FUJ00088068

Document Title: SECURITY FUNCTIONAL SPECIFICATION

Document Type: Specification

Release: **BI3 onward**

Abstract: This Security Functional Specification (SFS) defines the security functionality that is incorporated into the operational Horizon System.

Document Status: APPROVED

Originator & Dept: Graham Hooper, CS Security.

Contributors: Nigel Taylor, Chris Rayner, Pete Sewell, Geoffrey Vane, Jane Bailey, Dave Tanner, Glenn Stephens.

Internal Distribution: Alan D'Alvarez, Graham Chatten, John Coakes, Warren Welsh, Peter Dreweatt, Jan Holmes, Graham Hooper, Peter Jeram, Dave Hollingsworth, Ian Morrison, Mik Peach, Martin Riddell, Peter Wiles, John Wright, Mark Ascott, Tony Drahota, Dave Tanner.

External Distribution: Bob Booth (Post Office Ltd.)

Sue Lowther (Post Office Ltd.)

Approval Authorities: (See PA/PRO/010 for Approval roles)

Name	Position	Signature	Date
Stephen Muchow	Managing Director		
Colin Lenton Smith	Director Commercial and Finance		
Peter Jeram	Director of Programmes		
Gill Jackson	Director of Development		
Martin Riddell	Customer Service Director		
Dave Hollingsworth	Director Consultancy Services		
Bob Booth	Post Office Ltd.		

FUJ00088068

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	15/8/96	Initial Draft for internal review	
0.2	16/8/96	Incorporates comments from internal review	
0.3	20/9/96	Incorporates comments from CASA	
0.4	24/9/96	Incorporates comments from internal review	
0.5	10/10/96	Incorporates comments from PDA	
1.0	23/10/96	Submitted for formal approval	
1.1	4/11/96	Minor changes incorporated	
2.0	11/11/96	Approved	
2.1	25/2/97	Incorporates Energis inter-site link, Data Warehouse, virus protection, etc	
2.2	19/6/97	Incorporates revisions to Security of Links, Message Protection and Filestore Encryption.	
2.3	15/7/97	Incorporates revisions to Audit and Alarms.	
2.4	31/7/97	Incorporates revisions following review by PDA.	
3.0	3/12/97	Approved	
3.1	31/7/98	Incorporates VPN changes and updates, mainly to sections 8 and 9.	
3.2	5/8/98	Landis and Gyr changes added.	
3.3	11/12/98	Incorporates comments and minor corrections, following review of version 3.2. Siemens Metering text replaces Landis and Gyr.	
3.4	18/3/99	Incorporates comments from review of version 3.3, Including new sections on Solaris, SecurID and ACE/Server.	
4.0	30/4/99	Approved	
4.1	24/6/99	Removal of references to Benefits Agency and Benefits Encashment Service relating to Contract changes.	
4.2	11/1/00	Incorporates minor corrections.	
4.3	24/2/00	Incorporates minor corrections following reviews.	

FUJ00088068

4.4	3/4/00	Incorporates minor changes following external review.	
4.5	22/8/01	Adoption of document by CS Security. Amendments to layout to reflect revises in Pathway Organisation and document template. For review and baselining as a NWB dependency.	
4.6	18/2/02	To incorporate changes up to release S10 to provide a baseline prior to the introduction of Network Banking. To reformat the document to conform to the latest Pathway Template	
4.7	11/07/02	Incorporate changes following internal review. Correcting template, format, spelling and organisational names. Amendment to future tense. Removal of HAPS. Addition of Oracle 8I and change to SQL Server 2000. Contracting Authorities changed to Post Office Ltd.	
5.0	16/09/02	Approved	
5.1	23/09/02	Incorporates changes at BI2 and BI3 including FRIACO, Radius Servers and VPN on the LAN. Introduction of changes for Network Banking including a new chapter on security enforcing functionality for the NBS.	
5.2	23/09/02	Incorporates comments received from internal and external review. Revision of the structure and content of Section 11.	
6.0	13/11/02	Incorporates section on access controls for remote support; minor typographical changes and clarification in text; abbreviations added. Approved	
6.1	30/12/02	Incorporates security elements relating to Debit Card MoP introduced at BI3 S30. New Chapter 12.	
7.0	24/01/03	Incorporation of comments at 12.2 and 12.3 concerning keys and signing / cryptographic key management for DC. Amendment to Section 12 and Figure 12.1 to reflect introduction of MPPE Server on link to MA. Minor typographical corrections and additional abbreviations added to Section 0.4. Approved	

FUJ00088068

0.2 Review Details

Review Comments by :	
Review Comments to :	

Mandatory Review Authority	Name
APDU Manager	Mark Taylor
IPDU Security Analyst	Mark Ascott
System Manager Architect	Glenn Stephens
NT Technical Support	Warren Welsh
Quality and Audit Manager	Jan Holmes
Director of Programmes	Peter Jeram
Technical Manager	Dave Tanner
IPDU Manager	Ian Morrison
Director Consultancy Services	Dave Hollingsworth
SSC Manager	Mik Peach
CS Director	Martin Riddell
Chief Architect	Tony Drahota (Peter Wiles)*
Customer Services	John Wright
Security Architect	Geoffrey Vane*
Ref Data	Dave Wilcox
Debit Card Project Manager	Klaus Loffler
Post Office Ltd.	Bob Booth*
Optional Review / Issued for Information	
Post Office Ltd.	Sue Lowther

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	7.0	2nd April 2002	Fujitsu Services Document Template	PVCS
CR/FSP/004			System Architecture Design Document	PVCS
RS/POL/002			Pathway Security Policy	PVCS

FUJ00088068

[SECPOL]				
RS/FSP/003			Statements on Security Objectives and Methods for the Protection of Siemens Metering Code and Data	PVCS
RS/REQ/001 [SECOBJ]			Pathway Security Objectives	PVCS
RS/POL/003 [ACCPOL]			Pathway Access Control Policy	PVCS
RS/DES/010			KMS High Level Design	PVCS
NB/PRO/007			Network Banking Manual Key Management	PVCS
CR/FSP/006			Audit Trail Functional Specification	PVCS
TD/ARC/001 [TED]			Technical Environment Description	PVCS
RS/PRO/028 [SECPRO]			Pathway Security Management Procedures	PVCS
EF/SER/001			DC MoP Functional Description	PVCS
EF/SPE/002			Debit Card RAC Data Flow Model	PVCS
Oracle	-	-	Oracle Server DBA Guide	
Sequent	-	-	Dynix Operating System – System Administrator's Reference Manual	
Microsoft	-	-	Microsoft Windows NT Resource Guide	
ITSEC	-		IT Security Evaluation Criteria	
RS/PRD/004			Security Incident Management	PVCS Post Office Ltd.

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACC	Area Computer Centre
ACD	Automated Call Distributor

FUJ00088068

API	Application Programming Interface
APS	Automated Payment Service
ASP	Active Server Pages
Base64	(A mechanism for encoding arbitrary binary information)
BDK	Base Derivation Key
BKLK	Base Key Loading Key
BT	British Telecommunications
CA	Certification Authority
CCS	Common Charging System
CESG	Communications-Electronic Security Group
CGI	Common Gateway Interface
CHAP	Challenge Handshake Application Protocol
CLI	Calling Line Indication
CNIM	Communication Network Infrastructure Manager
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CRC	Cyclic Redundancy Check
CS	Customer Services
CS	Correspondence Server
DBA	Database Administrator
DC	Debit Card
DCA	Debit Card Authorisation Agent
DCE	Distributed Computer Environment
DCM	Debit Card Manager
DC MoP	Debit Card Method of Payment element of EPOSS
DES	Data Encryption Standard
DLL	Dynamic Link Libraries
DSA	Digital Signature Algorithm
DMZ	De-Militarised Zone
DUKPT	Derived Unique Key Per Transaction
DWP	Department for Work and Pensions (formally Department of Social Security (DSS))
EPOSS	Electronic Point Of Sale Service

FUJ00088068

ESNCS	Electronic Stop Notice Control System
FRIACO	Fixed Rate Internet Access Call Origination.
FTMS	File Transfer Management System
Fujitsu Core Services	Fujitsu Services, Core Services
GKLK	Global Key Loading Key
GL/AP/AR/PO	General Ledger / Accounts Payable / Accounts Receivable / Purchase Orders
GRK	Global Roll-out Key
HAPS	Host Automated Payments System
HSHD	Horizon System Help Desk
HSM	Host / Hardware Security Module
HTML	Hyper Text Mark up Language
HTTP	Hyper Text Transfer Protocol
ID	Identity
IK	Initial Key
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
KAREA	A global key used to encrypt code installed in PINPads.
KCV	Key Check Value
KMS	Key Management System
LAN	Local Area Network
MA	Merchant Acquirer
MAC	Message Authentication Code
MIDU/MIDU-A	Secure hardware devices used in PINPad key initialisation
MIS	Management Information Services
MPPE	Microsoft Point-to-Point Encryption
NAO	National Audit Office
NB	Network Banking
NBS	Network Banking Service
NDIS	Network Device Interface Specification
NMS	Network Management System
OBCS	Order Book Control Service
OLAP	On-line Analytical Processing

FUJ00088068

OLE	Object Linking and Embedding
OMG	Object Management Group
OPS	Office Platform Service
Pathway	Fujitsu Services (Pathway) Limited
PIN	Personal Identification Number
PK	Public Key (for PK Certificate)
POL / PO Ltd	Post Office Limited (in diagrams)
POM	Post Office Manager
PPD	Processes and Procedures Description
PSI	Post Office Ltd. Service Infrastructure
RAC	Request, Authorisation, Confirmation
RIPA	Regulation of Investigatory Powers Act (2000)
RPC	Remote Procedure Call
RCD	Release Contents Description
SADD	System Architecture Design Document
SCT	Secure Configuration Terminal
SFS	Security Functional Specification
SHA	Secure Hashing Algorithm
SLA	Service Level Agreement
SLCA	Service Level and Contract Administration
SM	System Management[1]
SMS	System Management Service
SMDB	Service Management Database
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
SQL	Structured Query Language
SSC	System Support Centre
TDES	Triple DES
TFTP	Trivial File Transfer Protocol
TIP	Transaction Information Processing

[1] To avoid confusion Siemens Metering is not abbreviated within this document.

FUJ00088068

TME	Tivoli Management Environment
TMP	Tivoli Management Platform
TMS	Transaction Management Service
TPS	Transaction Processing System
UDP	User Datagram Protocol

0.5 Changes in this Version

Version	Changes
6.0	Section 6.10 added to include access controls for external support. Diagram 8.2 amended. Section 8.8.1 amended to include support access via SSH Client. Addition of various abbreviations in Section 0.4.
6.1	Approval Authority and review lists updated. Associated documents and abbreviations updated Re-add figure 8.2 to Figures table. Re-add figure 3.4 to document as missing in version 6.0 DC add to the following sections; 1.5, 2.10, 3.1, 3.2, 3.4, 4.1, 4.5.1, 4.5.4, 4.7.2, 8.10, 8.11. New section 12.0 for DC additional security features.

0.6 Changes Expected

Changes
Comments for initial review.

FUJ00088068

Table of Contents

FUJ00088068

FUJ00088068

FUJ00088068

FUJ00088068

FUJ00088068

FIGURES

FUJ00088068

1.0 Introduction

1.1 Purpose

This Security Functional Specification (SFS) defines the security functionality that is incorporated into the Horizon system. It is primarily concerned with the technical features rather than the surrounding management or operational controls (defined in [SECPRO]).

1.2 Context

There are three broad categories of security controls, as illustrated in Figure 1.1

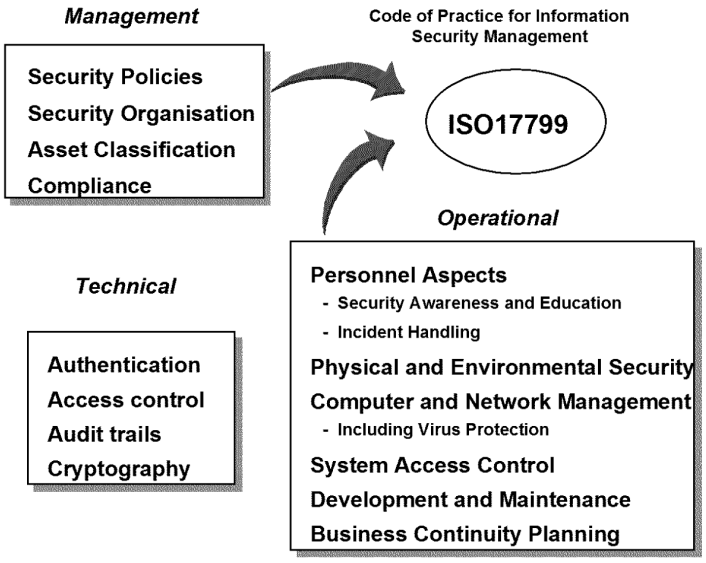

Figure 1.1 Security Control Categories

This document focuses on the technical security controls that are primarily concerned with authentication, access control, audit and the use of cryptography (as illustrated above).

ISO 17799, "A Code of Practice for Information Security Management", is primarily concerned with management and operational controls. It is used as the basis of Pathway's Security Procedures [SECPRO] to define the controls used throughout Pathway.

1.3 Scope

This Security Functional Specification (SFS) identifies the technical controls that are used to implement the security functionality within the Horizon system [SADD].

The (logical and physical) environment to be protected is defined in the Technical Environment Description document.[TED].

Where ever possible Commercial off-the-shelf (COTS) components have been used as the primary building blocks throughout the Horizon solution. This reduces the need for bespoke code and enable suppliers' standard product documentation to be used.

FUJ00088068

An overview of the security functionality, provided by the security components (identified in section 4.0), has been included in order to define the security features and system options that are used.

Control of access to the Horizon system and data is in accordance with the Pathway's Access Control Policy [RS/POL/003].

1.4 Pathway Security Policy

Pathway Security Policy document [SECPOL] encompasses all of the security requirements specified in Pathway's agreement with Post Office Ltd. A summary of these security requirements is defined in the document Pathway Security Objectives [SECOBJ].

By implementing the agreed Security Policy, Pathway will minimise and control liabilities to itself and Post Office Ltd. The Security Policy also explains how Pathway will comply with the controls defined in ISO17799.

This Functional Specification forms part of the IT security infrastructure identified in the Security Policy.

1.5 Document Structure

This document specifies security functionality within a framework of explanatory text. References to the associated documents, listed in section 0.3, are indicated by the document reference name in square brackets (e.g. [SADD]).

Additional functionality introduced with the Network Banking Service (NBS) and Debit Card method of payment (DC MoP) is incorporated where appropriate within the main text. Specific NBS security functionality has been captured in Section 11.0. Specific DC security functionality has been captured in Section 12.0

FUJ00088068

2.0 Management Summary

2.1 About this Document

This Security Functional Specification (SFS) defines the security functionality that is incorporated into the Horizon system. It is primarily concerned with the technical features rather than the surrounding management or operational controls.

2.2 Security Domains

The term "domain" has been used to describe distinct parts of the system characterised by type(s) of service provided, components used (e.g. NT), and/or area of responsibility. The domains are:

- Post Office Ltd. Central Services Domain,
- Office Platform Service Domain,
- Post Office Ltd. and Post Office Ltd Clients Domain,
- System Management Service Domain, and
- Pathway Corporate Services Domain.

The Post Office Ltd Central Services Domain contains the Horizon application hosts at the central Pathway sites.

The Office Platform Service Domain encompasses the Electronic Point Of Sale Service (EPOSS) including Debit Cards (DC), which supports all services, or products, provided by the counter clerk to the customer.

The Post Office Ltd. and Post Office Ltd. Clients Domain contains a variety of hosts associated with applications running in the OPS Domain.

The System Management Service (SMS) Domain contains the central elements of the System Management (SM) and Network Management System (NMS) facilities.

The Pathway Corporate Services domain supports Pathway's own management processes. The domain encompasses the Data Warehouse and Pathway's managed services.

There is no special (or cryptographic) protection required for the Order Book Control Service (OBCS) service and Electronic Stop Notice Control System (ESNCS) link, therefore it is not shown as a separate domain.

The NBS utilises functionality within the Office Platform Service and POL Central Service domains to deliver NBS related messages to the Network Banking Engine operated within the context of the POL and POL Clients Domain.

2.3 Security Components

The security enforcing components within the Horizon system are Windows NT, Dynix operating system (on Sequent platforms), Solaris operating System (on Sun platforms), Oracle 7/8i and MS SQL Server database products, networking components (including firewalls and routers) and encryption devices.

