRE BALANCE WITH BALANCE REPORT 3) BALANCE ENQUIRY For all of the above transactions, the balance held on account after each transaction will be printed on the customer receipt only if: - the transaction is successful or - the transaction was refused due to insufficient funds Availability of transactions to each presented token will be determined by IIN, which will be maintained and provided by *PO Ltd* Reference Data.	Yes [87]	6.3.2.1, 6.3.2.9
NBR430	'Withdrawal of Entire Balance' means that no value is entered on Horizon by the Clerk. The amount of the withdrawal is to be returned by the Universal Bank, along with the remaining outstanding balance.	Yes[88]	6.3.2.2, 6.3.2.6

[85] *Subject to existing support for the type of Token at the Counter*

[86] *Pathway will not monitor the state of Reference Data on the NBE*

[87] *Pathway supports the transfer of transactions between Counter application and NBE, and access to the printer from the Counter application, but is only responsible for that part of the content generated within the Horizon Domain as agreed with PO Ltd, e.g. from Reference Data*

[88] *Pathway support the transfer of transactions between Counter application and NBE and access to the printer from the Counter application*

	For a withdrawal of an entire balance, the maximum amount that is permitted at the Outlet for the Universal Bank will be passed through to the NBE. If the outstanding balance exceeds this value, the transaction will be limited to this maximum. There is no requirement for this to be overridden, i.e. the customer cannot set up a special arrangement for a transaction maximum. *Pathway Comment: PO Ltd have renamed Transaction "Withdraw Limit"*		
NBR431	PIN functionality for the Universal Bank will be in line with that specified by the Network Banking Project *Pathway Comment: Withdraw Limit Transactions will be PIN based only, i.e. there will be no signature verification*	Yes[89]	6.3.2.1, 6.3.2.13
NBR432	Card Receipt functionality is required for Universal Bank transactions at NBS Release 1. Receipt of Card will be recorded at the Outlet by use of a zero value 'Automated Payment' type transaction fed back to the card supplier. This can be setup using the existing Horizon capabilities. This process is required for each card received and will utilise a barcode on the envelope containing the card. Card receipt volumes are not required to be recorded on the Cash Account	Yes – subject to clarification[90] ESF	6.3.2.14.1, 6.3.2.14.2
NBR434	The system should provide management information to support the monitoring of incidents of money laundering. The information will be produced monthly, by Outlet, for Deposit transactions over a pre determined – parameter driven amount.	Yes	5.11.1
NBR438	Input of NBS transaction data at the Counter should be by both touch screen and keyboard	Yes ESF	3.4.1.13, 6.2
NBR439	The system shall provide 'screen prompts' at appropriate stages of the transaction, e.g. obtain signature, to support/inform the Clerk in performing the NBS transactions. *Pathway: Discussion required with PO Ltd to establish Counter dialogues*	Yes	6.2
NBR441	An audit trail of all transactions and events (including abandoned ones) must be maintained. This has to be in conformance with Banking Standards, PO Ltd Information Security Policy and a Code of Practice for Post Office Information Security Systems.	Yes[91] ESF	13.2.3.1, 13.5.1.1, 13.5.1.2, 13.5.2.1
NBR442	Access must be provided to any additional material required to support the records e.g. premises, facilities, services, documentation, information (magnetic or otherwise), staff, procedures and timesheets and other data used directly as a basis for charging.	Yes ESF	n/a
NBR443	Data held in Outlets can be accessed to enable PO Ltd and Consignia audit requirements to be met. Also assistance has to be provided by Suppliers during the life of the contract and for 6 years afterwards to allow information to be accessed to fill obligations to supply information for parliamentary, judicial or administrative purposes	Partial[92] [93] ESF	13.2.3.1
NBR444	On notification of an audit reasonable access to the Audit Trail and the facility to interrogate the trail shall be supplied to the auditors	Partial[94] ESF	13.5.4.3
NBR445	The confidentiality, integrity, validity and completeness of data has to be maintained throughout e.g. storage, processes and transmissions, including during periods of service failure and recovery from service failure	Yes (security) ESF	13.2.3.1, 13.5.4.6
NBR446	In the case of any criminal investigations and prosecutions the Audit		

[89] *Pathway is dependent upon PO Ltd discussing Counter dialogue requirements*

[90] *There will be minimal development at the AP Host if an existing AIS on AP is used for card receipt (e.g. type 'G'), but significant development may be incurred if a new interface be written and proven.*

[91] *Excluding audit of NBE functions, which is the responsibility of the NBE supplier*

[92] *Discussion required on details of the processes to be adopted*

[93] *Provided NBS does not require any additional audit reports to be available at the Counter*