FUJ00088068

Firewalls are used to protect the Horizon system from unauthorised access via external networks and other local networks collocated at Pathway or Fujitsu Services sites. Protection is provided by a combination of packet filtering functionality within router components and application level firewalls.

Riposte, which is security relevant, is also security enforcing whenever it is configured to handle user authentication.

Virus protection facilities are installed on selected platforms.

External support users of Horizon systems are permitted access to Pathway Data Centre systems only from approved outlets/environments and subject to agreed network and other controls (see 6.10).

2.3.1 Identification and Authentication

Identification and authentication mechanisms are required to ensure that all users are uniquely identified, with only authorised users being granted any access to the system.

This document, therefore, defines overall requirements for user identification and authentication followed by specific consideration of users of NT, Dynix, Solaris, Oracle, Help Desk operators and Post Office Ltd. staff.

2.4 Logical Access Control

This document considers the access rights that need to be supported by system components and the ability of the system to enforce access rights.

To provide effective control of system resources, Pathway has produced a clearly defined Access Control Policy that identifies all users who are authorised to access any part of the system and the access rights that are to be permitted.

The Access Control Policy is expressed in terms of roles rather than named individuals. Users are then associated with one or more roles so that all persons are individually accountable for their actions.

In addition to control of access to databases, use of the access controls supported by Windows NT, Dynix, Solaris and Routers has been included.

2.5 Audit and Alarms

The audit and alarm facilities provided by the Horizon system are a combination of application level transaction logs and lower level audit tracks.

The Riposte application provides an ideal basis for logging all transactions to give a complete picture of actions within Post Offices Infrastructure Service.

Patrol is used to manage all Sequent systems and the Oracle applications that run on Sequent platforms.

Wherever possible, application level auditing is used. The notification services provided by the systems management products (notably Tivoli) is used wherever appropriate. Low level Windows NT audit tracks is also used to provide additional facilities where application level auditing of system management activities is not supported.

FUJ00088068

2.6 Crypto Functionality

This document describes the cryptographic functionality, within the Horizon system, used to protect:

- data on individual communications links,
- individual messages from creation to use (end-to-end),
- data stored on physically insecure Post Office filestore,
- sensitive data held throughout the Horizon system, and
- PINs in PINPads (including PINPad seeding, PIN blocks and PIN block translation in HSMs.

Key management is also covered. Communications aspects (as distinct from security functionality) are described in [TED].

Pathway's inter-campus links, between the Data Centres, are very high-speed (155Mbps) connections, which gives them a significant level of inherent security. There is, currently, no suitable encryption hardware capable of operating at this speed, so particularly sensitive data is protected using Red Pike.

DSA signatures are used to protect the integrity of data on the "TIP link" in both directions. Verification entails validation of the incoming public key certificate against a CA public key. The same end-to-end integrity protection is used, where appropriate, to protect other low volume data such as Post Office Outlet reconciliation totals.

The kilostream links that connect remote operational and support services to the Data Centres, are protected using commercial encryption or Rambutan based encryption hardware where this is considered necessary.

All APS data is sent directly to Post Office Ltd. customers using an on site FTMS remote platform.

The "SM/HSHD links" used, by Fujitsu Core Services, for support and system management, is protected using Government approved point-to-point encryption devices employing the Rambutan algorithm.

Links from the Pathway headquarters site to the Pathway campuses also use Government approved point-to-point encryption devices.

The "Post Office links", from the Post Office Ltd. Central Services Domain to the Post Offices Outlets, is protected by use of Virtual Private Networks (VPN), with each member of the VPN community having a different key pair. VPN also protects the Post Office LAN.

2.7 Message Protection

Message protection, where a digital signature is required, is performed using DSA with a 768 bit modulus. Each DSA signature requires a cryptographically strong random initialisation value, known as a K-value.

Standard public key technology is used, with Pathway's "PK certificates" based upon the X.509 standard. PK certificates contain the public key, the name of the possessor of the corresponding private key and an expiry date.

FUJ00088068

Automated Payments are signed in the Post Office Outlets for verification by a central harvester.

Message protection of data transmitted via the Horizon-NBE link is via Message Authentication Code (MAC).

2.8 Filestore Encryption in Post Office Outlets

Red Pike, incorporated into the Team Crypto product, is used to protect information held on hard disks within Post Office Outlets. The NT workstations installed in Post Offices do not have operable floppy disk drives (since, if fitted, they are physically blanked off and disabled in the BIOS).

Selected files on Post Office Outlet workstations and gateway machines are automatically encrypted at disk access level to preserve data confidentiality in the event of the workstation being stolen.

The Post Office Manager (or authorised representative) is the only person on site who has the means of unlocking the key to the filestore encryption.

2.9 Administration of Security

Roles have been broadly defined under three category headings, namely Operational, Systems Management and Support. The Pathway Access Control Policy contains a detailed definition of roles and responsibilities for all personnel who have any kind of access to the services provided by Pathway.

Systems management services are based upon three main products, namely Tivoli, HP OpenView and Patrol. The services provided include:

- Software Distribution - using Tivoli Software Distribution,
- Event Management- using Tivoli Event Console,
- Network Management - using HP OpenView,
- Resource Monitoring - using Tivoli Software Distribution, and
- Inventory Management - using Bespoke Inventory.

User management, which is primarily concerned with administration of user accounts and access controls, uses Riposte and the standard facilities provided for the Sequent, Sun and Windows NT platforms.

2.10 Network Banking and Debit Card Security Functionality

Details of the specific security enforcing functionality introduced to support the Network Banking Service are included at section 11.0. Details of the specific security enforcing functionality introduced to support Debit Card MoP are included at section 12.0.

Other security relevant changes introduced with Network Banking and Debit Cards are incorporated into pertinent sections of the main text.

FUJ00088068

3.0 Security Domains

3.1 Domain Definition

Within this document the term "domain" has been used to describe distinct parts of the system characterised by:

- type(s) of service provided,
- components used (e.g. Oracle, Dynix, NT), and
- area of responsibility (e.g. Pathway, Post Office Ltd.).

The domains, which may be geographically distributed, provide services that are used within the domain and/or by other domains.

The services offered by several domains combine to provide the end-to-end services, namely the Post Offices Infrastructure Service(POIS).

These services are defined in the System Architecture Design Document [SADD].

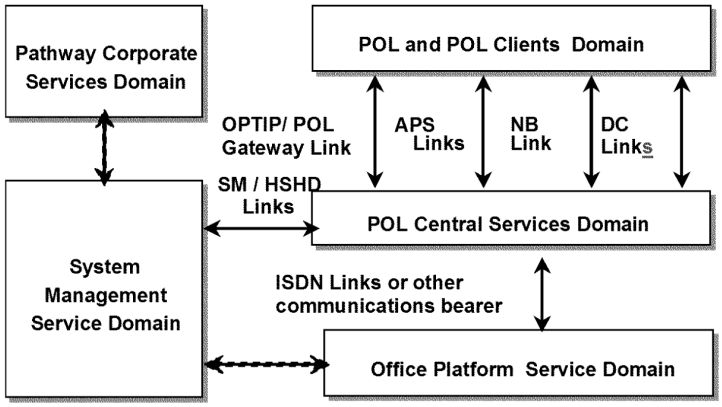

Figure 3.1 Communications Links Between Domains

Figure 3.1 illustrates the primary communications links between the domains. These links, which are the external connections to the Pathway central sites, are protected to preserve the integrity and confidentiality of information handled by the system.

There is no special protection required for the OBCS service and ESNCS link, therefore it is not shown as a separate domain.

Specific cryptographic protection is provided on the NB link between the POL Central Services Domain and the Network Banking Engine (NBE) operated within the POL and POL Clients Domain.

Cryptographic protection is applied on the DC link between the POL Central Service Domain and the Merchant Acquirer (MA) operated within the POL and POL Clients Domain for Payment and EMIS files.

Where domains encompass two or more geographic locations, the external links between sites are protected.

FUJ00088068

The authentication, access control and audit functionality, described in sections 5.0, 6.0 and 7.0, applies to all domains. The crypto functionality and message protection mechanisms, specified in sections 8.0 and 9.0, have been described for each type of link.

3.2 The Post Office Ltd Central Services Domain

The Post Office Ltd Central Services Domain contains the Horizon application hosts at the central Pathway sites. These hosts support the Post Office Ltd; APS, EPOSS, LFS, TPS, Reference Data and OBCS applications.

All applications run on Sequent machines with Oracle databases.

This domain also contains the Network Banking Agents that interface with the Network Banking Engine (NBE) Domain and the DC agents that interface with the Merchant Acquirer.

The Post Office Ltd. Central Services Domain interfaces with the OPS Domain as illustrated in figure 3.2.

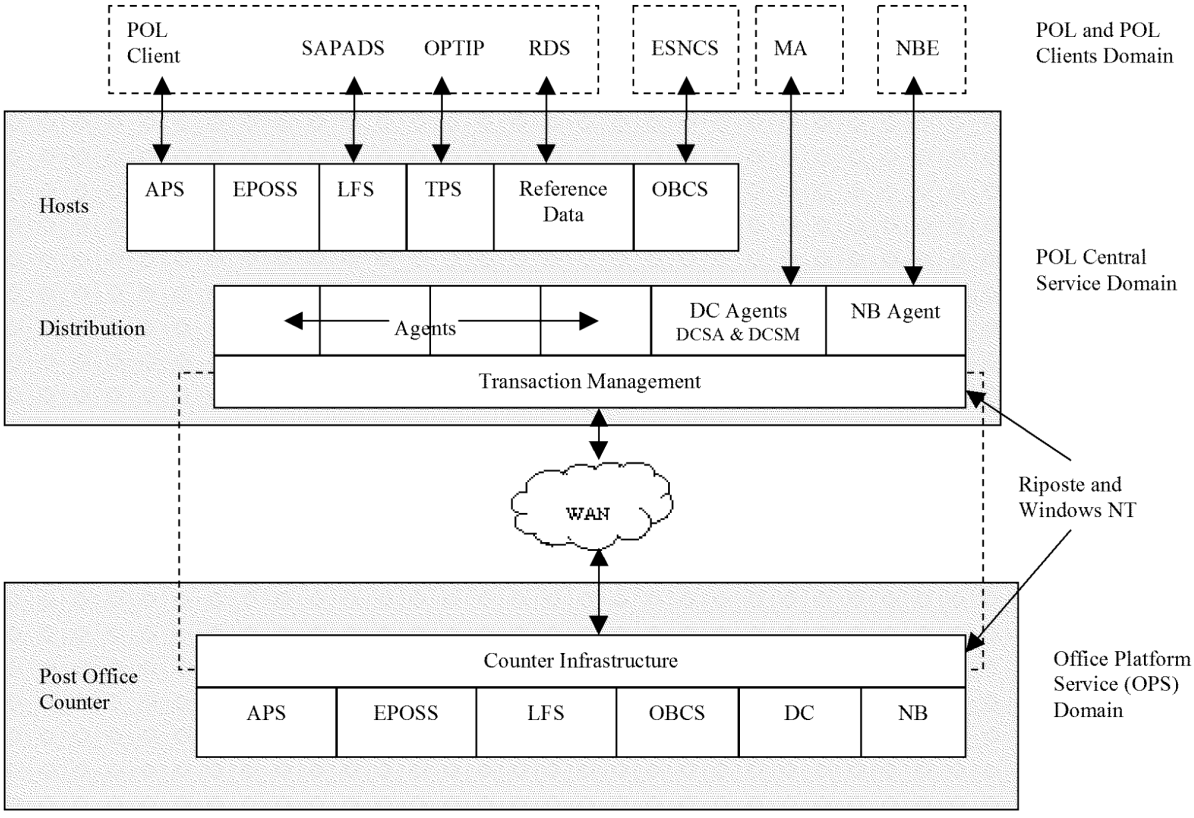

Figure 3.2 Post Office Ltd. Central Services and OPS Domains

As can be seen, the Post Office Ltd. Central Services Domain contains agents for each service provided at the Post Office counter. These agents provide the interface between Riposte and host systems.

FUJ00088068

Transaction Management Service (TMS) Agents assemble information from these hosts for distribution. The Correspondence Servers, which are the central part of the Riposte TMS, distribute the information to/from the Riposte journals at the Post Offices.

This domain includes the Key Management System used to generate and distribute keys within the Central Services Domain and to Post Offices.

The Central Service Domain spans two sites that are often referred to as Pathway's Data Centres or campuses.

The transaction management facilities provided by Riposte, including the Correspondence Servers and agents, run on Windows NT platforms.

The Post Office Ltd. Central Services Domain should not be confused with the Transaction Management Service (TMS). The Post Office Ltd. Central Services Domain is limited to the central Pathway sites, whilst TMS is defined to include the Riposte components that run on PCs within the Post Office Outlets.

The Order Book Control Service (OBCS) is, commercially, a Post Office Ltd. service, but data is exchanged over the unprotected Electronic Stop Notice Control System (ESNCS) link to the DWP.

The Network Banking Service (NBS) initially supports several On-line counter transaction types, each being initiated by the presentation of a bank card. Verification is via the use of PINPads or a visual check of customer signature by the Post Office clerk. There is no customer verification for deposits. Dedicated NB Agents within the POL Central Service Domain exchange data with the Network Banking Engine (NBE) over an encrypted link.

Debit Card MoP also supports several on-line counter transaction types, each being initiated by the presentation of a bank card. Verification is via a visual check of the customer signature by the Post Office clerk. Dedicated Agents within the POL Central Service Domain exchange data with the Merchant Acquirer (MA). Payment files are exchanged over an encrypted link.

3.3 The Office Platform Service Domain

The OPS Domain encompasses all Post Office sites as illustrated in figure 3.2. The applications, that run on Windows NT workstations, support the:

- Electronic Point of Sale Service (EPOSS) including Debit Card Service (DCS),
- Automated Payment Service (APS),
- Logistics Feeder Service (LFS),
- Order Book Control Service (OBCS) and
- Network Banking Service (NBS).

Reference data, sourced mainly from Post Office Ltd, is distributed to the target applications in the OPS domain. Validation procedures (specified in section 8.1) and CRC based integrity checks are incorporated.

Cryptographic mechanisms are used to protect hard disks within the OPS Domain. Filestore encryption and the associated key management facilities are described in section 10.0.

FUJ00088068

3.4 Post Office Ltd. and Post Office Ltd. Clients Domain

The Post Office Ltd. and Post Office Ltd. Clients Domain contains the Horizon system components that provide the interface with Post Office Ltd. and Post Office Ltd. Clients.

Pathway provides Post Office Ltd. Transaction Information Processing (TIP) system with records of all transactions at Post Office Outlets. The associated Post Office Ltd. system, which shares the TIP link, provides reference data for the applications.

Post Office Ltd. Automated Payments (APS) system, which processes payments on behalf of Post Office Ltd. Clients, uses direct links from the Pathway Data Centre to each of the Post Office Ltd. Client systems.

The Network Banking Engine (NBE) interfaces with the external Banking infrastructure.

The Debit Card Authorisation Agent and Debit Card Manager, in the POL Central Service Domain interfaces with the Merchant Acquirer for all DC Transactions.

3.5 System Management Service Domain

The System Management Service (SMS) Domain contains the central elements of the System Management (SM) and Network Management System (NMS) facilities.

By their very nature SM and NMS are potentially system wide since all components of the system need to be managed. It is, however, consistent to include an SMS Domain to identify the centre of control for SM and NMS.

The Horizon System Help Desk and System Management Centre (SMC) Help Desk are within the SMS Domain.

3.6 Pathway Corporate Services Domain

The Pathway Corporate Services domain supports Pathways own management processes. The domain encompasses the Data Warehouse and Pathways managed services as illustrated in Figure 3.3

FUJ00088068

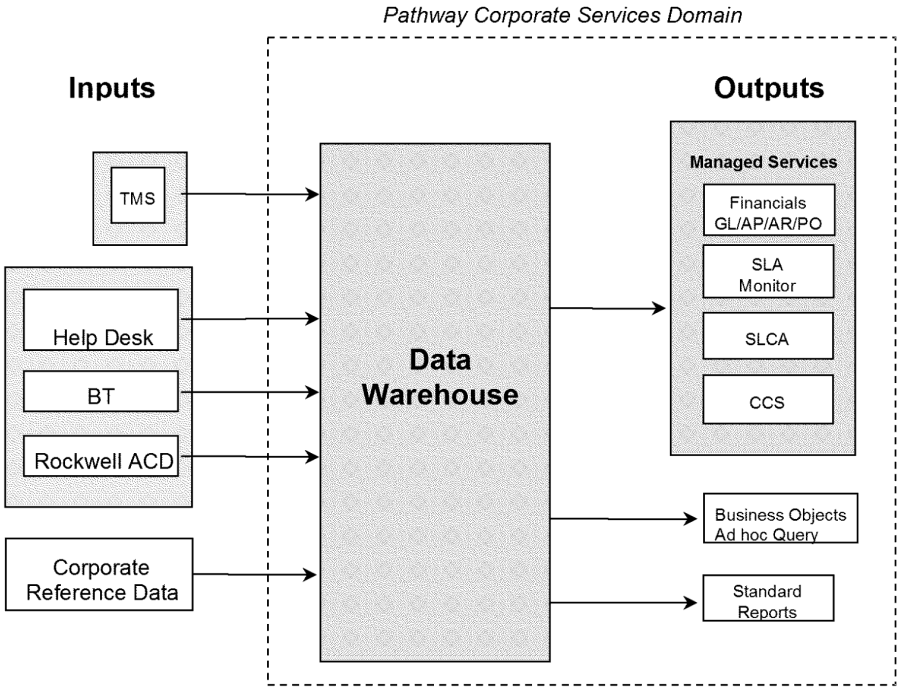

Figure 3.3 Pathway Corporate Services Domain

Inputs to the Data Warehouse, from the operational system, are provided by TMS, SMC and Help Desks.

Pathway's CS Management Service Unit, use the aggregated information stored within the Data Warehouse. The information is used to assist in reporting on the operational system, accounting and monitoring of service levels.

The SLAs produced by the Data Warehouse only get updated overnight, the SMDB was introduced to meet the requirement for detecting more immediate problems in meeting SLAs. The SMDB is placed in a DMZ to block any form of access from the Pathway Corporate LAN to the Data Centre.

FUJ00088068

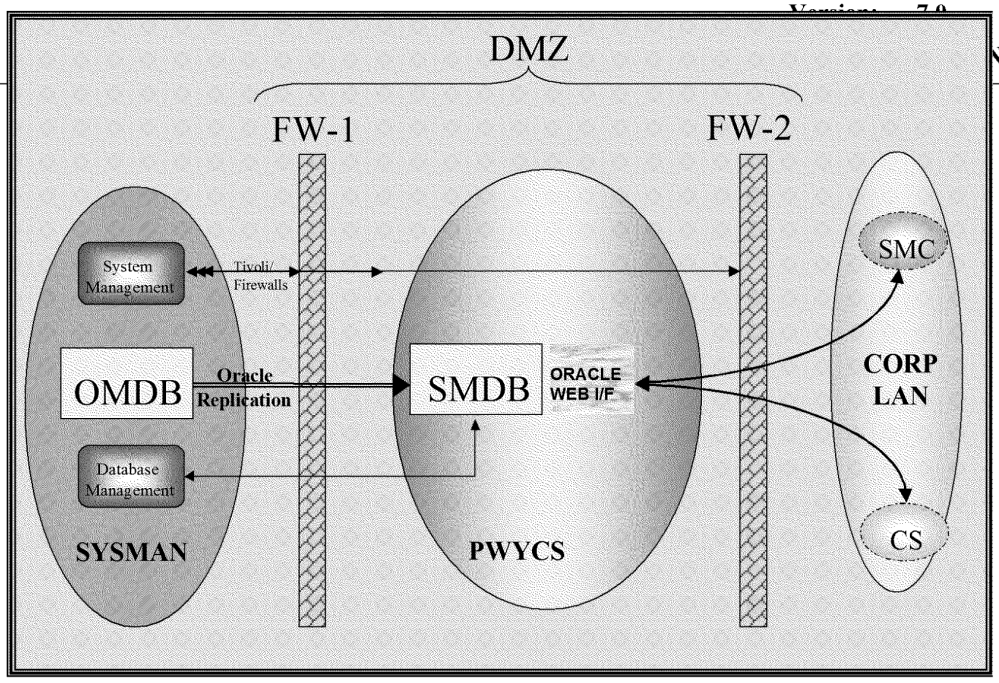

Figure 3.4 Service Management DMZ.

The DMZ is formed by using two separate firewalls. Oracle Web Server 1.0.2 is used for the Web Server on the SMDB.

FUJ00088068

4.0 Security Components

4.1 Security Enforcing Components

The security enforcing components within the Horizon system are:

- Windows NT Workstation and NT Server,
- Dynix operating system (on Sequent platforms),
- Solaris operating system (on Sun platforms),
- SecurID tokens and associated ACE/Agent and ACE/Server,
- Oracle 7 & Oracle 8i database products,
- Riposte (see below),
- Networking components (including firewalls and routers),
- Encryption devices, and
- Virus protection products,
- MS SQL Server 2000,
- Web Servers.

For NBS these are supported by:

- Replay protection for PINs, and
- Sensitive Card data and PIN protection.

For DC these are supported by:

- Encryption of Sensitive Card data protection up to the DC Authorisation Agent.

APS Smart Cards, NBE and DC also use Digital Signatures.

Riposte is a security enforcing component whenever it is configured to handle user authentication [TED]. The overview of Riposte, in section 4.6, highlights the security implications of Riposte components.

FUJ00088068

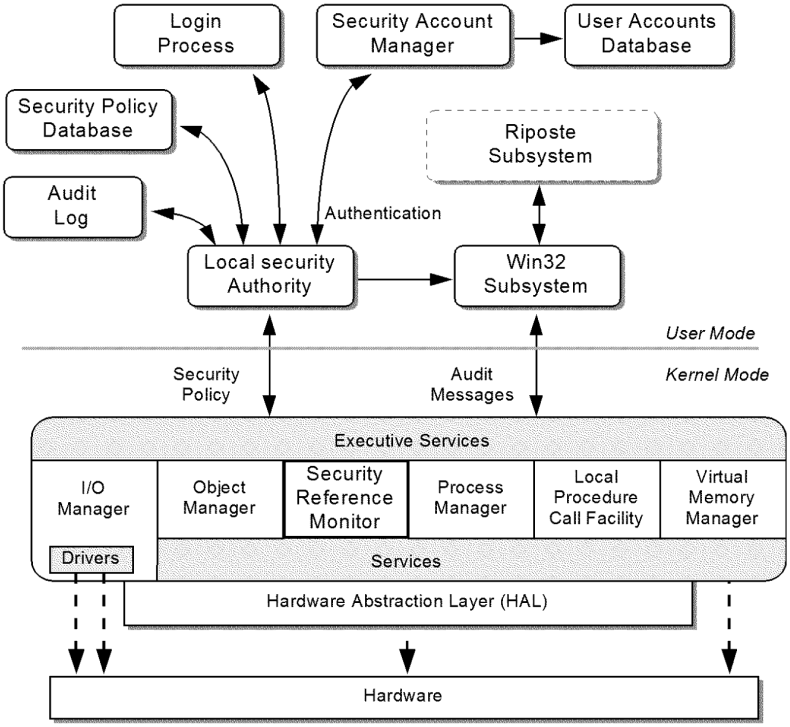

Figure 4.1 Windows NT Security Components

4.2 Operating System Security Functionality

Windows NT is used as the operating system for workstations and most servers.

Pathway also uses two proprietary operating systems based on UNIX:

- Sequent's Dynix operating system, and
- Sun Microsystems Solaris operating system.

4.2.1 Windows NT Security Functionality

Microsoft's Windows NT Workstation and Windows NT Server have security functionality that can be described as ITSEC F-C2 [ITSEC].

4.2.1.1 Pathway use current stable supported version(s) of Microsoft's Windows NT products updated with the appropriate (proven) Microsoft Service Packs.

4.2.2 Dynix Operating System

Sequent's DYNIX/PTX operating system is an enhanced version of UNIX developed for the Symmetry series of multiprocessing systems.

Sequent Host Central Servers are used to run the principal business applications and associated Oracle databases.

Sequent Data Warehouse Servers act as a repository for a large amount of financial and service-related information, which is used principally for Pathway's internal business purposes.

FUJ00088068

4.2.2.1 Pathway use the current version(s) of DYNIX/PTX.

4.2.3 Solaris Operating System

Sun's Solaris operating system is used on servers in each campus, running HP OpenView and Cisco Works to manage the Routers, Hubs and other network equipment.

4.2.3.1 Pathway use the latest industry approved version(s) of Sun's Solaris operating system.

4.3 Database Management Systems

Oracle V7 and 8i are used to support the databases used by the host applications running on Sequent servers. Oracle products used include the Oracle Relational Database Management System and SQL*Net.

4.3.1.1 Pathway use current version(s) of Oracle products.

4.4 SecurID Tokens and ACE/Server

SecurID tokens from Security Dynamics are used for identification/ authentication of privileged users, as specified in section 5.1.5.

Appropriate Windows NT workstations include an ACE/Agent that is automatically invoked during the authentication process to request a password and Personal Identification Number (PIN) number from the user. The PIN proves that the token belongs to the user.

Similar ACE/Agents are located on Sequent Dynix servers and Sun Solaris servers.

The ACE/Agent sends the password and PIN, suitably obfuscated, to an ACE/Server process running within the Authentication Server at the campus. This verifies the user's credentials, and returns a yes/no indication to the ACE/Agent.

4.5 Network Security

The Horizon solution incorporates five main components for enforcing network security:

- Firewalls (typically Firewall-1),
- Routers (Cisco and Nokia products),
- Post Office link components (VPN and ISDN adapter),
- Encryption devices (incorporating Rambutan or other commercial algorithm), and
- Cryptographic services incorporating for example either Red Pike, or DES or 3DES algorithms.

4.5.1 Firewalls

Firewalls are used to protect the Horizon system from:

- unauthorised access via external networks, and
- other local networks collocated at Pathway sites.

FUJ00088068

Protection is provided by a combination of packet filtering functionality within router components and application level firewalls.

Control of access to these components is specified in section 6.7.

For Network Banking and the need to access the Network Banking Engine (NBE), separate firewalls are introduced. A firewall De-Militarised Zone (DMZ) protects the Pathway Network Banking Agents from unauthorised access outside of the Data Centres. Two firewalls are employed and the traffic is 'Load Balanced' across them. RADIUS servers are employed in both Data Centres for Authentication and Accounting for all calls to and from the Post Office Outlets.

For DC, firewalls are used to mediate communications between the DCA and DCM in the POL and POL Clients Domain and the Merchant Acquirer.

4.5.2 Routers

The routers used are standard Cisco products and Access Servers.

Control of access to these components is specified in section 6.6

4.5.3 Post Office Outlet Link Components (VPN and ISDN Adapters)

This section considers Post Office Outlet links.

Specific security controls include:

- Virtual Private Networks (VPN), across all Post Office Outlet links - as described in section 8.6 (and also across the outlet LAN as described in section 8.5), and
- Call screening for Integrated Services Digital Network (ISDN) links - where a list of valid callers is configured in the central Router and all other calls are rejected. For call screening (on ISDN links) the list of valid caller information is subject to access controls and maintained using Tivoli.
- CHAP authentication performed by the RADIUS servers at each Data Centre. The RADIUS servers, introduced with metered and unmetered (FRIACO) network services for NB, hold all the CHAP user names and passwords for the live estate.
- CLI for inbound calls from Post Office Outlets to the Data Centres.

The use of VPN from Post Office Outlets to the Data Centres is independent of whether the connection is via the ISDN voice network or the Metered/Un-Metered (FRIACO) data networks. Data Centre communications with Post Office Outlets for software distribution and support access, utilise a Post Office Outlet 'dial back' to the Data Centre via FRIACO or RemoteConnect services. This function known as 'Call Reversal' is undertaken by CNIM on the Gateway PC at the Outlet. A reduced ISDN capability is also maintained in order to provide 'dial-out' in the situation where no FRIACO services are available to support existing Horizon services.

An ISDN adapter is installed in the gateway workstation at every Post Office location that uses ISDN.

FUJ00088068

The interface between Windows NT and the adapter is provided by a Network Device Interface Specification (NDIS) adapter that is supplied by EICON. The NDIS adapter provides the following security enforcing functionality:

- it only calls phone numbers that exist in the NDIS configuration data,
- it only passes network traffic at the IP level, and
- it protects the NDIS configuration information.

Where satellite is employed at Post Office locations for communications to and from the Data Centres, the ISDN adapter in the gateway workstation is replaced by a second Ethernet card. This second Ethernet interface connects via a cross-over cable to the Personal Earth Station (PES) which is the interface to the satellite Antenna at the Post Office Outlet. The VPN interface at the Post Office is 'bound' to this second Ethernet card as opposed to the ISDN adapter, thus maintaining full VPN functionality over the satellite link.

4.5.4 Encryption Devices

4.5.4.1 All NDIS configuration data is stored in the Windows NT Registry. Windows NT access controls and the filestore encryption (described in section 10.0) protects the files used.

The encryption devices in Pathway's solution are types ED600RTS and ED2048R3 supplied by Baltimore Technologies (formerly Zergo).

These devices are Certified products (ITSEC) and provide cryptographic protection using the CESG designed Rambutan crypto-kernel.

Encryption devices are utilised on Kilostream and Megastream circuits, where appropriate, to provide link-level encryption.

The use of encryption is specified, on a link by link basis, in section 8.0.

For the NBS, router encryption is operated on the WAN link between Horizon and the NBE. This utilises commercial algorithms.

For DC, router encryption is operated on the link between the Debit Card Manager and the MA. This utilises commercial algorithms.

4.5.5 Red Pike

Pathway uses a CESG approved implementation of Red Pike to provide the protection of selected links, as described in section 8.0.

The key management facilities used with Red Pike are implemented and used in accordance with CESG policy.

The Team Crypto product, used to protect Post Office Outlet filestore, also incorporates Red Pike, as described in section 10.0.

4.5.6 Commercial Encryption Algorithms.

Pathway uses commercial encryption algorithms (typically 3DES / 1024 bit modulus and RSA) for some elements of the NBS.

FUJ00088068

MACs and digital signatures are also employed where appropriate.

4.6 Riposte

Riposte (Retail Integrated Point of Sale Transaction Environment) is a message oriented middleware product designed to support distributed branch automation.

Riposte provides a 32-bit OLE based application development environment for use with Windows NT.

4.6.1 Riposte User Authentication

Within the OPS Domain, Riposte is configured to provide user authentication facilities in conjunction with the underlying Windows NT logon mechanisms. This is particularly useful at Post Office counters where it is desirable to present an easy to use user interface with minimal logon overheads.

Riposte is used to provide the Post Office user logon interface as specified in section 5.2.3 and [TED].

4.6.2 Riposte Messages

Riposte messages are self-describing, have a unique identity and are immutable. Message types include:

- transactions,
- enquiries and responses,
- audit (and monitoring information),
- authorisations,
- session context,
- application reference data, and
- system configuration data.

Messages can contain as much data as is required to describe:

- Riposte,
- audit information,
- security properties,
- system management information,
- system administration information, and
- application information.

When messages are created, standard message attributes are added by Riposte (including date, time, user and a cyclic redundancy check (CRC) code). Only Riposte can create messages and the message store is protected using Windows NT Access Control Lists.

Riposte Servers use Windows NT services for:

FUJ00088068

- configuration information - stored in the Windows NT Registry,
- error reporting via the Windows NT Event Log, and
- performance monitoring.

4.6.3 Riposte Message Servers

A Riposte Message Server is, typically, a Windows NT workstation or NT Server running the Riposte services.

A Riposte "group" is a domain in which messages are replicated to a set of message servers, which are uniquely identified by their Node Ids. A group normally consists of a set of units that are providing a common service in the same physical location (e.g. a Post Office Outlets).

Riposte provides peer-to-peer message replication that increases the resilience and reliability of the system. When a message is created, it is first committed in the local message store and then broadcast to all of the local neighbours. Other Riposte Message Servers, which receive broadcast messages, store them in local message stores, then forward them to other local neighbours who have not been sent the message. In this way, messages are propagated to all members of the group.

Message synchronisation is achieved using "marker" messages that are exchanged between Message Servers. This allows any messages, which may be lost or missing from its local message store, to be requested. The activity, which normally takes place across the LAN, is totally transparent to Riposte applications.

If a message store is lost, all messages are recovered from other members of the group. For a single terminal outlet, a dual disk configuration is used with fallback to the associated correspondence servers at the central site to provide secondary backup.

4.6.4 Riposte Correspondence Servers

A Correspondence Server is a Riposte message server that is a member of more than one group.

Correspondence Servers are used to provide:

- access to central systems,
- office backup and recovery, and
- distributed group extension.

4.6.5 Riposte Agents

Riposte Agents provide a service to a Riposte application or group of applications. They are also used to provide an interface between Riposte messaging environments and external systems.

Examples of how the Horizon system uses Riposte Agents include:

- transaction harvesting, and
- Riposte related system management activities.