[94] *PO Ltd to clarify information retrieval requirements*

	Trail and other information required has to be retained for the duration of the investigation and prosecution. In addition information has to be in accordance with [PACE][95]		
NBR447	The transaction time at the Counter must be kept to a minimum subject to detail Clerk dialogue design. *Pathway Comment: Pathway only responsible for the elements developed by Pathway. This is a qualitative requirement and not measurable. Pathway does not accept it is solely responsible in view of PO Ltd's Counter dialogue and manual processes. The Counter dialogue will be agreed in* [CNTRDLG]*.*	Yes – but see NBR259	6.3.2.9
NBR448	The implementation of the banking product on the Horizon architecture must be seamlessly integrated and transparent to the user. It must not degrade any aspect of the existing service nor must it affect the availability and functionality of existing products. Note: Except for the rearrangement of the menu hierarchy to cater for the introduction of the banking solution.	Yes [ESF]	6.2. et seq
NBR449	All transactions must be conducted under a common Access Control regime; the user must not be required to log on to more than a single system and must only be required to use his/her Horizon UserID and password.	Yes [ESF]	6.3
NBR450	Customers must be presented with a seamless customer offer covering all the transactions available to them. The total banking service must be offered to the Customer in such a way that the benefits to the Client and its Customers are maximised.	Yes	3.4.1.13, 6.3.1
NBR451	The system must be designed to de-skill the banking transaction task through simplification and standardisation of all processes, thereby minimising the reliance on the skill and knowledge of the Counter Clerk. This must be achieved by leading the Counter Clerk through the transaction with prompts provided where appropriate, clear instructions where actions are required e.g. retain customer card and where a selection is necessary, only valid options must be presented. These prompts must be standard for all banks.	Yes – subject to dialogue design jointly with PO Ltd	3.4.1.13, 6.3.2 et seq
NBR452	Support for the banking product must be provided through the existing helpdesk setup. *Pathway Comment: Level 1 and Level 2 services to be provided by Pathway (existing helpdesk setup)*	Yes ESF	20.2.6
NBR453	All [audit] data must be recorded at source to ensure the integrity of the data.	Yes ESF	3.4.1.1, 13.5 et seq
NBR454	Existing processes within Horizon will ensure that all Banking Transactions will be successfully posted to the Cash Account	Yes	5.4.4.1.6
NBR455	Existing processes within Horizon will ensure that all transactions at the Outlet are successfully transferred to the Campus and delivered to TIP. *Pathway comment: [C]s are completed at Outlets, forwarded to PO Ltd TIP along with other standard EPOSS transactions in* [TIPAIS]*. Reconciliation and incident management will be identical to those currently adopted and defined in [CA] schedule G01 and* [TPSREC]	Yes	5.12.2
NBR456	Daily information by Client, Product and Posting Date shall be available to support settlement with Post Office Clients. This shall detail complete transactions, incomplete transactions and all unreconciled items	Yes[97]	9.3.2.1
NBR457	All suppliers will implement a solution that meets the NBS requirements	Partial[98]	This SDS
NBR458	The system will allow transactions to be voided according to Reference Data rules	Partial[99]	3.3.2.2.1, 6.3.2.8

[95] *Section s69 and s70 of [PACE] are no longer applicable. Pathway will ensure that relevant information will be provided, at PO Ltd's request, in support of prosecutions*

[97] *NBE to supply [C4], [S], [D] and [EoD] information in support of this*

[98] *For those aspects within their domain of responsibility*

[99] *No support for Contra transactions; NBE and Client interfaces are outside Pathway domain*

	while processing the peak load, including peak ten minute load, detailed in the spreadsheet 'NB volumetrics' *Pathway Comments: See* NBR053, NBR055 & NBR057. *[SRS] refers to [SRSVOLS]*		
NBR463	All existing front-end processes will be reviewed and modified if required, in order to support the new functionality provided by the NBS Release. *Pathway Comment: Check* NBR232, NBR275	Yes	6.3.1, 17.9
NBR464	The system shall support Outlet accounting for NBS transactions via the Cash Account. *Pathway Comment: See* NBR018/NBR017	Yes	3.4.1.10, 5.4.4.1.1, 5.4.4.1.4
NBR468	Once a banking transaction has been initiated, it must complete (i.e. be voided, declined or confirmed as successful) before another transaction can commence. For example, Horizon must not register further token swipes until the first transaction is Confirmed and added to the transaction stack.	Yes	3.4.1.5
NBR472	In the event of full disaster, Pathway will switch operation Wigan to Bootle or visa versa	Yes ESF	14.3.2
NBR473	The results of various testing phases will confirm that the release is fit for the live environment, and that the risks of going live are known and assessed. *Pathway Comment: Each test will be confined to the criteria agreed between all the parties.*	Yes	18.3
NBR474	Security testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. *Pathway Comment: Security testing will be confined to the criteria agreed between all the parties.*	Yes	13.2.4.1, 18.3.2.8.1
NBR475	Volume testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties *Pathway Comment: Volume testing will be confined to the criteria agreed between all the parties.*	A2A	18.3.2.8.2
NBR476	Disaster Recovery testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. *Pathway Comment: Disaster Recovery testing will be confined to the Requirements agreed between all the parties.*	A2A	18.3.2.8.3
NBR477	System testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. *Pathway Comment: System testing will be confined to the criteria agreed between all the parties.*	A2A	18.3
NBR478	Interface testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. *Pathway Comment: Interface testing will be confined to the criteria agreed between all the parties.*	A2A	18.3.2.7
NBR479	Each supplier will comply with the security standards agreed in BS7799.	Yes ESF	13.2.4.2
NBR480	Dependent upon rules defined within Reference Data, it must be possible to void a transaction after a Request has been generated and prior to a value Confirmation being placed on the stack. A successful void will result in a system change to the status of the [C] that has yet to be written to disk. It is akin to a 'change of mind' during the original transaction and affects the [C] in a similar fashion. The status of the [C] is amended reflecting the voiding and the value amended to zero. The transaction remains on the stack as the work has still been undertaken. The Client will only get one [C], in this case the amended one	Yes[101]	3.3.2.2.1, 6.3.2.8