FUJ00088068

The Riposte Agents used with Windows NT are multi-threading and use the NT event logging interfaces. They are configured to run as background processes that either run on demand or automatically as system services when the system is booted.

The type of each message defines the action to be taken by the Agent upon message receipt. The action(s) taken may:

- interact with an external system,
- retrieve information from the message store,
- update internal (volatile) state,
- update persistent state in the message store, and
- write response message(s).

When Agents are restarted, they co-ordinate recovery with external systems and restore their state information. Restart is automated by the System Management Components (described in section 13.2). Recovery includes processing messages that may have arrived when the Agent was down.

The use of Riposte Agents with Post Office Ltd. Clients, APS host(s) and TIP host(s) is illustrated in figure 3.2.

4.6.6 Riposte Communications

Riposte has a Remote Procedure Call (RPC) interface that may be called from any DCE compliant RPC implementation. This enables applications on other platforms (e.g. UNIX or Sequent's Dynix) to be integrated.

Riposte communications are based on a connectionless, best-effort messaging model.

The User Datagram Protocol and Internet Protocol (UDP/IP) are used to provide high performance communications. The Sockets implementation of UDP/IP, provided by Windows NT, is used.

4.6.7 Riposte Desktop

Each Riposte user application:

- runs (Desktop.EXE) on a Windows NT Workstation,
- contains and manages Riposte visual components,
- is integrated with RetailBroker, Peripheral, Validate, and TRState,
- provides session mobility (with stateless applications), and
- has a modular structure (using DLLs for each application).

The Riposte Desktop System incorporates several Dynamic Link Libraries (DLL) that are used for:

- transactions and Riposte services (RetailBroker.DLL),
- session mobility and logon/logoff (TRState.DLL),
- peripheral device handling (Peripheral.DLL), and

FUJ00088068

- input validation (Validate.DLL).

4.7 Virus Protection

This section considers the threat of virus infection and identifies the components needed to provide an appropriate level of protection. Viruses in this context includes all malicious software including network worms, logic bombs and Trojan horses.

4.7.1 Threat of Virus Infection

The threat of virus infection in most parts of the Horizon system is relatively low since:

- tightly controlled Windows NT configurations are used throughout the Office Platform Service Domain,
- floppy disk drives cannot be used within Post Offices,
- there are no E-mail connections to external systems,
- MS Office documents (including any documents/files that could contain macro virus) are not normally imported,
- operational files transmitted by file transfer contain data rather than executable code, and
- the main processing platforms are Unix based.

There is, however, a need to protect against the introduction of viruses from the following external sources:

- executable files introduced for maintenance purposes, and
- HTML documents containing user Help information.

4.7.2 Virus Protection Measures

Virus protection relies upon adherence to the security procedures defined in [SECPRO] and the measures supported by the Horizon system.

4.7.2.1 All workstations running Windows, except those within the Office Platform Service Domain, have virus protection software installed.

4.7.2.2 All workstations used to import executable code, destined for any Windows platform, have virus protection software installed.

4.7.2.3 The “import” of executable code shall normally be from external sources (e.g. floppy disk) into the System Management Service Domain. This enables virus checked software to be distributed throughout the Horizon system (e.g. to PCs located in Post Offices) over the network without requiring the recipient PCs to run further virus checks.

4.7.2.4 All executable code is virus checked prior to being imported into any part of the Horizon system.

FUJ00088068

4.7.2.5 All files susceptible to macro or related viruses (including HTML files), for which virus checks are feasible, are checked for viruses prior to being imported into any part of the Horizon system, by whatever route.

4.7.2.6 Anti-virus software is maintained by installing current upgrades, as they become available.

4.7.2.7 Selected workstations are fitted with logical and/or physical floppy drive locking mechanisms to prevent the unauthorised physical introduction of malicious software.

4.7.2.8 Protection is enhanced and extended for NBS with the installation and appropriate configuration of NBS-dedicated firewalls at the interface between the NBE and each Data Centre.

4.7.2.9 Protection is enhanced and extended for DC with the installation and appropriate configuration of DC-dedicated firewalls at the interfaces between the MA and each Data Centre.

4.7.2.10 As an additional safeguard, Pathway ensures that the Horizon system has adequate facilities for recovery in the event of a virus being detected.

4.8 MS SQL Server 2000

MS SQL Server 2000 runs on NT Servers and is accessed from clients running on NT Workstations. MS SQL Server 2000 has three modes of Authentication, namely Standard, Mix, and NT Authentication. The NT Authentication mode should be used.

4.9 Web Servers

The http protocol is used for Web Servers, this allows access to text usually in HTML format. Basic authentication is defined within the http protocol, however the user id and password are only encoded using Base64 encoding, this can easily be converted back to plain text, the authentication information is sent as part of the request every time a GET request is sent to the Web Server. All traffic to and from Web Server is text, where binary data is transferred this is Base64 encoded to produce a text string. The traffic between the Web Client and Web Server can be encrypted using SSL (https protocol).

The Web Server used in accessing the SMDB and OMDB databases is Oracle Web Server version 1.0.2 this does not support SSL.

4.10 Business Objects

Business Objects is an OLAP reporting tool that is used both for producing standard and ad-hoc reports from the Data Warehouse and from OCMS databases.

Business Objects includes security functionality allowing the grouping of Business Objects Users, however this is dependent on the information being stored in the repository. Business Objects Users may be assigned passwords, in order to allow the user to change the password, that user requires update access to the table containing the password, which contains all the other user's passwords.

FUJ00088068

4.10.1.1 Business Objects should not be relied upon to provide security and access controls alone. Use within Horizon is limited to specific authorised users and supported by NT access controls.

4.10.2 Business Objects and Oracle databases

When Business Objects accesses an Oracle database it is under a configured database user id not under either the users regular NT User id or Oracle User id.

4.10.2.1 Business Objects user should be granted only select access to database tables / views.

4.10.3 Business Objects and MS SQL Server databases

MS SQL Server should be configured to use integrated security (NT Authentication). Business Objects allows not only access to defined reports but also allow users to select other databases, and execute SQL commands on those databases.

MS SQL Databases should not rely on the front application to provide security.

FUJ00088068

5.0 Identification and Authentication

5.1 Identification and Authentication Requirements

Identification and authentication mechanisms are required to ensure that all users are uniquely identified, with only authorised users being granted any access to the system.

Reliable identification and authentication is essential in order to:

- provide the basis for access control decisions, and
- ensure that all users are individually accountable for their actions.

Authentication is based upon the information received, so the Horizon system protects both:

- the collection of authentication data, and
- the transmission of authentication data.

Particular attention is focused upon users situated in any remote location because these can represent higher risks to the system.

5.1.1 User Identification

Identification is the means by which the user provides their identity to the system. This can be based upon a combination of what the user knows (a User Id), what the user possesses (a smart card or other token) or some biometrics characteristic of the user.

5.1.1.1 All users are allocated an identifier (User Id) by which they are known to the system.

User Ids shall be unique within the scope of that part of the system. For example, the Post Office Manager would set up and maintain the User Id information for each counter clerk within that Post Office, using the Riposte application interfaces provided.

5.1.1.2 An individual's User id is sufficient to trace the identity of the person who has been authenticated.

In exceptional cases, where the same User id is used for infrequent access by users in particular roles, additional information is recorded to maintain traceability. This applies, for example, to Post Office Ltd. Auditors who are required to authenticate with the Help Desk before getting a one-shot password.

5.1.1.3 The Horizon system does not allow (normal) users to change their User Id.

The aim is to ensure that "users" remain individually accountable. It is, however, recognised that for very privileged users this might be difficult (or unrealistic) for the system to enforce. Procedural rules and auditing are used to provide additional controls that support this objective.

5.1.1.4 The format of User Ids depends upon the platform(s) used and the server used for authentication.

FUJ00088068

In all cases, the procedures used by Pathway [SECPRO] provide guidelines to cover operational aspects, including:

- the allocation of User Ids to individuals,
- selective removal of User Ids from the system, and
- constraints on re-allocation of User Ids to other personnel.

5.1.1.5 The system distinguishes between identification information (User Ids) and authentication data (including passwords).

5.1.1.6 The security of the system does not rely upon the secrecy of any User Id information.

5.1.2 User Authentication

Authentication is concerned with establishing the validity of the user's claimed identity. It increases confidence that the claimed identity is the right one for the user.

5.1.2.1 All users are authenticated before any access is granted to the Horizon system.

Human users, therefore, complete the logon sequence before they are able to invoke any other actions.

5.1.2.2 Users are allowed a predetermined number of attempts to logon, as specified in [ACCPOL]. After this number is exceeded the user's logon facility is disabled.

Other action taken upon failure to logon are configurable from the following options:

- an alarm message shall be raised,
- logon failure will be recorded in the audit track, and
- an application level audit message will be generated.

In all cases the logon failure will be recorded.

5.1.2.3 Following logon failure, the user's logon facility will be reset by:

- positive action by the system manager, or
- expiry of a timeout period.

The optional timeout facility will only be available within the Office Platform Service Domain. The configuration of this facility, including the time between retries, is specified in [ACCPOL].

5.1.2.4 During logon, the responses provided by the system to the user shall be simple messages reporting success or failure. No reason is given in the event of logon failure.

5.1.2.5 On successful logon, the system displays the date and time of the user's last successful logon at Post Office outlets.

FUJ00088068

5.1.2.6 Within each Post Office Outlet, users will not be able to run more than one counter PC with the same user identity.

A subsequent logon at a second PC will cause Riposte to terminate the users previous session and transfer use to the new counter position.

5.1.3 Passwords

Human users and system/process users use passwords. This section defines the requirements for all passwords, whilst the additional requirements specified in section 5.1.4 apply only to passwords used by human users.

5.1.3.1 The Horizon system is not required to provide automated generation of passwords.

5.1.3.2 The format of passwords depends upon the platform(s) used and the server used for authentication.

In all cases, the procedures used by Pathway [SECPRO] provides guidelines on the use of passwords, including:

- the allocation of new passwords,
- appropriate choice of replacement passwords,
- the need to avoid disclosure of passwords, and
- the frequency and timing of password changes.

5.1.3.3 The system uses volatile memory for operations associated with password checking. For Pathway specific code, when the checking is completed all “in clear” password information is overwritten.

Ideally, all “in clear” password information should be overwritten after use but the use of COTS products and standard applications may dictate that this can not be achieved or verified.

5.1.3.4 Passwords will never be visibly displayed by the system.

5.1.3.5 Passwords will not be transmitted “in the clear” to or from any location outside the central Pathway sites unless they are one-shot passwords.

5.1.3.6 Passwords will not be transmitted “in the clear” within Pathway sites unless the link used is entirely within a physically protected area (e.g. Campus sites) and a risk assessment has indicated that the residual risk is acceptable.

5.1.3.7 All Routers are configured in the mode that ensures that password information is stored in encrypted format.

5.1.4 Human User Passwords

The requirements specified in this section apply only to passwords used by human users.

FUJ00088068

After an initial password has been issued, the choice of passwords is the responsibility of individuals.

5.1.4.1 An initial password is made known to each individual. The system marks these initial passwords as expired.

As this password is known by more than one person, the user is forced to change the initial password before other options can be selected. This mechanism also applies to any passwords reset by a third party.

5.1.4.2 An appropriate one-way algorithm is used to encrypt password information used by human users, before storage or transmission.

5.1.4.3 All users have the ability to change their own password (without requiring intervention from a supervisor or Post Office Manager).

Password change interfaces are expected to depend upon platform type (e.g. Dynix and Windows NT will differ) but in all cases the user will complete the logon sequence before initiating a password change. The change sequence will also require the old password to be correctly quoted.

5.1.4.4 The OPS provides facilities to enable the Post Office Manager to establish new users and set an initial password for each user in their Post Office.

5.1.4.5 If a user forgets their password the Post Office Manager is able to reset the password.

5.1.4.6 For situations where the sole user (e.g. Post Office Manager in a single counter office) has forgotten his password, a secure backup procedure is used.

5.1.5 Use of Tokens

The Horizon system only use tokens when the protection provided by passwords alone is not considered to be sufficient. In general, token use is limited to system management personnel and management operations conducted from or on remote sites, as defined in [ACCPOL].

5.1.5.1 Tokens are allocated to named individuals for their sole use.

In certain circumstances (e.g. fourth line support,) a card may be “assigned” to an individual for a limited period. In such cases, a full audit trail of such cards is retained.

5.1.5.2 The identity of users who have been issued with tokens is made known to the system and the authentication processes enforce their use.

5.1.5.3 The system is capable of selectively revoking the validity of tokens.

5.1.5.4 Smart tokens are used in all cases where a password alone is not considered to be sufficient. The user is obliged to prove that he/she possesses the token at the time of logon.

FUJ00088068

Tokens that generate a one-time password, thereby protecting against password replay, is used.

5.1.5.5 Each token has an associated Personal Identification Number (PIN) that is used to activate the device, as defined in [ACCPOL].

5.1.5.6 Personnel who are authorised to access the Horizon system from remote locations are required to identify themselves using hand held tokens.

This group comprises selected system administrators authorised to use remote access for system management activities.

The Pathway Headquarters site is categorised as being a "remote location". Pathway personnel who require access to the operational system and/or Data Warehouse are required to use tokens.

5.1.5.7 Personnel who are authorised to access the Horizon system using UNIX root privilege are required to identify themselves using hand held tokens.

5.1.5.8 Personnel who are authorised to access the Horizon system as a database administrator (DBA) are required to identify themselves using hand held tokens.

5.2 Authentication of Windows NT Users

5.2.1 Authentication Methods

Windows NT [WINNT] is used as the base operating system for:

- platforms within the Post Office Ltd. Central Services Domain,
- workstations within the Office Platform Service Domain, and
- servers within the Post Office Ltd. and Post Office Ltd. Clients Domain.

The standard Windows NT logon mechanisms (outlined in section 5.2.2) is used for users in all domains listed above, except the Office Platform Service (OPS) Domain. Users in the OPS Domain, which includes all Post Office staff, use a simpler interface provided using Riposte (as described in section 5.2.3).

In both cases:

5.2.1.1 Information used to authenticate users is protected by the authentication mechanisms used.

5.2.1.2 All users are named individuals with their own password.

All account information associated with Guests are disabled or, where possible, removed entirely.

Removal of other generic Windows NT users (namely System and Administrator) can result in installation problems. These users will, therefore, be retained for System Management purposes but are subject to additional controls, as defined in [ACCPOL[.

FUJ00088068

5.2.1.3 The standard Windows NT password algorithm is used.

5.2.2 Standard Windows NT Logon

The Windows NT logon process is illustrated in Figure 5.1. For users in domains (defined in 5.2.1) that use this form of logon:

5.2.2.1 The trusted logon process (as illustrated in figure 5.1) is used to authenticate users, based upon their User Id and password.

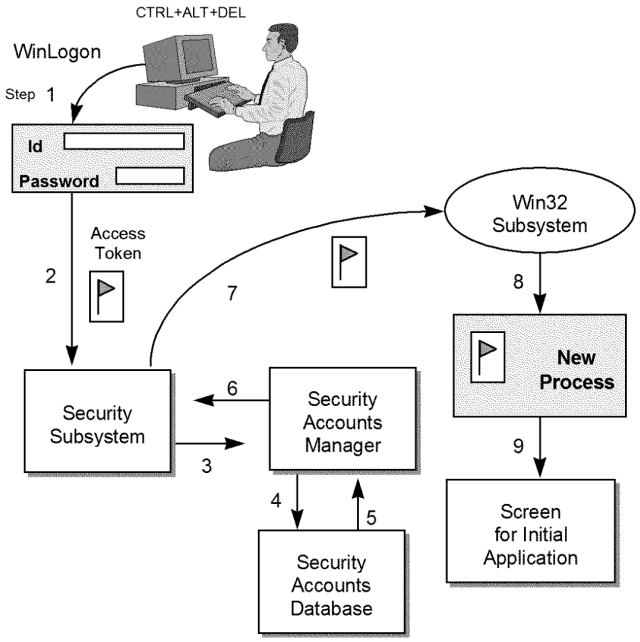

Figure 5.1 Windows NT Logon Process

5.2.2.2 The logon process is reliably initiated by the user invoking a trusted communication path (from the user to the system).

Windows NT users use the combination Ctrl+Alt+Del to invoke this trusted path.

5.2.2.3 Windows NT requires each user to change their password periodically. The initial change is required the first time the user logs on and subsequently as defined in [ACCPOL].

The exact interval is configurable and depends upon the user's role and location.

5.2.2.4 The Windows NT Account Policy controls are used to set parameters, in accordance with [ACCPOL], including:

- password expiry period,
- minimum password length,
- minimum password age (before change),
- remember password history (number of passwords per user),

FUJ00088068

- number of consecutive failed logon attempts before lockout, and
- whether to reset logon count after a delay period (see 5.1.2.3).