[100] *Subject to PO Ltd clarifying volumes*

[101] *Pathway will make available the Reference Data. Also second paragraph, first sentence, should read "A successful void will result in a system change to the status of the [C] that has yet to be written to **the stack**" as agreed at meeting in Chesterfield 22/06/01*

	Pathway Comment: As documented in [CNTRDLG]		
NBR481	If the Horizon Counter PC fails, the following procedures should be adopted Single PC Outlet: - Clerk must decline the transaction – no fallback operation is currently supported Multiple PC Outlet: - The Clerk should move to another terminal. If a banking transaction is already underway, the clerk may transfer the customer session, as defined in NBR070 In all instances, a call to the HSHD shall be made to resolve the problem.	PO Ltd Only	n/a
NBR482	If The Horizon Monitor fails, the following procedures should be adopted Single PC Outlet: - Clerk must decline the transaction – no fallback operation is currently supported Multiple PC Outlet: - The Clerk should move to another terminal. If a banking transaction is already underway, the Clerk may transfer the customer session, as defined in NBR070 In all instances, a call to the HSHD should be made to resolve the problem.	PO Ltd Only	n/a
NBR483	Monthly and weekly summary report of withdrawals, deposits and balances by FI, account type (defined by IIN range), transaction type, volume and value at national level (UK), country level (e.g. Scotland), territorial level, HORN level, RNM level and Outlet level. It should be noted that Consignia may, from time to time, alter the above reporting hierarchy through normal OBC/Reference Data channels (for example, RNMs may soon be replaced with RLMs, with some degree of overlap during implementation).	Yes[102]	5.11.1, 8.5.2
NBR484	If a Horizon Touch screen fails, the transaction can be completed via the LIFT keyboard. A call to the HSHD should be made to resolve the problem.	Yes ESF	14.2
NBR485	If the keyboard aspect of the Horizon Keyboard fails, the transaction can be completed via the touch screen. A call to the HSHD should be made to resolve the problem.	Yes ESF	14.2
NBR486	If the Magnetic Card Reader aspect of the Horizon Keyboard fails, the card details can be entered manually. A call to the HSHD should be made to resolve the problem.	Yes ESF	6.3.2.1, 14.2
NBR488	If the PIN Pad reader fails, the following procedures should be adopted: Single PC Outlet: * Clerk must decline the transaction if no other means of verification (e.g. signature) would be acceptable Multiple PC Outlet: * If no other means of verification (i.e. signature) is acceptable for the presented token, the Clerk should move to another Counter. The Clerk would have to abandon any existing NBS transaction and start again on another Counter In all instances, a call to the HSHD should be made to resolve the problem	Yes	6.3.2.1
NBR489	Performance testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties. *Pathway Comment: Performance testing will be confined to the criteria agreed between all the parties.*	Yes	18.3.2.8.2
NBR490	If a back office printer should fail, the Outlet will be unable to produce	PO Ltd Only	n/a

[102] *Requires changes to Reference Data interfaces. [RDSAIS] has been updated to reflect the reporting hierarchy shown in [NBR483]*