5.2.3 Logon at Post Office Outlet Locations

To reduce logon overheads and improve operational efficiency, the logon user interface used throughout the OPS Domain uses Riposte desktop facilities [TED] rather than the native Windows NT interface.

This does not imply that the Windows NT Registry is not used.

5.2.3.1 All authorised users have individual User Ids (allocated by the Post Office Manager) and passwords that are held in the Windows NT Registry for that Post Office Outlet.

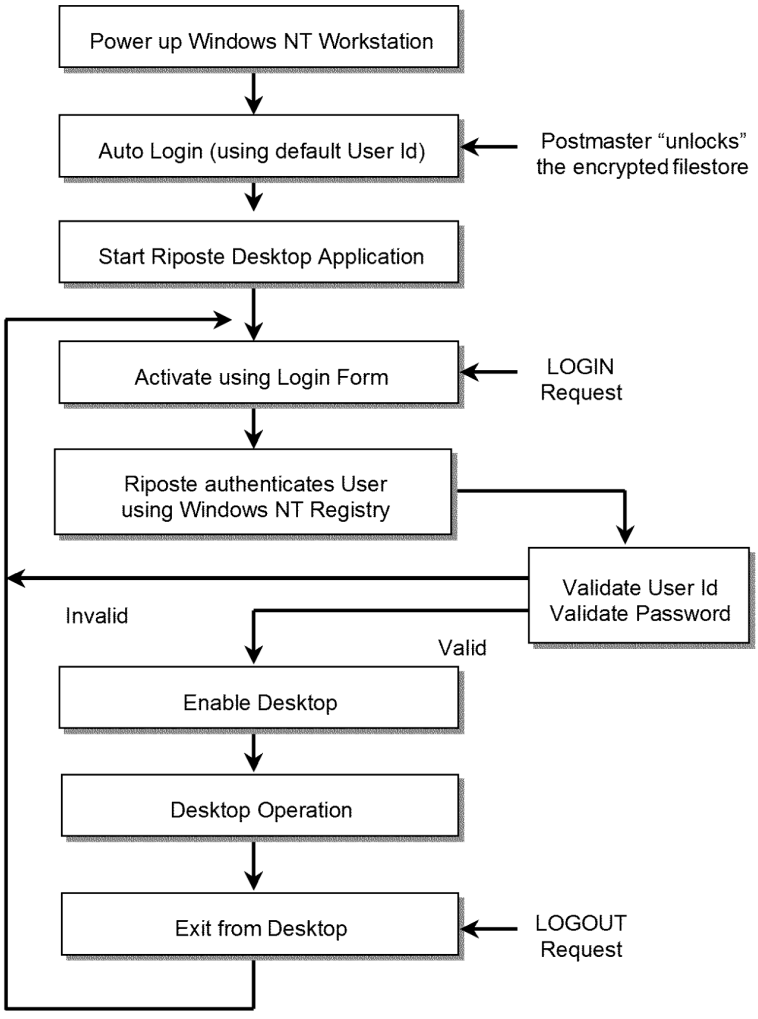

Figure 5.2 Logon Sequence at Post Offices

The logon sequence used is illustrated in figure 5.2. For simplicity, filestore encryption logic (described in section 10.0) associated with initial power up is not shown.

FUJ00088068

When the Windows NT workstation is powered up, the Windows NT facility for automatic logon is initiated instead of the normal manual NT user logon sequence. This enables a dummy user with username (u1) and password (p1). The first security check is then forced by automatic entry into a Post Office Manager's (POM's) authentication protocol, which requires the POM to authenticate using his/her Memory Card and associated PIN in order to continue the boot up sequence and unlock encrypted filestore.

5.2.3.2 Facilities that enable the automatic logon to be bypassed, to give access to a standard Windows NT logon, is disabled.

In particular, the booting of Windows NT is not interruptible.

On completion of the automatic logon, the Desktop process is entered automatically. Once the Desktop process has completed loading and Initialisation, the Desktop displays a User logon form.

This Desktop user logon is integrated with Windows NT. A successful logon requires the username and a one way hash of the password to be valid within both Riposte and Windows NT.

Once the Desktop user logon has been completed successfully, the user can execute applications within the Desktop.

It is important to note that the Desktop process runs within the security context of user u1. However, the Desktop process does not access files directly, but acts as a Client to the Riposte service that is running under a privileged user u3. When the Desktop calls on the Riposte service to perform a function (such as write a message to the Riposte message store), the Riposte service 'impersonates' username u2, the Desktop username (provided by the real user).

Impersonate is an NT term defined in the Microsoft Developer Studio, Visual C ++ version 4.2 as:

"Impersonation is the ability of a thread to execute in a security context different from that of the process that owns the thread. Typically, a thread in a server application impersonates a client. This allows the server thread to act on behalf of that client to access objects or validate access to its own objects."

When the user logs off from the desktop, the desktop logon form is displayed whilst the desktop remains active in the security context of username u1. This allows the Post Office user to subsequently logon without incurring the delay arising from loading the desktop.

5.3 Authentication of Oracle Users

Oracle DBMS products [ORACLE] support two methods for user validation, namely:

- authentication by the associated Oracle database, and
- authentication by the operating system.

5.3.1.1 Oracle is used to authenticate all database users in the operational Horizon system.

FUJ00088068

5.3.1.2 The Sequent Dynix operating system, which provides the platform for Oracle, is used for authentication of all Operational Support users (e.g. Security Manager) in the operational Horizon system.

5.3.1.3 Database access from the Post Office Ltd. Central Services Domain is provided by Riposte Agents running on Windows NT. Each agent is associated with a Port (or multiple Ports) on the Sequent machine.

The default IP port for SQL*Net connects to Sequent. Normal Oracle id/password/role authentication applies.

5.3.1.4 The database authentication is supplemented when client applications are used, adding password ageing and maintenance.

5.4 Authentication of Post Office Ltd. Staff

Mechanisms are provided to enable the Post Office Manager to verify his/her identity when making requests to the appropriate Help Desks. This ensures that significant requests, including all changes to the system, are only accepted from authorised personnel.

The mechanisms needed to authenticate Post Office Ltd staff are described in the respective Help Desk Processes and Procedures Description (PPD). Horizon representatives have agreed these PPD documents.

5.5 Authentication of MS SQL Server Users

MS SQL Server should be configured to use NT Authentication. Users are required to authenticate a second time, Windows NT using the users existing credentials handles this authentication seamlessly.

5.5.1.1 MS SQL Server 2000 should be configured to use integrated security.

5.5.1.2 MS SQL Server 2000 should be configured to use encrypted passwords.

5.5.1.3 MS SQL Server 2000 should have the password for the built-in user “sa” set.

5.5.1.4 MS SQL Server 2000 should not use the built-in ‘Guest’ user in any databases.

5.6 Authentication on Web Servers

A Web Client access to a Web Server is authenticated on each individual document/CGI Script being accessed. The normal default is normally for no authentication to be performed.

5.6.1 Basic authentication

The http definition includes Basic Authentication, the transmission of the user id and password is in B64 Encoded. The initial http GET/POST request from the Web Browser fails returning an error; this causes the browser to display a login request. The Web Client then repeats the same GET/POST request followed by an authentication header field containing the authentication details which are Base64 encoded. On all subsequent GET/POST requests the Web Browser sent is followed by the authentication header field and encoded details.

FUJ00088068

The Web Server verifies the authentication details, which is dependent on the Web Server, Operating System and configuration.

5.6.2 Oracle Web Server 1.0.2

The Authentication can be configured for the Oracle Web Server.1.0.2 the method of Authentication provided, has user id and passwords held in plain text within the configuration file, excludes using plain text for storing passwords.

When accessing the Oracle RDBMS database via the Web Server the CGI program performs the authentication, this can use the Oracle RDBMS to provide the authentication.

5.6.2.1 Where authentication is required for browser access to the Oracle RDBMS the Oracle Web Server should be configured to use the Oracle RDBMS for user authentication.

5.6.2.2 The Oracle Web Server should not hold passwords in control files.

The Oracle Web Server 1.0.2 should only be used to give access to non-sensitive data.

FUJ00088068

6.0 Logical Access Control

6.1 Access Control Requirements

There are three aspects to access control:

- Authorisation - determining which subjects are entitled to have access to which objects,
- Access rights - determining the combination of access modes permitted (e.g. read, write, execute and delete), and
- Enforcement - of the access rights.

This Security Functional Specification considers the access rights that are supported by system components and the ability of the system to enforce access rights. The topic of authorisation and assignment of rights to individuals is addressed in the Access Control Policy [ACCPOL].

6.1.1 Access Control Policy

Pathway's Access Control Policy identifies all users who are authorised to access any part of the system and the access rights permitted.

For practical reasons, the Access Control Policy is expressed in terms of roles rather than named individuals. All users are associated with one or more roles so that all persons are individually accountable for their actions.

6.1.1.1 Pathway's Access Control Policy identifies all roles associated with the system and defines the access rights that are to be granted to each user acting in that role.

6.1.2 Privileges and Roles

Users of the operational Horizon system carry out their duties in a variety of roles, including system administrator, database administrator, help desk advisor, Post Office counter clerk and maintenance engineer.

Users require certain privileges in order to perform their allotted tasks. The privileges associated with each role will, therefore, be sufficient to allow all tasks associated with that role to be performed whilst not providing any additional capabilities.

6.1.2.1 Pathway applies the principle of least privilege when assigning privileges to roles and users.

6.1.3 Separation of Duty Controls

Separation of duty controls is based upon Roles as defined in [ACCPOL].

Administrative and procedural controls are also defined within Pathway operational procedures.

6.1.4 Two Person Controls

Two person controls have been considered for system and database management operations but are not employed. They are however used extensively in key management.

FUJ00088068

6.1.5 Use of Discretionary Access Controls

Discretionary Access Controls (DAC) are used to provide resource owners with the ability to specify who can access their resources and the type of access permitted.

6.1.6 Control of Access to Files and Directories

Access to each file or directory is controlled by the owner of the object who is able to grant access rights to other users or groups of users. The types of access supported normally include Read, Write, Execute and Delete.

6.2 Control of Access to Databases

The three main ways of controlling access to the Oracle database facilities are by:

- being selective about the choice of potential users,
- ensuring that user authentication is effective, and
- defining profiles that limit the use of system resources.

6.2.1 Schemas and Users

Each Oracle database has a list of schemas that define collections of schema objects (including tables, views, clusters, and procedures).

Each Oracle database also have a list of valid database users. These users are permitted to access the database by running a database application (such as Oracle Forms, SQL*Plus, a precompiler etc) and connect to the database using a valid username defined in the database.

When a database user is created, a corresponding schema of the same name is created for the user. This schema defines the objects that may be accessed by the user, unless otherwise constrained.

Access rights of a user are determined by the security administrator who sets up the user's domain. These parameters specify:

- whether user authentication information is maintained by the database or the operating system (see section 5.3),
- resource limits, defined in a profile (see section 6.2.3), and
- the privileges and roles (see section 6.2.4) that provide the user with appropriate access to objects needed to perform database operations.

6.2.2 Changing User's Parameters

A user's security domain can be altered using:

- Oracle's Server Manager, and/or
- the SQL command ALTER USER.

Users are permitted to use these facilities to change their own password but other operations, which require additional privilege, can only be performed by the security administrator.

FUJ00088068

6.2.3 Profiles

The allocation of resource limits (e.g. CPU time) to individual database users is simplified by use of the default profiles. Limits found to be necessary are defined as the default wherever possible.

6.2.4 Oracle Privileges and Roles

The Oracle Database Administrator's Guide [ORACLE], which includes a lengthy section on Privileges and Roles, describes:

- system and object privileges,
- database roles,
- how to grant and revoke privileges and roles,
- how to create, alter, and drop roles, and
- how role use can be controlled.

A privilege is a right to execute a particular type of SQL statement or access to another user's object. It can be granted to users explicitly or can be granted to a role (as a named group of privileges) that are then granted to one or more users.

Within the Horizon system all privileges are associated with roles rather than being explicitly assigned to individual users. This provides more effective management control of both system privileges and object privileges.

6.2.5 MS SQL 2000 Privileges and Roles

The MS SQL Books provide details of Privileges and Roles.

The MS SQL Security Manager is used to administrate the NT Groups that can access MS SQL Server 2000.

The MS SQL Server Enterprise Manager, provides a GUI interface which can use used to assigned User/Group permissions to individual databases, tables, Views, columns, stored procedures and/or Triggers.

6.2.1.1 All demonstration databases should be removed.

The pubs database is always installed when MS SQL is installed, and allows guest user access.

6.2.1.2 The NT 'Everyone' group should not be granted database access.

6.2.1.3 The KMA is configured so that DB Admin and System Admin are kept separate.

6.3 Access Controls Supported by Windows NT

The following subsections identify the main access control facilities provided by Windows NT. For a more detailed explanation, the reader may refer to the standard Microsoft Windows NT documentation [WINNT].

FUJ00088068

The security functionality provided by the base Windows NT products is sufficient to meet the access control requirements on all NT Workstations and NT Servers within the Horizon system.

6.3.1 Configuration of Windows NT

Configuring Windows NT platforms to provide secure operation is quite complex. The underlying mechanisms are sound but the products, as supplied by Microsoft, have default settings that permit Guest users and do not adequately constrain access to objects.

Configuring each platform, in accordance with [ACCPOL] (see section 6.1.1), is essential.

6.3.1.1 Windows NT based platforms are configured strictly in accordance with [ACCPOL] prior to their installation.

6.3.2 Windows NT Access Control Lists

Windows NT [WINNT] supports Access Control Lists (ACLs) that identify the resource access permissions granted to users and groups.

6.3.2.1 Windows NT Access Control Lists are used to define permitted access to objects in accordance with [ACCPOL].

Wherever possible, ACLs will be defined in terms of roles rather than individuals to simplify system configuration.

6.3.3 Windows NT Tools Used to Control Access

Windows NT supports a number of tools that can be used to control access to resources (e.g. File Manager and Print Manager).

6.3.3.1 The ability to access Windows NT tools has been removed on the basis of roles, in accordance with [ACCPOL], prior to installation.

6.3.4 Windows NT File and Directory Access

The types of access associated with files and directories have been outlined, in general terms, in section 6.1.6

Appendix A explains how each type of access is interpreted in terms of Windows NT files and directories.

6.3.5 Windows NT Privileges and Roles

The use of Windows NT privileges and roles are defined in [ACCPOL].

6.4 Access Controls Supported by Dynix

Sequent's DYNIX/PTX operating system is an enhanced version of UNIX developed for the Symmetry series of multiprocessing systems.

FUJ00088068

6.4.1 Configuration of Dynix

The Dynix operating system components are configured in accordance with [ACCPOL].

6.4.2 Dynix Access Controls

6.4.2.1 The Sequent Dynix operating system, which provides the platform for Oracle, is used to support the access controls associated with the database (as described in section 6.2).

6.4.2.2 The Sequent Dynix operating system is used to control access to all input and output devices directly connected to Sequent platforms.

6.4.3 Dynix Tools Used to Control Access

Access to Dynix tools, notably those capable of being used to configure the access control mechanisms, is controlled in accordance with [ACCPOL].

6.4.4 Dynix File and Directory Access

The standard Dynix tools are used to configure the access control mechanisms provided by the operating system. These are configured in accordance with [ACCPOL].

6.4.5 Dynix Privileges and Roles

Dynix privileges and roles are configured in accordance with [ACCPOL].

6.5 Access Controls Supported by Solaris

Sun's Solaris operating system is a version of UNIX developed for use on Sun Servers.

6.5.1 Configuration of Solaris

The Solaris operating system components are configured in accordance with [ACCPOL].

6.5.2 Solaris Access Controls

6.5.2.1 The Sun Solaris operating system, which provides the platform for HP OpenView and Cisco Works, is used to support the access controls associated with system and network management services.

6.5.2.2 The Sun Solaris operating system is used to control management access to Routers, Hubs and other network equipment.

6.5.3 Solaris Tools Used to Control Access

Access to Solaris tools, notably those capable of being used to configure the access control mechanisms, are controlled in accordance with [ACCPOL].

FUJ00088068

6.5.4 Solaris File and Directory Access

The standard Solaris tools are used to configure the access control mechanisms provided by the operating system. These are configured in accordance with [ACCPOL].

6.5.5 Solaris Privileges and Roles

Solaris privileges and roles are configured in accordance with [ACCPOL].