	any Outlet reports until the issue is resolved via a call to the HSHD. *Pathway Comment: The HSHD will provide a single point of contact for fault management. In the event of failure, existing procedures will be followed.*		
NBR493	The system will be designed to have the same "look and feel" as the existing Horizon system	Yes	6.2
NBR497	Operational Level Agreements (OLAs) – to be defined	A2A	n/a
NBR498	The system shall be able to migrate from one Release to another with minimal disruption to operational service.	Yes[103] ESF	19.2
NBR499	End to End testing will be defined in a detailed Test Strategy, which will be agreed and approved by all parties *Pathway Comment: end to end testing will be defined to the criteria agreed between all the parties*	Yes	18.3.2.4
NBR500	Management of operational incidents to be documented with supporting processes and procedures. *Pathway Comment: HSHD will embrace fault management, overall service management, information and administration.*	Yes	17.9
NBR501	The system will adhere to relevant standards where appropriate. *Pathway comment: The appropriate standards are given in the* [SRS]	Yes – as defined in SRS[104]	6.3.2.1, 13.2.3.2, 13.2.4.2, 0, 13.4.5
NBR502	The system shall be able to revert to any earlier version of the banking service without disruption to the operational service.	Partial[105]	19.2
NBR503	The system shall adhere to the requirements of the law and of the financial services industry	Yes [ESF]	13.2.1
NBR504	Identification of operational incidents must be defined within each service boundary	Partial[106]	20.2.3
NBR505	In the event of failure, the system should, where possible, provide fallback processes to allow business to continue, and provide a facility to recover information once the system is restored.	Yes[107]	3.4.4, 5.4.3.4, 14.2
NBR506	The system shall comply with [ISO 11568] (Key Management)	Yes[108]	13.4.2
NBR507	Processes and procedures to handle Campus to NBE Communication failure are to be defined. *Pathway Comment: Management of incidents will be in accordance with current, jointly agreed working practices. Operational procedures to handle NBE/Horizon 'handshakes' around the boundary to be defined (exception reporting and escalation points).*	Yes [ESF]	
NBR509	The introduction of PIN Pad functionality shall be designed and developed and implemented for Release 1. Any such device selected and the associated technical architecture shall be compliant with the requirements of the Security Annex (Appendix B)	Yes, subject to PIN Pad selection	6.4, 13.4.2 passim
NBR511	Existing procedures and processes to handle Campus to TIP Communication failure should be adopted	Yes ESF	3.3.4, 5.10.1
NBR512	Processes and procedures to define wide-area network failure are to be defined.	Yes [ESF]	
NBR513	Existing procedures and processes to handle Campus failure are to be	Yes[109] ESF	

[103] *Requires discussion with NBE supplier on NBE related aspects*

[104] *A definition is needed of which standards are appropriate to which aspects of end to end system operation*

[105] *Release plan to be agreed with PO Ltd, ensuring minimal disruption (see [NBR498]); also subject to PO Ltd regenerating Reference Data if reversion is at PO Ltd's request*

[106] *For those aspects within Pathway domain*

[107] *Fallback working at the Outlet is not required;* Pathway *will provide for transaction recover at the Counter after failure.*

[108] *Except where this conflicts with HMG standards agreed with PO Ltd*

[109] *Will require to discuss continuity of online services to external hosts*

	adopted *Pathway Comment: This includes the Business Continuity Strategy and Business Continuity Test Plan*		
NBR514	A process for escalating operational incidents will be developed *Pathway Comment: Operation of escalation procedures affecting NBS in accordance with the Service Management Framework, Interface Agreement for NBSC, HSHD and Problem Management.*	Yes[110] [ESF]	
NBR519	Each helpdesk will provide relevant information for referring queries between the other helpdesks *Pathway comment: Calls may be received directly from user or PON help desks/lines queries may be referred to other helpdesks. Calls outside HSHD responsibility to be transferred appropriately.*	Yes[111]	
NBR534	System Health Monitoring – Tivoli will enable Consignia to monitor the system and produce alerts for error states that can then be rectified. However there is a requirement to have real time monitoring of selected error messages that produce alerts when they exceed a certain threshold even though in small numbers they may be quite acceptable. For example: a large volume of late messages or messages with bad bit maps, may indicate a problem not otherwise reported by the system but nonetheless producing an unacceptable loss of functionality. This requirement includes all messages to and from the NBE not just those exchanged with external parties such as POCA or LINK. *Pathway Comment: Pathway will design the most appropriate and cost-effective system monitoring processes to enable it to meet its SLAs. This may or may not involve real-time alerts. Pathway is willing to discuss the system monitoring it will implement, but feels the determining factor is the SLAs. This requirement is inappropriate as expressed in that it anticipates a specific solution. To be discussed at a commercial review. Approach is documented in this SDS*	Partial	12.8.4, Chapter 20 passim
NBR536	Each system which processes a transaction shall record the transaction details including the transaction type, date, time, sequence number, the amount(s) where applicable, the account number/PAN, and status (success/failure with reason). Any authorisation code allocated by the card issuer shall be included. The record shall also indicate if the card data was manually entered as opposed to being read from the magnetic stripe.[S24] Note: This is not intended to include communications systems that simply provide a transport mechanism. Transaction sequence number can be a combination of a number of attributes that provide a system wide unique transaction identifier. All messages shall contain sufficient information to enable all messages within a single transaction to be identified.	Yes [ESF]	7.3.2.1, 13.2.3.1, 13.5.1.1
NBR537	The source and destination of the transaction shall be recorded where not implicit in the system design. It shall be possible to trace transactions based on any reference allocated by the originating system and by any reference allocated by the destination system. [S25]	Yes[112]	
NBR538	No discretionary data from Track 1 or Track 2 (as defined in ISO 7813) shall be recorded in plain text in any log or Audit Trail. This clarifies the existing requirement. The recording of encrypted PIN Blocks is deprecated. [S26] Note: This does not imply a specific requirement to store discretionary data.	Yes[113]	7.3.2.1, 13.4.2.1.2
NBR539	For each transaction involving a cardholder, the cardholder shall be	Yes	6.3.2.9

[110] *HSHD and problem management - will require agreement in detail*

[111] *For the HSHD, and to be agreed in detail*

[112] Pathway *to NBE is a single channel, hence the source and destination is implicit in the system design and security mechanisms. Meeting in London 31/07/01 - PO Ltd clarified "any reference" to be transaction identifiers allocated by Horizon or the Client bank (see [RAC] e.g. section 4.2.5)*

[113] *The encrypted PIN Block will be retained in audit files in order to preserve the integrity of the audit records generated from the Riposte Message Store*

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

	provided with a printed advice that includes the data as described in NBR536. The advice shall also identify the location of the terminal. Printed advices shall not include the entire PAN by masking at least five digits by an asterisk (*) or other fixed character. No discretionary data (as defined in ISO 7813), PIN or encrypted PIN shall be printed or displayed. [S27] Printed advice need not indicate whether card data was manually entered Post office location on receipt will be provided in accordance with other systems (e.g. APS) which shows FAD, office name, address lines 1-3, post code. Note that BES deliberately omitted the office location on the receipt. Details to be agreed with PO Ltd. Status to be printed in clear on the receipt (either AUTHORISED or DECLINED). The reason for a decline is not to be printed.		
NBR540	For transactions authenticated by a cardholder's hand-written signature, a copy of the printed advice defined in NBR539 shall be produced for signature by the cardholder. The signed copy shall be retained on behalf of Consignia as part of the Audit Trail. Note that some banks (but not LINK) require a signed printed advice for a debit transaction (e.g. cash withdrawal) to include the words such as 'Please debit my account with the total amount shown'. [S28]	Yes	6.3.2.9
NBR541	It shall be possible to identify the Counter terminal operator responsible for each transaction from audit data. [S29]	Yes ESF	7.3.2.2, 7.3.2.3, 7.3.2.4, 7.3.3.1, 7.3.5, 7.3.6.2
NBR542	Audit Trails shall be protected against alteration and unauthorised deletion. They shall be retained in accordance with current practice for at least seven years. Audit data shall be produced on demand in accordance with current practice. [S30]	Yes[114] ESF	13.5.3, 13.5.4.3, 13.5.4.4
NBR544	Suppliers shall provide limited query facilities to enable the extraction of all records from Audit Trails that satisfy the following criteria: a) Date, time-range, office and PAN, or b) Date, time-range and office. All queries are assumed to be made one or more days after the date in question, and to require a response within seven days. [S47]	Yes [ESF]	13.5.3
NBR545	The same facilities shall be provided to enable querying of suppliers fault logging and help desk records. [S48]	Yes ESF	20.3
NBR546	In all cases, the query facilities shall be sized to cope with the volumes and performance stated.[S49] Refer to NBR260 & NBR315 for volumes and performance as per NBR544.	Yes – but see caveats on NBR260 and NBR315	13.5.3, 13.5.4.4
NBR547	The level of any documentation and support that Consignia needs to support its activities in these areas depends on the nature of the security incident to be supported. In the case of prosecutions, suppliers shall provide standard type Witness Statements to support Consignia in any legal actions it undertakes. It is envisaged that these statements will be standardised as far as possible. [S50]	Partial[115]	18.2.1.4
NBR548	The suppliers shall support the activity of annual renewal of the LINK Compliance Certificate. This activity is expected to consist of the following. Consignia will receive a request from LINK. Consignia and the suppliers will review the LINK security documents to identify any changes to requirements. If any changes are required, they will be handled within change control. Otherwise suppliers will be asked to sign a statement that they are still in conformance with the original requirements as agreed. [S34]	Yes – subject to PO Ltd organising the process and documenting the requirements	n/a
NBR549	The overall system, and hence the systems and services from individual suppliers, shall pass the following overall acceptance tests:	Yes – subject to PO Ltd	13.2.4.1

[114] *Potential mismatch with NBR443*

[115] *Pathway believes standardised witness statements will not be accepted by the courts until sufficient case law is established.*