6.6 Control of Access to Routers

6.6.1 Access Methods

Cisco provides four methods of access for controlling routers:

- Console access - using a terminal attached directly to the Router via a "control port" on the back,
- Telnet access - using a Telnet, run over IP, to provide a remote login,
- Simple Network Management Protocol (SNMP) access - using the SNMP protocol to configure the router and collect information, and
- Indirect - using the Trivial File Transfer Protocol (TFTP) to download configuration files from a configuration server.

6.6.1.1 Console access mode is not disabled by router configuration. In normal running, however, the routers will not have consoles attached.

6.6.1.2 Telnet access will only be permitted in exceptional cases, where more direct access to the routers is essential, as defined in [ACCPOL].

The Terminal Access Controller Access Control System (TACACS+) is used to authenticate all telnet users. Their actions are audited at the NMS.

6.6.1.3 SNMP access is used for remote system management of routers (as outlined in section 13.3.3)

6.6.1.4 Use of TFTP is controlled.

6.6.2 Privileged Mode Access

Provided that Console or SNMP mode of access is used (as defined in section 6.6.1) the use of privileged mode access can be controlled as follows:

- For a given user (or group of users), non-privileged and privileged access can be permitted. Non-privileged access allows users to monitor the Router but not configure the Router. Privileged mode allows the user to fully configure the Router.
- The access mode is enabled for Console access by setting up two types of password. The logon password allows non-privileged access to the Router. The user enters privileged mode by use of the enable command and an additional password.

FUJ00088068

- With SNMP access different community strings are used to distinguish between non-privileged and privileged access modes. Non-privileged access allows a host to send the Router SNMP get_request and SNMP get_next_request messages. Privileged mode allows the host to send the Router SNP set_request messages in order to change the Router's configuration and operational state.

6.6.2.1 Session Timeout values are selected to limit the period of time allowed for operation of a console in privileged mode.

6.6.3 Access Lists

Access List perimeters allow IP addresses to be specified along with protocols (IP, UDP, TCP and ICMP) and port numbers.

6.6.3.1 Access lists are used to define the actual traffic that is permitted or denied through a Router.

6.6.3.2 Only traffic associated with IP addresses that are explicitly defined in Access Lists are permitted.

6.6.3.3 Constraints associated with particular port numbers are defined as part of the network design.

6.6.3.4 Constraints associated with particular protocols are defined as part of the network design.

Access lists can be applied to specific interfaces and they can be used to filter packets before or after routing decisions are made. The use of input access lists can prevent specific address spoofing scenarios whereas use of output access lists only does not.

6.6.3.5 Input access lists are used to ensure that filtering is enforced before routing decisions are made. Outlet filtering is also used to ensure that valid Pathway packets are not exposed (to say TIP etc) when the same router is shared.

6.7 Control of Access to Firewalls

Firewalls are used to protect the Horizon system from unauthorised access via external networks and other local networks collocated at Pathway sites. Access Methods

Pathway firewalls are managed using Firewall Enterprise Centres, one at each Data Centre, as described in [ACCPOL]. These reside on Sun Solaris systems which provides access controls as specified in section 6.5.2.

6.7.1.1 All access to the firewalls is via the Enterprise Centre, except for hardware maintenance.

6.7.1.2 As for routers, firewalls should not have consoles attached, except for hardware maintenance purposes.

FUJ00088068

6.7.2 Access Lists

The parameters to an Access List allow IP addresses to be specified along with protocols (IP, UDP, TCP and ICMP).

6.7.2.1 Access lists are used to define the actual traffic that is permitted or denied through a firewall.

6.7.2.2 Only traffic associated with IP addresses that are explicitly defined in Access Lists are permitted.

6.7.2.3 Constraints associated with particular protocols are defined as part of the network design.

6.8 Control of Access to VPN Management Information

The VPN product includes a number of controls over the manipulation of policy and other sensitive control information.

6.8.1.1 Access to VPN policy and other sensitive control information is confined to named users.

6.8.1.2 Access to sensitive operations are confined to users with administrator privilege.

6.8.1.3 Access to the VPN policy file are limited, by the VPN product, to the standard VPN policy editor.

6.8.1.4 Access to the VPN policy editor is confined to nominated privileged users.

6.8.1.5 All VPN access control features are configured in accordance with [ACCPOL].

6.9 Web Server Access Controls

The Web Server runs under its own user id, there is the potential for the Web Browser to cause the execution of programs under this user id. Access Control should be used to limit this user id's access to the rest of the platform, preferably denying access.

6.9.1 Web Server documents

6.9.1.1 The Web Server document files that are to be accessed via the Web Server should be placed in a separate area from other files.

6.9.1.2 Only read access should be granted to Web Server document files by the Web Server user id.

6.9.1.3 Clients under a given role should be given access to documents according to the role.

FUJ00088068

6.9.2 Server side scripts and Programs

Most Web Servers allow scripts or programs to be executed on the server, CGI scripts or programs are supported by most Web Servers, ASP (Active Sever Pages) are supported in MS IIS.

These scripts or programs are executed either under the user id of the Web Server or in some cases the user's id.

6.9.2.1 The user id under which the Web Server executes should be given execute access only to run the Web Server, those CGI scripts, programs or ASP that are required.

6.9.2.2 Where possible CGI Script / Programs and ASP should be stored in separate sub-directories from other programs.

6.9.3 Web Server Database Access Controls

Web Servers can access databases such as Oracle or MS SQL using CGI scripts or ASP.

6.9.3.1 Roles on the Databases should include roles for Web Clients where a Web Server is given access.

6.9.3.2 A Role should exist on the Database for the Web Server Database user id.

6.9.4 Oracle Web Server 1.02 Access Controls

The Oracle Web Server is used to access the Oracle RDMBS, using a CGI program. There are no further specific access controls required.

6.10 External Support Access Controls

Specific controls apply in respect of external support of Horizon systems for diagnostic and maintenance purposes (e.g. by EMC, Sequent and Oracle). All requests for technical support are made via the HSHD and callers validated as defined in [ACCPOL]. Subsequent support is generally undertaken on site. All visitors are subject to identity validation and must be accompanied.

Where site visits are impractical (e.g. because of the urgency of the required diagnosis), remote access may be permitted subject to compliance with agreed network and procedural controls. These include:

- permitting access only by authorised staff from secure support outlets/environments;
- permitting access only by dedicated support client or link utilising authentication mechanisms to maintain confidentiality and integrity of the connection;
- changing relevant passwords and disallowing permitted access configurations after use;
- auditing all access and subsequent maintenance / support activities.

FUJ00088068

Actions that may impact the system are not permitted unless an engineer is on site. In extremis (and for EMC only) where data integrity may be at risk, such actions may be performed without an on-site engineer presence. All maintenance action will be audited.

FUJ00088068

7.0 Audit and Alarms

7.1 Audit and Alarm Requirements

The audit and alarm facilities provided by the Horizon system must satisfy the business level audit and security audit requirements of "external" auditors (including Post Office Ltd. and NAO) and the Post Office Ltd. and Pathway's "internal" monitoring (including Security Audit).

The Audit Trail Functional Specification [AUDFS], which is primarily concerned with addressing business level audit requirements, specifies audit trails as one or more "tracks" that can be selectively viewed by the appropriate auditors.

7.2 Sources of Audit Events

Auditable events are recorded in application level transaction logs and lower level audit tracks[2]. Figure 7.1 illustrates the main sources of system generated events.

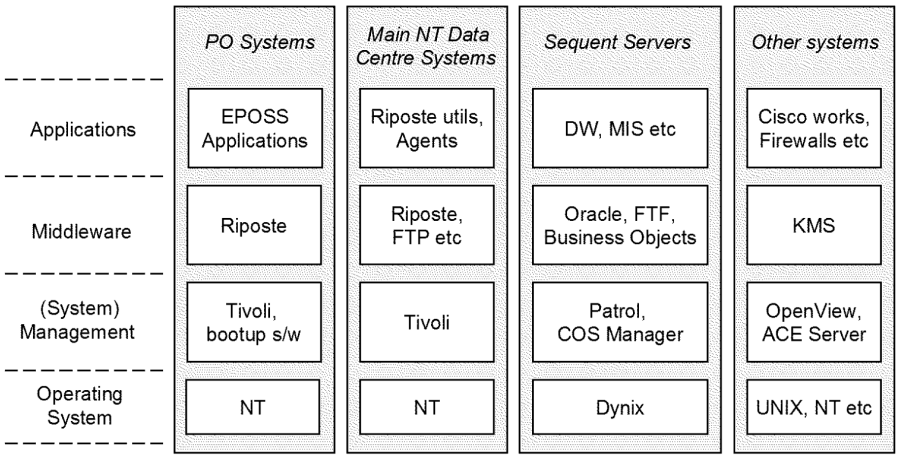

Figure 7.1 Sources of Auditable Events

Riposte provides an ideal basis for logging all transactions to give a complete picture of actions within the Post Office Outlets Infrastructure Service. It is used within the Post Office Ltd Central Services and OPS Domains to provide a complete record of all transactions.

Applications running on the Sequent servers generate logs of the business transactions and file transfers. The Oracle databases, used for the Data Warehouse and MIS, have the ability to audit security relevant events that are recorded in tables.

Patrols used to monitor all Sequent systems and the Oracle applications that run on Sequent platforms. The audit events and alarms gathered by Patrol are captured, for recording and analysis, via a Patrol Tivoli event adapter (as outlined in section 13.0).

[2] An "audit track" is a record of activities made within a subsystem for one or more of its interfaces (as defined in [AUDFS]).

FUJ00088068

COS Manager generates the main system level log on the Sequent servers. All users logging onto Sequent at the operating system level (for system administration, security management etc) will invoke COS Manager, which records their logon and subsequent actions selected from its menus.

Windows NT can provide essentially the same audit capability for both workstations and servers. These facilities are powerful but need to be used with caution to avoid generating vast quantities of low level events, which are difficult to analyse in a business context. Selective filtering is used to reduce the volume of events to be gathered, analysed and stored.

Tivoli is used to monitor selected Windows NT logs regularly and picks up agreed event types for transmission to the Data Centre as Tivoli events.

Wherever possible, application/middleware level auditing are used. Low level Windows NT audit tracks will, however, provide appropriate facilities for auditing system management activity across the system.

7.3 Auditable Events

7.3.1.1 All events in the following categories are capable of being audited:

- authentication actions (including logon, unsuccessful logon attempts and logoff),
- exception conditions (detected by operating systems and at the application level),
- system start-up,
- change of user rights (including granting of additional privileges),
- write access to selected files,
- system management activities (including addition of new users and reset of any user's password).

7.3.1.2 Where there are multiple mechanisms capable of recording a particular event, duplication is avoided and the most appropriate audit method is used.

For example, within the OPS Domain, activities at Post Office Outlet counters are recorded in the TMS journal rather than the lower level NT event logs. Similarly, within the Post Office Ltd Central Services Domain, Tivoli is used to gather events for central analysis.

7.4 Application Level Audit

7.4.1 General Requirements

7.4.1.1 The TMS journal is used to record data traversing between the Order Book Control Service (OBCS) and TMS.

7.4.1.2 The audit track includes the following:

- User id, date and time,
- all systems access, and

FUJ00088068

- all exception conditions (e.g. file sequence or control total failures).

7.4.2 Riposte Transaction Log

All transactions that pass through TMS are recorded in the journal. The journal is maintained on magnetic media within TMS for a period of (typically) 90 days. Following this, the journal data is archived to long term storage. The current or archived TMS journals can be accessed to provide an audit track of all TMS transactions.

7.4.2.1 For transactional-based data transfers, logging is provided at the message level.

7.4.2.2 All data captured at a Post Office counter, either as part of a counter transaction (i.e. Stamp sale) or as an administration function (user log-on, teller balance), forms part of a unique transaction that is given a unique reference number by Riposte.

7.4.2.3 The format of this journal entry varies according to the transaction type, [TED] but typically contains:

- Post Office ID,
- Counter Position ID,
- Unique Transaction ID,
- Date,
- Time,
- User ID,
- Application, and
- Transaction Details.

7.4.2.4 Each counter PC contains a journal and all journal entries shall be automatically replicated to all other members of the workgroup. This includes remote Correspondence Servers that form part of the TMS.

7.4.2.5 This Correspondence Server in turn replicate all its transactions to other Correspondence Servers located on different sites.

7.4.2.6 A complete audit track of all transactions and other significant events are maintained for the Post Office Counter systems, as specified in [AUDFS]. It can be extracted, when needed, for analysis.

7.4.2.7 All events that occur either in TMS or in OPS are written to a journal. The journal message content is identified in section 7.4.2.3.

7.4.3 Logging in Fall-back Mode

7.4.3.1 The audit track are maintained during periods of fallback and recovery.

FUJ00088068

7.4.3.2 The integrity of the audit track is maintained during periods of partial or complete service loss or failure. Starting and restarting transactions will make appropriate audit track entries.

7.4.3.3 The distributed nature of the Pathway TMS enables an audit track to be maintained and accessed during any recovery of a TMS server.

7.5 Application Level Audit Analysis

The tool set used to support audit analysis is expected to evolve as experience is gained in analysis of the various logs. The basic tools include facilities to selectively read:

- TMS journals,
- Tivoli event data,
- Oracle database information (e.g. using Oracle forms),
- Windows NT event logs (for exceptional investigations), and
- any other sources of audit information.

The output generated by these tools is a combination of standard reports and ad hoc enquiries.

As the tools develop, the ease of use and format consistency of the information reported is expected to improve.

7.5.1.1 Standard reports include all exception events (e.g. sequence or control total failures), plus daily/weekly/monthly control summaries.

7.6 Protection of Audit Tracks

7.6.1.1 The audit track has a level of security such that it cannot be altered or deleted.

The journals are written as append-only files, owned at the system level and protected by the subsystem's access control.

7.6.1.2 Pathway keeps copies of vital files, including the audit track, at the alternate central site or off site. The frequency of transferring backup copies is defined in [ACCPOL].

7.7 Audit of Systems Management Functions

The Systems Management function provides the audit track with a record of operational events, inventory, distribution and remote operations.

7.7.1.1 The Systems Management Service provides a repository for recording all physical events affecting the platforms that support TMS and the OPS.

All these environments operate under Windows NT and are managed from the Tivoli SMS server. The Tivoli SMS provides, in conjunction with the native Windows NT and messaging middleware services, a comprehensive facility for trapping, recording and interrogating audit events relating to the operational status of the hardware, software and applications.

FUJ00088068

7.7.1.2 The Tivoli notification features and Windows NT auditing support the recording of events such as which users access which objects, what type of access is being attempted and whether or not the attempt was successful.

7.7.1.3 Logging facilities supported by HP OpenView are used provide a record of network management actions.

An OpenView Tivoli event adapter is used to map SNMP traps into the central Tivoli Event server.

7.7.1.4 Administrative privilege is required for controlling audit and auditing policies within the Windows NT Registry.

7.7.1.5 Audit events are viewed through the appropriate audit analysis applications.

7.7.1.6 Replacement or modification of selected files containing security critical code is audited.

In particular, attempts to update or delete modules concerned with integrity checking and crypto functionality shall be monitored.

7.8 Windows NT Audit

This section provides an overview of the audit facilities provided by Windows NT. It should be noted, however, that Tivoli is used on all NT platforms to provide central event management services derived from the local mechanisms.

The local audit facility collects audit records from several components (including Riposte and local applications) in addition to recording its own NT system events. Tivoli then picks up the NT logs selecting the event to be collected according to the filtering criteria.

7.8.1 Selection of Auditable Events

For each audit category the selection criteria can include:

- audit successful events,
- audit failed events, and
- audit both successful and failed conditions.

The Windows NT Audit Policy dialogue box is used to select from the following auditable event categories:

- Logon and Logoff,
- File and Object Access,
- Use of User Rights,
- User and Group Management,
- NT Security Policy Changes,
- Restart and Shutdown, and
- Process Tracking.

FUJ00088068

7.8.2 Audit of File and Directory Actions

Appendix A lists the types of file and directory access that can be audited and explains the meaning of each option.

7.8.3 Audit of Registry Actions

Appendix A lists the types of Registry access that can be audited and explains the meaning of each option.

7.8.4 Audit of Printer Actions

The printer related actions that can be audited are defined in [AUDFS].

7.9 Alarm Conditions

Auditable events that require immediate investigation shall be used to trigger alarms in real time.

Events are selected in accordance with Pathway's Security Policy [SECPOL].

FUJ00088068

8.0 Security of Links

This section describes the cryptographic functionality, within the Horizon system, used to protect:

- data on individual communications links, and
- individual messages from creation to use (end-to-end).

Key Management throughout is based on advice from CESG and performed as agreed with Post Office Ltd.