	a) All the tests defined for LINK Certification, as defined in the LINK Test Strategy, Version 2.6, 21 June 2000 (or as subsequently updated) ('Consignia self-certification') b) Tests to verify that all requirements of the LINK Information Security Standard, version 1.0, January 2001 (or as subsequently updated) are satisfied, and may include penetration tests, by prior specification and agreement with the suppliers (' Consignia self-certification') c) Security tests derived from any agreed contractual requirements not covered by the above ('Consignia self-certification') d) Policy and system audit conducted on behalf of Consignia by an independent third party ('provision of evidence of a third party evaluation'), expected to be conducted by Ernst and Young. Note that the preceding is additional to any specific technical tests, e.g. throughput, performance, resilience. In the case of Horizon, penetration tests on the live estate will not be carried out. However, Pathway shall enable a third party to carry out penetration tests against a 'Live Test' environment. The configuration of the Live Test environment shall be agreed between Consignia and Pathway as part of developing the Test Strategy. Note: The Test Strategy shall incorporate the concept that Consignia reserves the right to carry out such checks as Consignia deems necessary to ensure that the specified requirements have been implemented, and the resultant systems and services meet the specified requirements and that changes to the Test Strategy shall not be unreasonably withheld. [S33]	organising the process and documenting the requirements	
NBR550	Suppliers shall provide a test strategy and plans for their own domains, which includes, but is not limited to, a testing sequence as outlined in the LINK Member Test Strategy, or as subsequently updated. ICC ATM testing referenced in the LINK document is not required.[S31]	Yes	13.2.4.1, 18.3.2.1
NBR551	The suppliers shall support such validation/inspection of the design and implementation as necessary for stage testing and acceptance. [S32]	Yes	17.3
NBR552	The Web Riposte Framework shall not impose constraints that adversely affect Counter dialogue design or lengthen Counter transaction time.	No[116]	n/a
NBR553	The Web Riposte Framework shall support the capability to carry out parallel threads of processing within a transaction, including the capability for an online authorisation request to be in progress while printing a receipt or processing Counter terminal dialogue with the Clerk	No – Not in NBS Release 1	
NBR556	The development of this overall [security] policy **shall** be supported by the suppliers	Yes[117]	13.4.9
NBR557	Each supplier **shall** provide to Consignia, the security policy applicable to its domain of activity, consistent with its proposal.	Yes	13.4.9, Chapter 13 passim
NBR558	Suppliers are free to propose controls they believe necessary in addition to those in this specification in order to meet their obligations. The reasoning for additional measures **shall** be described.	Yes[118]	10.7.2, 13.4.3
NBR559	All suppliers, and systems and services supplied specifically for this project **shall** comply with standards compatible with [ISO 17799], in particular: - Personnel security - Physical and environment security - Computer and network management - System access control - Systems development and maintenance - Business continuity planning.	Yes [ESF]	13.4.2.1

[116] *The WebRiposte Framework will not be used in NBS Release 1. The properties of the Framework, and any constraints, will be identified outside of NBS Release 1.*

[117] *Where it is applicable to the Horizon system*

[118] *Provided and described within design and specification documents*

NBR560	All suppliers, and systems and services supplied specifically for this project **shall** comply with standards compatible with [ISO 17799] and ISO9003, Part 1 at all stages in the lifecycle.	Yes[119]	13.4.2.1
NBR561	Each supplier **shall** advise Consignia of the assumptions made and the recommended security processes on which the supplied products and services may depend.	Yes	Chapter 17 passim
NBR562	In exceptional circumstances the suppliers shall not unreasonably refuse to assist Consignia in the investigation of residual security incidents not addressed by facilities defined in these requirements.	Yes[120]	n/a
NBR563	Suppliers **shall** be responsible for reporting to Consignia, investigating and resolving security incidents within their own domains that present an actual or potential threat to the NBS environment or to any of the Network Banking participants.	Yes[121]	n/a
NBR564	When a PIN Pad device is provided it will meet the requirements of [ISO 9564]. Suppliers' architectures and technical infrastructure must be capable of supporting the incorporation of PIN Pads and must be independent of specific PIN Pad models and suppliers. [S11] *Pathway Comment: Suppliers of PIN Pads use proprietary architectures and APIs, and hence it is not possible for Pathway to develop the Horizon infrastructure such that it is independent of specific PIN Pad suppliers or models*	Yes (ISO9564) No (independent of PIN Pad model/suppliers)	Chapter 17 passim
NBR566	The suppliers' architectures **shall** conform to the technical security architecture requirements described in this section, including diagrams.	Yes	13.4.4 passim
NBR567	Suppliers' proposals **shall** provide supplementary design and operational information as required to assure Consignia of their end to end and domain security solutions including, but not limited to: - Storage security - Transmission security between devices - Key initialisation.	Partial[122]	Chapter 13 passim.
NBR568	The protection for the existing Horizon Outlet network, Horizon Campus network and other existing network connections **shall** continue without change as per current practice, unless expressly stated otherwise in this specification	Noted ESF	
NBR569	Any message having a financial value **shall** be protected such that the recipient can authenticate the source and integrity of the message.	Yes	13.4.3
NBR570	Message Authentication Codes (MACs) **shall** be used for the authentication and integrity protection of all messages between the NBE and Horizon system. Detailed document to be agreed	Yes	13.4.2.2.1, 13.4.3
NBR571	Any direct connection to the public Internet **shall** additionally be protected by an appropriately configured firewall and **shall** be subject to periodic penetration tests by Consignia or its authorised agents designed to ensure that the configuration is effective.	Noted[123] ESF	10.7.2
NBR572	Any remote system maintenance or diagnosis via a public network (including PSTN) **shall** be effected via a connection under the control of the on-site operational management team responsible for the specific system concerned. Such connection **shall** only be made at the instigation of the operational management team and for the duration that the team have reason to believe that there is a problem requiring remote access. At all other times, the connection **shall** be physically disconnected from the public networks.	Yes ESF	20.4

[119] *Pathway is registered for [ISO 9001], which exceed the requirements of [ISO 9003] Part 1*

[120] *Pathway assume that any additional costs incurred will be reimbursed, by PO Ltd, on a Time and Materials basis*

[121] *Pathway assumes that the mechanism and procedures for reporting incidents to PO Ltd will be defined as a part of the (future) Network Banking Automation Security Policy*

[122] *High level information is provided within this SDS and elsewhere. Pathway will provide high level information but does not accept the "without limitation" qualification.*

[123] *The Horizon system has no direct connection to the internet. The firewall configurations described in Section 10.7.2 are designed to protect the Horizon network from internet access via the NBE.*

NBR573	Line encryption hardware devices **shall** be located within the physical security boundary of the host system and **shall** use different keys than used for PIN encryption or message authentication	Yes ESF	10.7.2.5, 13.4.3
NBR574	It **shall** be possible to recover the security of the system to a secure operating state from the compromise of any key that could directly or indirectly expose plain text PIN values	Yes	13.4.3
NBR575	PINs **shall** be protected in accordance with the requirements of [ISO 9564].	Yes	13.4.2.1.2
NBR576	PIN Block formats **shall** comply with the standard. [ISO 9564]	Yes	13.4.2.1.2
NBR577	PINs **shall** never appear in plain text other than within a tamper-resistant hardware security module or a tamper-evident PIN Pad as defined by the standard (ISO 9564) [S40]	Yes	13.4.3
NBR578	Instances of PIN encipherment keys **shall** not be used for any other cryptographic purpose.	Yes	13.4.3
NBR580	There **shall** be protection against replay of messages	Yes	13.4.2.1.4
NBR581	Replay of encrypted PIN values shall be prevented	Yes	13.4.2.1.4
NBR582	Keys that could directly or indirectly expose plain text PIN values and any keys used in association with banking MACs **shall** be managed in accordance with the principles established in [ISO 8732] or [ISO 11568]	Yes	13.4.5
NBR584	The technical security architecture for message interchanges where a PIN Pad is not installed in an Outlet **shall** differ from the architecture with a PIN Pad, simply by the omission of the encrypted PIN Block and associated cryptographic controls [S19]	Yes	7.3.2.1
NBR585	It **shall not** be necessary to have a PIN Pad installed in order to operate the security scheme for hand-written signature transactions	Yes	7.3.2.1
NBR586	The suppliers **shall** support the provision of an overall Technical Design Authority in the security area.	Yes[124] ESF	
NBR588	The suppliers **shall** specify what enforced disconnection facilities they consider necessary. Note that the introduction of multi-channels is expected to be phased. The introduction of channel support beyond the Horizon channel (e.g. Internet access) is expected to be scheduled after the implementation of the Horizon channel.	Yes[125]	10.5.1
NBR589	Protection against malware (malicious software including viruses, Trojans etc) **shall** be provided and **shall** be demonstrably commensurate with the anticipated risk as agreed with Consignia	Yes[126]	

Table 36 – Conformance to Requirements in [SOR]

21.2 PIN PAD REQUIREMENTS

Support of PIN Pads for transaction authentication will be mandatory for NBS Release 1. The requirements pertaining to PIN Pads are documented separately, in [PPREQ] and are repeated in [SRS]. Many of the requirements stated are specific to the particular device selected, or to the physical roll-out of devices to Outlets. These requirements are omitted from the following table.

Reference	Description	Status	Location
PPR001	The PIN Pad implemented at the Counter must support PIN validation for Magnetic Tokens	Yes	
PPR002	Magnetic Tokens issued on behalf of certain Clients may continue to be subject to signature verification. When required, signature	Yes (see also [PPR014])	

[124] *In support of the Horizon system and the interfaces to connected Domains*

[125] *The detailed criteria and procedures to be applied require further discussion within a wider Programme context and are required to be resolved prior to the start of the NBS*