Figure 8.1 illustrates the overall communications configuration to be protected:

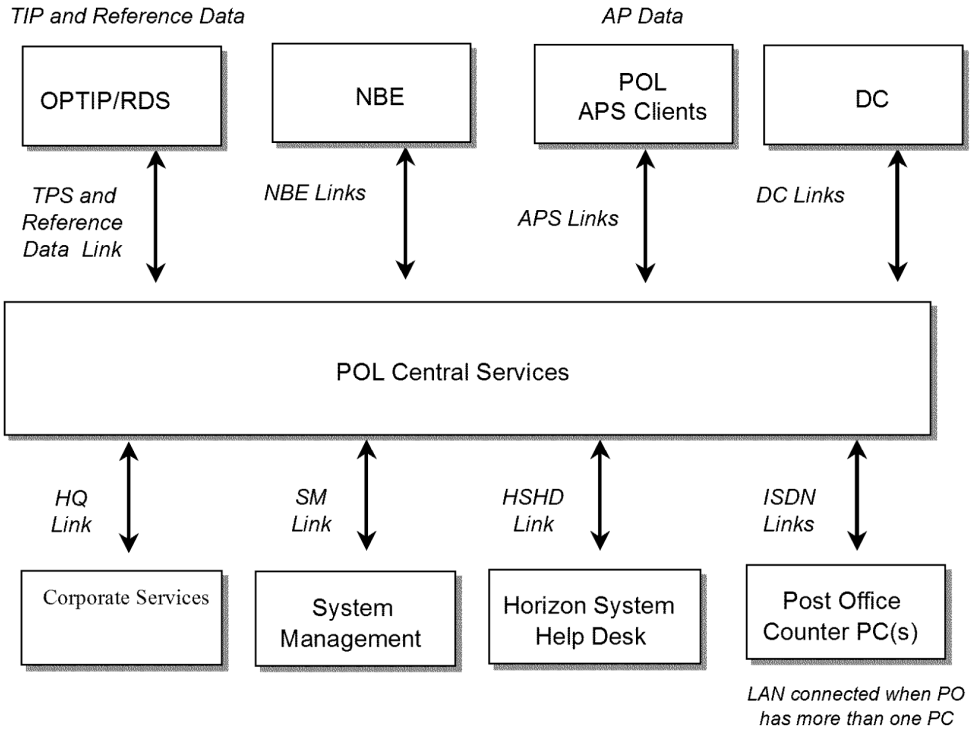

Figure 8.1 Links for Protection

For each client, Pathway implements link protection as each client interface is agreed.

8.1 TPS to OPTIP and Reference Data to RDS Link

These are the links used to transfer information to/from Post Office Ltd. They carry the entirety of Post Office Ltd's outlet transaction business and stock data, plus reference data

FUJ00088068

back to Pathway via a FTMS gateway service. There is an explicit requirement from Post Office Ltd. for integrity protection of this link, in addition to the end-to-end protection of APS records, as defined in section 9.3.

8.1.1 Protection

8.1.1.1 DSA signatures are used to protect the integrity of data transferred on this link in both directions. This protection is also provided for traffic to and from the disaster recovery site.

8.1.1.2 Verification is done by validating the incoming public key certificate against a CA public key using a pre-installed key stock at the receiving PC, then validating the file's signature using the public key in the certificate.

8.1.1.3 The same end-to-end integrity protection is used, where appropriate, to protect other low volume data such as Post Office Outlet reconciliation totals.

8.1.2 Key Management

8.1.2.1 The private signing key is managed in two parts that must be combined before either part is of any value.

8.1.2.2 Key distribution is effected by transmitting one of the parts electronically and the other by diskette. The part sent electronically is held on filestore. At each system start-up, the diskette part is introduced by the key custodian or key handler and combined with the filestore part to create the key in memory.

8.1.2.3 The full key will not be stored persistently on a disk file.

8.1.2.4 Each end of the link has a different signing key.

8.1.2.5 The keys are changed at intervals agreed with Post Office Ltd, based on advice from CESG.

8.2 Post Office Ltd HAPS Link - decommissioned

The HAPS system has been decommissioned. This section has been retained to keep references to this document fixed.

8.3 Post Office Ltd. APS Client Links

8.3.1.1 Files transferred on these links are digitally signed by the transmitting PC, providing authentication and integrity protection. The signature is DSA, done using a private key owned by the Pathway PC transmitting the file. The file is accompanied or preceded by the public key certificate needed to verify the signature.

8.3.1.2 Not all receiving clients choose to validate the signatures, but for those that do wish to do this, Pathway provides the CA public key stock needed to validate the certificates.

FUJ00088068

8.4 Post Office Outlet Links

These are the links from the Post Office Ltd Central Services Domain to the Post Office Outlets. Key Management of these links is automated by the Key Management System (KMS)

8.4.1 Protection

8.4.1.1 The protection ensures the authenticity of the parties to every communication session over the Post Office Outlet Links.

8.4.1.2 Concealing data from eavesdroppers is not a primary objective of this protection (unlike other forms of protection that may operate within a communication session).

8.4.1.3 A specific Post Office Outlet becomes a member of the VPN community as a result of the initial key distribution prior to auto-configuration phase. A commercial VPN product utilising Red Pike and a custom encryption module is used to support this.

8.4.1.4 Inbound ISDN calls (Post Office Outlet to Data Centre), is validated at the BT / Energis Interchange prior to onward transmission to the Data Centres. CLI is not validated outbound to the Post Office Outlet.

8.4.1.5 Where symmetric encryption is used, it employs the Red Pike algorithm.

8.4.1.6 Where asymmetric encryption is used, it employs either the DSA algorithm or, if embedded in a bought-in technology, RSA.

8.4.1.7 A Virtual Private Network (VPN) is established to enable Post Office Outlets to communicate with the campuses. The VPN members are the Post Office Outlets and a set of central VPN servers.

8.4.1.8 Communicating entities are authenticated as valid members of the VPN community by mutual cryptographic challenge and response based on asymmetric keys.

8.4.1.9 As a result of successful mutual authentication, the parties establish a shared secret symmetric key for the duration of the session.

8.4.1.10 Continued authentication is achieved by using the session key to encrypt all transmitted data. During a session, all data, both Riposte and Network, travelling across the link is encrypted as an added value consequence of using VPN technology.

8.4.2 Key Management

8.4.2.1 At routine intervals, similar to those used for other key material, the VPN keys at each Post Office Outlet are replaced by new values.

8.4.2.2 The KMS delivers replacement VPN keys to the Post Office Outlet under the additional protection of a communication key established with the help of Diffie-

FUJ00088068

Hellman exchange. This protection is over and above the incidental encryption afforded by the VPN.

8.5 Post Office LANs

These are the LANs that connect multiple-workstations in the larger Post Office Outlets.

8.5.1 Protection

Protection on these LANs is afforded by VPN.

Key material that needs to be transferred between Post Office Outlet PCs is passed either using the Post Office Manager's Memory Card or via Riposte messages encrypted under a key carried on the Memory Card.

8.5.1.1 Payment Authorisation and APS messages have the digital signature applied on their respective source machine (hence they are integrity protected over the LAN).

8.5.2 Key Management

8.5.2.1 The Post Office Manager (or other individual authorised to access the Memory Cards and the associated PIN) has to be present in order to successfully start up a workstation at a Post Office Outlet, since the card is the only repository at the Post Office Outlet for the filestore encryption key. To authenticate, the Post Office Manager signs on presenting credentials. These are held, protected by PIN (containing 64 bits of entropy) on a read-write Memory Card.

8.5.2.2 Keys are replaced at a Post Office Outlet, by a routine key refreshment procedure, at intervals agreed with Post Office Ltd., based on advice from CESG.

This involves the KMS initiating the same protected Diffie-Hellman exchange undertaken during roll-out, to establish key values used to protect the new key material. When required, the POM is alerted to insert his Memory Card into the Gateway PC to pick up the new key material, and to move from PC to PC in the Post Office Outlet, propagating the values to the other PCs, where the key material from the Riposte key distribution messages is also decrypted and installed as appropriate.

8.5.2.3 If the Post Office Manager forgets the PIN or the Memory Card is lost or damaged, recovery is achieved as follows:

- the Post Office Manager verbally authenticates to the Help Desk,
- the Help Desk authorises the KMS to send a special recovery key package to the Post Office Outlet. The package contents is similar to the key material issued during a routine key change, but the keys are the existing ones,
- the KMS sends recovery information to the Post Office Outlet using the Post Office Outlet link as a (virtually) normal routine key refreshment procedure,
- the material is then loaded onto a new Memory Card for which a new PIN is dynamically generated, and

FUJ00088068

- the Post Office Manager uses the new Memory Card and PIN to enable the gateway and counter PCs.

8.5.3 Rollout to Post Offices

8.5.3.1 Every PC will either be preloaded with the CA public keys it needs, to verify any public key certificates and revocation lists transmitted to it, or they will have been transmitted to the PC during the roll-out process and verified for their integrity prior to use. Other public key material will have be transmitted during the roll-out process.

8.5.3.2 With the exception of the CA keys, changes can be made if necessary through a routine key refreshment procedure. The same procedure is used to verify that the CA public keys held at the Post Office Outlet have not been tampered with.

8.5.3.3 During auto-configuration, the KMS forms an interactive connection with the Post Office Outlet in order to establish an end-to-end communications key with the Post Office Outlet Gateway PC.

The Diffie-Hellman exchange used has been extended to protect against man-in-the-middle attacks.

8.5.3.4 The communications key is used to encrypt confidential key material sent to the Post Office Outlet.

8.5.3.5 A specific Post Office Outlet becomes a member of the VPN community during the auto-configuration phase of its roll-out process, following the initial boot server exchanges. A commercial VPN product is used to support this.

8.5.3.6 The presence of the global public key and certificate material in a key package sent to the Post Office Outlet allows pre-KMS Post Office Outlet PCs to be upgraded to the full solution design by transmitting the necessary key material to them via this key package.

In a multi-workstation Post Office Outlet, relevant key material from the package is passed on, by the Post Office Manager (POM), to all workstations. The mediums used to transfer keys is the POM's Memory Card and message replication.

8.5.3.7 All keys issued to Post Office Outlets are generated by the KMS (using cryptographic quality random numbers provided by a hardware supported random number generator). Active keys are changed at intervals, as agreed with Post Office Ltd., based on advice from CESG.

8.6 Pathway Inter-campus Links

These are the links between the two Pathway campuses.

FUJ00088068

8.6.1 Protection

The physical characteristics of the high-speed connections between the campuses give a significant level of inherent security. There is, currently, no hardware available that could provide link level protection on these links.

8.6.1.1 Any key material passed between the Key Management Systems on the two campuses is encrypted under Red Pike using a key shared between the two KMSs.

8.6.2 Key Management

8.6.2.1 The KMS to KMS key is established automatically using an exchange protected by the DSA private keys owned by the KMSs.

8.7 Horizon Help Desk and System Management Links

8.7.1 Overview

In addition to the Pathway inter-campus links (described in section 8.6), there are a number of dedicated links into campuses that need to be protected. The network configuration is illustrated in [TED].

8.7.1.1 All links from the Core Service sites to the campuses are encrypted.

8.7.2 Protection

System modifications (e.g. fault reporting) are done through the Horizon System Help Desk. Caller authentication will, therefore, be strong and proofed against eavesdropping.

8.7.2.1 All data is encrypted for confidentiality and integrity using bought-in Government approved point-to-point encryption devices employing the Rambutan algorithm (see section 4.5.3).

8.7.2.2 System management functions, which could cause changes to security sensitive data on campus machines forming a serious security threat, is protected.

8.7.2.3 The risks are considerably reduced by permitting only the activation of pre-authorised fixing scripts and pre-defined Oracle Forms. The scripts used are stored away from the management workstation.

A combination of integrity protection and the use of one-time passwords provides the basic mechanisms.

8.7.3 Key Management

8.7.3.1 The standard key management facilities, provided by the bought-in devices, is used.

FUJ00088068

8.8 Links with Pathway Headquarters

8.8.1 Overview

There are dedicated links into the campuses sites from the Pathway Headquarters.

8.8.1.1 All links from the Pathway Headquarters site to the campuses is encrypted.

8.8.1.2 The System Support Centre (SSC) has controlled access. Remote access to FTMS Gateways and Counters is managed and supported using SSH client on a support Terminal Server.

8.8.1.3 The On-line Analytical Processing (OLAP) and Oracle Financials connections only provides client access to the respective applications that run on the Management Information System (MIS).

8.8.1.4 The SSC platforms use a different LAN segment from that used by the OLAP and Oracle Financials.

A router is used to prevent access between the two LAN segments. The network configuration is illustrated in figure 8.2

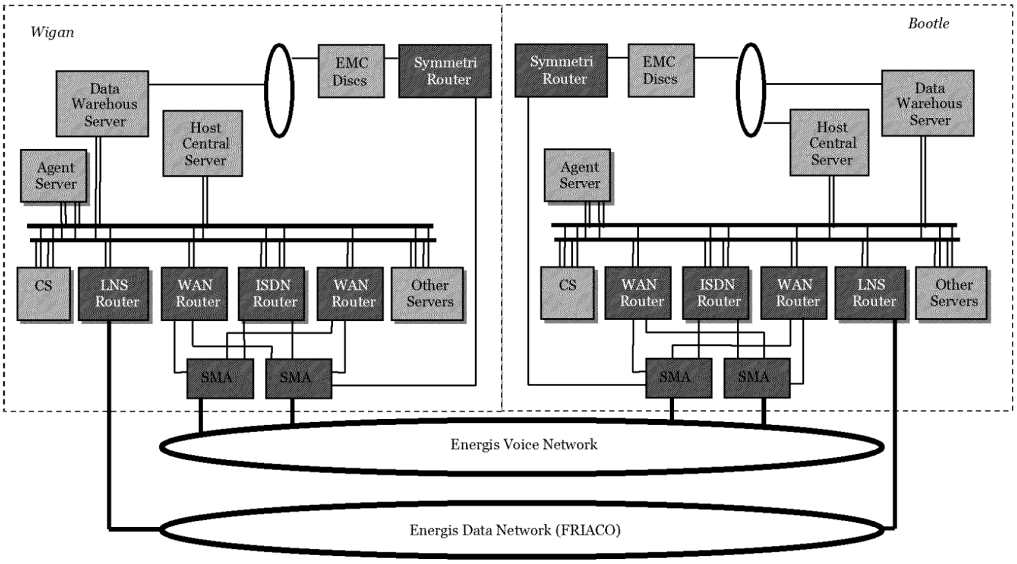

Figure 8.2 Network Configuration

8.8.2 Protection

8.8.2.1 All data is encrypted for confidentiality and integrity using bought-in Government approved point-to-point encryption devices employing the Rambutan algorithm (see section 4.5.4).

FUJ00088068

8.8.3 Key Management

8.8.3.1 The standard key management facilities, provided by the bought-in devices, is used.

8.9 Link to the NBE

8.9.1 Overview

This is the link between the Post Office Ltd. Central Services Domain and the Network Banking Engine (NBE).

8.9.2 Protection

The WAN link between Horizon and the NBE is encrypted. This facility is implemented using encryption available on the CISCO routers which employ hardware encryption utilising an Integrated Service Adapter which provides IPSec / 3DES encryption.

All message or file exchanges with the NBE are authorised and their integrity validated through the use of MACs (Message Authentication Codes). MACs are calculated using a bi-directional MAC key. The mechanism for protecting keys across the interface requires the use of a shared Zone Master Key (ZMK) between Horizon and the NBE.

8.9.3 Key Management

Key management uses specialised cryptographic hardware known as a Host Security Module (HSM). The MAC keys (utilising 3DES) are generated in an HSM on the NB Agents. Each message carries with it the MAC key encrypted under the ZMK.

Further details are in Section 11.

8.10 Link to MA

8.10.1 Overview

This is the link between the Post Office Ltd. Central Services Domain and the Merchant Acquirer (MA).

8.10.2 Protection

The link between the Debit Card Authorisation Agent and the MA is used for Requests and Acknowledgements following the RAC model. This link is not encrypted. The link between the Debit Card Manager external MPPE Server and the MA is encrypted. This facility is implement using Microsoft Point to Point Encryption (MPPE).

Digital Signatures are used to protect the integrity of all messages or files exchanged between Horizon and the MA .

8.10.3 Key management

The encryption key for the MPPE is established from a shared password/passphrase.

Further details are in section 12.

FUJ00088068

8.11 Key Generation

Cryptographic keys are generated in one of the following ways:

8.11.1.1 Where government approved hardware devices are purchased, key material is provided in whatever standard approved way is normally recommended for that product.