[126] *Provided such Risks are notified to Pathway by PO Ltd within the SDS development time-frame*

	verification will be performed by Counter staff, following screen prompts issued by the Horizon system, and will not call upon functionality offered by the PIN Pad *Pathway Comment: See [PPR014]*		
PPR004	The Horizon software required to enable the processing of EMV cards may be delivered at a later date to meet the availability of EMV-compliant service. Pathway are responsible for ensuring that the Horizon software is EMV compliant, within the timescales dictated by Consignia.	Not in Release 1	
PPR011	On receipt of the appropriate command from the Horizon terminal, the PIN Pad will display the text message received from the terminal and prepare for keypad entry.	Yes	6.3.2.11
PPR012	The PIN Pad will not be limited to the type of transactions that it can support. The software running on Horizon will determine the transaction. *Pathway Comment: The software running on Horizon at NBS Release 1 will be limited to defined transactions. The PIN Pad may support other transactions in the future, but this will not be proven with NBS Release 1 transactions*	Yes, subject to Pathway comment	
PPR013	Different Horizon applications will be using the same device. For example, the Counter clerk may perform an NBS transaction followed by an EFTPoS transaction, using the same Token. Each transaction is deemed to be unique, and will require a separate token swipe / read, and entry of PIN. *Pathway Comment: PO Ltd have not identified a requirement for PIN Pads with EFTPoS. See also PPR012*	Yes, subject to Pathway comment	
PPR014	Reference Data (provided by Consignia) will determine the method of verification to be used for each transaction type [NBR410] The Horizon terminal will send and request information from the PIN Pad as appropriate. For clarification: Tokens will be defined in Reference Data grouped by IIN (Issuer Identification Number). Each IIN grouping will have one or more *Customer Verification Method* lookups (see document [3]). Initially, the *Customer Verification Method* may be PIN, signature or PIN and signature (i.e. signature if PIN Pad not available). This will determine whether the Horizon terminal should utilise the PIN Pad or not. *Pathway Comment 1: The above clarification is misleading and a more accurate clarification reads as below (agreed between Reference Data teams in PO Ltd (Chesterfields) and Pathway (Feltham)).* *“Tokens will be defined in Reference Data grouped by Issuer Scheme. Each Issuer Scheme may support a number of banking operations (deposit, withdraw etc) and the appropriate Customer Verification Method can be specified for each. Initially, the Customer verification Method may be PIN, signature or PIN and signature (i.e. signature if PIN Pad not available). This will determine whether the Horizon Counter should utilise the PIN Pad or not. Pathway is dependent on PO Ltd providing the Reference Data to define the verification method to be used for the IJIN/operation on any valid NBS token.”* *Pathway Comment 2: Pathway takes “available” to mean “installed” (as determined by Reference Data). Pathway will not continuously monitor the presence of the PIN Pad to ascertain that it is functioning. PIN Pads have very high MTBF, and Pathway will not distinguish between PIN Pad deliberately turned off (potential fraud risk) and non-functioning. Decision to use PIN or signature will be controlled by the system at the outset of the Transaction depending on whether a PIN Pad is installed. See also PPR002 and NBR250*	Yes, subject to Pathway comment	
PPR021	The customer is not required to key in the amount that they require to deposit/withdraw, as this could encourage misuse of the system. Rather the amount will be captured on the Horizon system, which will then pass the information to the PIN Pad for display onscreen.	Supported subject to Pathway comment	6.3.2.11

	Pathway Comment: The Counter dialogue for NBS Release 1 will be restricted to magnetic stripe cards. The Counter dialogue will be agreed separately with PO Ltd, and may or may not involve PIN Pad displays of amount requested for withdrawal/deposit		
PPR023	The display content is to be driven by the computer to which the PIN Pad is connected. Any in-built dialogue e.g. for transacting EMV cards etc., must be publicised and agreed by Consignia.	Yes	6.3.2.11
PPR026	The Horizon application must pass instructions to the PIN Pad which prompt the customer to insert/withdraw their ICC card as appropriate	Yes	
PPR028	Conversion of the PIN encrypted value between the Horizon and NBE domains will be performed in a separate HSM that will ensure that the PIN value will never appear in plain text.	Yes	
PPR029	Consignia require that the status of all PIN Pads live in the network estate is routinely monitored through the use of an appropriate Systems Management tool. For definition: routine means as per the existing schedule for Systems Management of existing Horizon equipment *Pathway Comment: PIN Pad API is restricted as to what can be monitored. Pathway will monitor battery low condition*	Yes, subject to Pathway comment	12.8.4
PPR031	Consignia require that a cost effective management of firmware service is provided *Pathway Comment: The existing software management and distribution service, which is based on Tivoli, will be extended to cover the PIN Pad firmware*	Yes	12.6.2
PPR071	The recording of encrypted PIN values is not required (other than on audit logs) [NBR538]; specifically, this information should not be displayed on customer or office receipts [NBR539] Pathway Comment: Duplicate NBR538	Yes	
PPR074	Successful penetration shall not permit the disclosure of any previously entered Transaction PIN (i.e. prevent backtracking)	Yes	
PPR075	There shall be no feasible way to determine any past key given the knowledge of any data that has been transmitted to or from the device. ([ISO 9564-1])	Yes	
PPR096	Where the PIN Pad has proven capability to process cards (e.g. EMV) and SAMs, this should be exploited with the Horizon processing being limited to Clerk inputs to set up and control the transaction and Horizon acting as the communication channel should the PIN Pad need to communicate with other devices	Yes	

Table 37 – PIN Pad Requirements

!