8.11.1.2 Keys generated in bulk for use by Layer 7 crypto routines uses entropy sourced from an entropy generation product using hardware generation. This product performs its own randomness assurance procedures. It is being evaluated by CESG for government approval. In the meantime, Pathway provides independent software logic that will spot check for continuing quality of output, independent of the product's own checks.

8.11.1.3 The entropy will either be directly used as a Red Pike key or is passed to approved Layer 7 routines to generate private/public key pairs.

8.11.1.4 The variation of Diffie-Hellman that are used is the Thames Bridge key management algorithm, which is provided by the government approved crypto infrastructure in use by Pathway. At a Post Office Outlet, Thames Bridge generates its own entropy using approved algorithms.

8.11.1.5 Smaller quantities of keys for use with the Layer 7 crypto routines are generated using the approved Layer 7 key generation functions and the entropy they supply.

8.11.1.6 Key generation for the NBS is covered in section 11.

8.11.1.7 Key generation for the DC is covered in section 12.

8.12 Key compromise

In the event of a key compromise, key change mechanisms will be called into force.

FUJ00088068

9.0 Message Protection

9.1 Technology

Unless otherwise stated, all message protection is performed using DSA with a 768 bit modulus. Each DSA signature requires a cryptographically strong random initialisation value, known as a K-value.

Entropy for K-values is generated internally where they are needed (in the Post Office Outlet PC, the KMS or in the Tivoli signing system).

9.2 Key Management

9.2.1 Public Key Technology

Standard simple public key technology is used, as outlined below.

Under public key technology, protected messages are digitally signed by a private key and validated using the private key's matching public key. Working public keys are distributed either at roll-out of a new Post Office Ltd. Outlet or by a KMS in public key certificates ("PK certificates") signed by a private key from a Certification Authority (CA).

The "CA private key" has a corresponding public key called the "CA public key".

9.2.2 Public Key Certificates

Pathway's "PK certificates" are based upon the X.509 standard.

9.2.2.1 PK certificates contain the public key, the name of the possessor of the corresponding private key, an expiry date and key and certificate identifying information.

9.2.2.2 The CA private key is held securely on a PC in a secure cabinet, within a secure area and not connected to any network.

9.2.2.3 All digital signatures are verified using public key certificates either transmitted with the signed data to be validated or already available to the verifier. Public key certificates are checked to ensure that they are not expired and that they have not been revoked. Where relevant, the certificate owner is checked against the claimed origin of the data that is signed.

9.3 Automated Payments

9.3.1.1 Transactions digitally signed at Post Office Outlets are signature verified at the harvesting agent that takes the transaction from the correspondence servers and transfers it to the APS host. The signature is not carried forward into the APS Host database since this would more than double the size of the database. Direct protection of the transactions resumes when files containing APS transaction records are digitally signed prior to transmission over links to Post Office Ltd. APS clients (see Section 8.5).

FUJ00088068

For new integrity-critical products, the same overall architecture still holds. It entails signing in the Post Office Outlet, verifying at the harvester, and integrity protecting complete files of transactions for validation at the client-end PC.

9.3.1.2 Post Office private APS signing keys are replaced at intervals agreed with the Post Office Ltd, based on advice from CESG, using the routine key replacement mechanism.

9.4 Software Distributed to Post Office Outlets

New software releases are distributed to Post Office Outlets over communications links from the central campuses.

9.4.1 Tivoli

9.4.1.1 All software payload for installation by Tivoli mechanism is digitally signed, for protection in transmission, using the Software Issue Private Key (SIPR) and verified on receipt using the corresponding Public Key (SIPU). The signature uses 768 bit DSA.

9.4.2 Riposte

9.4.2.1 All software used via the Riposte desktop is digitally pre-signed off-line using the RSA algorithm and validated by Riposte every time the desktop is loaded. The key size is 512 bits.

9.4.2.2 The private key used in the signature is held in a high security environment at the Pathway central sites.

This protection regime uses standard Microsoft cryptographic interfaces.

9.4.2.3 The Riposte code (developed by Escher) allows digitally signed applications to be produced either by Escher or by authorised signatories.

Pathway is an authorised signatory, hence Pathway's public key is acceptable in the Riposte verification logic.

9.4.3 Protection of Non-desktop Software Resident on Post Office PCs

9.4.3.1 This is provided indirectly by the absence of a means of introducing software by any other means, other than over the communications link to Pathway, and by preventing modification through local interfaces by disallowing those functions.

9.4.3.2 Software whose functionality is confidential can be nominated for protection while on filestore by including it in a library marked to be encrypted.

9.4.4 Protection for Siemens Metering Code and Data

The statements below highlight the main features that provide protection on the live system to the counter application code and data from Siemens Metering at Post Office Outlets and during delivery to Post Office Outlets.

FUJ00088068

A full set of statements on security objectives and methods for the protection of this Siemens Metering material is given in the contract controlled document [STAT].

9.4.4.1 Siemens Metering software and data is encrypted on receipt and stays encrypted until installed at a Post Office Outlet.

9.4.4.2 Installed Siemens Metering software is held in encrypted filestore.

9.4.4.3 The key needed to decrypt uninstalled Siemens Metering software and data, and the key needed to activate the application, is encrypted prior to transmission to Post Office Outlets along the communications links from the Pathway central campuses.

9.4.4.4 Updates and bug fixes to Siemens Metering software is integrity protected under a digital signature.

9.4.4.5 Updates and bug fixes to Siemens Metering software is encrypted over the link between the central campus and the Post Office Outlet.

9.4.4.6 Compromise of a Post Office Manager's Memory Card and PIN will not by itself cause compromise of Siemens Metering key material.

9.4.4.7 No authorised means of locally introducing code to Post Office Outlet PCs is provided.

9.4.4.8 No authorised direct local access to NT operating system functions on Post Office Outlet PCs is provided.

9.4.4.9 Pathway key values used to protect Siemens Metering code, data and keys, is changed at a frequency in accordance with CESG recommendations.

9.5 Other Message Types

Key Package messages sent from the KMS is protected under a communications key dynamically established between the KMS and the Post Office Outlet (as described in Section 8.6).

9.5.1 DC Messages

9.5.1.1 The confidentiality of any sensitive data within DC Requests, Authorisations, Confirmations passed between counter and the data centres shall be achieved by encryption.

FUJ00088068

10.0 Filestore Encryption in Post Office Outlets

10.1 Data Confidentiality

Nominated files on Post Office Outlet workstations and gateway machines are automatically encrypted at disk access level to preserve data confidentiality in the event of the workstation being stolen. The parts that are encrypted are:

- the Windows NT swap file,
- the Riposte journal and any related working files,
- selected files containing the cryptographic keys held by the workstation, unless they are protected as part of the key management design,
- selected counter application code libraries, as required by the application providers, and
- selected counter application data files as required by the application providers.

The whole of the swap file is encrypted prior to the loading of any externally supplied key material. The key used is internally generated by the TeamCrypto product using its own entropy, and is different for each boot-up of the PC. TeamCrypto uses a key supplied by the KMS to encrypt all other areas of the hard disk (listed above).

The algorithm used is Red Pike.

10.2 Functionality

None of the NT workstations installed in Post Office Outlets have operable floppy disk drives (since, if fitted, they are physically blanked off and disabled in the BIOS). The workstations have been rolled out to the sites with the majority of the software, including the crypto software, pre-configured in the factory.

The delivered configuration of a particular workstation type (e.g. gateway or non-gateway) is the same to, whatever Post Office Outlet it is being delivered.

Protection is applied after delivery on site.

The Post Office Manager (or authorised representative) is the only person on site who has the means of unlocking the key to the filestore encryption. He/she is not, however, required to be IT literate since the procedures used is straightforward and well documented.

In general each workstation is used by a different counter clerk who uses other authentication data to sign on to the workstation. Counter clerks cannot unlock the filestore without assistance from the Post Office Manager. Typically, a workstation may be left running all day but counter clerks sign on and off at more frequent intervals.

10.3 Security Considerations

Some basic security considerations of the solution are:

10.3.1.1 The KMS is the source of the keys for all files except the swap file, for which a new key is dynamically established by TeamWare Crypto on each PC during each boot-up.

FUJ00088068

10.3.1.2 The product used to encrypt filestore is TeamWare Crypto, using the Red Pike algorithm, for which CESG approval is required.

10.3.1.3 The Post Office Counter Manager sign-on is used to unlock the filestore (on power on) so that normal counter clerks can then sign-on to the workstation.

It is inevitable that, across the large number of Post Office Outlets involved, some Post Office Managers will forget their password, lose or damage the token needed to authenticate and unlock the filestore.

10.3.1.4 Means are provided to enable the filestore to be unlocked securely by a central authority.

More detail is given in Section 8.5.2.3

10.3.1.5 The filestore encryption key is changed at intervals agreed with Post Office Ltd, based on advice from CESG.

The Post Office Manager is also able to change his/her authentication information (e.g. password or token).

FUJ00088068

11.0 Network Banking - Additional Features

The Network Banking Service (NBS) initially supports several On-line counter transaction types, each being initiated by the presentation of a bank card. apart from deposit transactions customer verification is via the use of PINPads or a visual check of customer signature by the Post Office clerk. Dedicated NB Agents within the POL Central Service Domain exchange data with the Network Banking Engine (NBE) over an encrypted link. Network Banking Release 1 utilises WebRiposte to the extent that it has an updated message server, but does not use additional web-services.

The RAC model of transactions and data flows has been adopted to support communication with the Clients via the Network Banking Engine (NBE) but the counter application is generic and supported by POL Reference Data.

This section deals with the additional security enforcing features and components introduced as a result of the NBS.

11.1 E2E Security Domains

The 'end-to-end' involvement and interaction of domain boundaries for NBS are shown schematically in Figure 11.1 below.

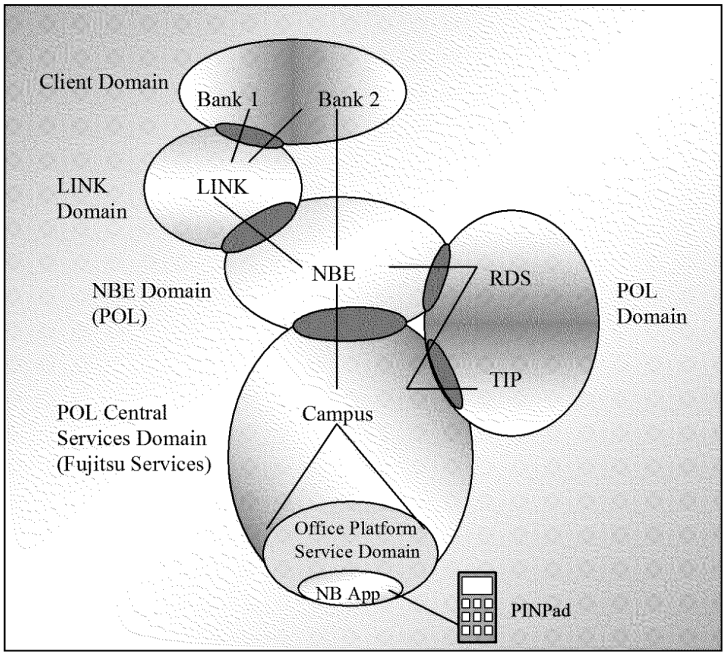

Figure 11.1 NB Domains and Boundaries

The figure identifies the domain boundaries that equate to the operational, management and contractual responsibilities of each of the participants. Each Bank (or financial institution) within the Client Domain are separate domains in their own right but are shown collectively for convenience.

FUJ00088068

The provision of the NBS introduces a change to the existing system paradigm (i.e. real-time interactions as opposed to message exchange) but does not alter the basic security posture of the Horizon system. The NBS is afforded the existing security protection of the Horizon infrastructure whilst within the POL Central Services Domain. Primary changes are related to the links between the Central Services and NBE domains.

11.1.1 Security Components

For the NBS, Pathway provides additional facilities that ensure amongst other things:

- the integrity of NB data between the POL Central Service Domain and the NBE;
- PINs are encrypted into a PIN Block at the point of entry into the PINPad and across the POL Central Service Domain;
- the confidentiality of sensitive NB data between the Counter NB application in the Office Platform Service Domain and the NBE is maintained. Sensitive data is identified as discretionary data held on the magnetic card tracks 1 and 2, or card details entered by the Counter Clerk;
- separate key management schemes are used for PINs and other sensitive (e.g. Track 2) data;
- the encryption of communications networks, between the POL Central Service Domain and the NBE;
- the authentication and integrity of all information exchanges with the NBE;
- that only authorised services and protocols operate between the POL Central Service Domain and the NBE;
- the installation and configuration of dedicated firewalls at the interface between the NBE and each Data Centre supported by log analysing software.
- 'Translation' of encrypted PIN values across the POL Central Service and NBE domain interface.

11.2 PINPads

The NBS provides for the introduction and operation of PIN Pads to support Customer authentication in respect of on-line banking transactions. All NB transactions (with the exception of deposit transactions) are authorised at the Post Office counter either by the counter clerk verifying the Customer signature or the Financial Institution via an online verification of the Customer entered PIN Number. PIN Pads are installed at every customer-facing counter position.

A single key management domain is provided for PIN Pads. This is supported by a secure key installation and management scheme that is compliant with the relevant parts of ISO 11568 and 8732. (see section 11.6)

The DUKPT scheme is used for PIN encryption - Key generation and management of (single length) DES keys and PIN Blocks comply with the required standard (ANSI X9.24:1998).

the characteristics of the PINPad are such that successful penetration of the PIN Pad does not permit the disclosure of any previously entered PIN value and that there is no feasible way to

FUJ00088068

determine any past key given knowledge of any data that has been transmitted to and from the PIN Pad.

11.2.1.1 PIN Value

The PIN value is encrypted by the PIN Pad upon entry by the customer and held in the transaction message within a standard compliant PIN Block format (ISO 9564 Format 0). The PIN value is only held in encrypted form within the Horizon system other than when first entered at the PIN Pad and when translated into the encrypted form suitable for the NBE. PIN block translation does not expose the clear text PIN. The translation process translates the PIN from encryption under the PINPad DUKPT schema to a key and schema known to the NBE.

The PIN encryption key is managed in accordance with the requirements of ISO 11568 or 8732. The PIN encryption key is specific to this function and is not used for any other cryptographic purpose within the Horizon system.

Remote key management of PIN Pads is being implemented in NBS Release 1 timescales. Remote key management of the PIN Pads will be performed remotely through enhancements to the existing KMA functionality. These enhanced capabilities will also be used to re-initialise the DUKPT scheme with a new initial key in the event of a key compromise.

All PIN processing and associated key management will be undertaken in accordance with ISO 9564 and with the LINK Information Security Standard.

11.3 Office Platform Service Domain

The confidentiality of any sensitive data within a NB transaction is achieved by separately encrypting the data at the counter application. Sensitive data is defined as either magnetic card track 1 or 2 discretionary data, card data entered by the counter clerk (issue number/ start date/ expiry date).

Key management is via an estate-wide key utilising the Red Pike algorithm, which is created and delivered via KMS.

From this point onward the data remains encrypted whilst it is within the Horizon system whether in transit or in storage.

11.4 POL Central Services Domain

Network Banking messages passing over the Horizon infrastructure are digitally signed in both directions. The use of digital signatures ensures the authenticity, integrity and non-repudiation of all exchanges between the Counter and the interface to the NBE. This protection is in addition to VPN encryption deployed at the Outlet LAN and the WAN between the Outlet and the Data Centres.

Replay protection is provided by a combination of measures. The (banking) transaction ID is MACed and checked using a variant of the PIN encryption key to protect against PIN replay attack, the origin of correspondence server banking message are validated to ensure that they originated at the counter and duplicate responses received at a counter are ignored.

FUJ00088068

11.5 Horizon - NBE Interface

The Horizon system implements a number of security measures with respect to the NBE interface. All Horizon components that interface directly to the NBE are protected by a DMZ (De-Militarised Zone) that uses a combination of firewalls and filtering routers to screen protocols and services across the interface.

All message or file exchanges with the NBE are authorised and their integrity validated through the use of MACs (Message Authentication Codes). MACs are calculated using a uni-directional MAC key (i.e. a separate key is used for data exchange in each direction). Key management and key change frequency for the MAC key follows the same principles as dictated for the (NBE) PIN encryption key. Key management is undertaken accordance with ISO 8732 and ISO 11568.

11.5.1 Host Security Module

The encrypted PIN value is only valid within the POL Central Services Domain. Whenever a domain boundary is crossed the encrypted PIN value is translated into the encrypted value of the second domain. Conversion of the PIN encrypted value between the Central Services operational domain and the NBE takes place within a separate host security module (HSM) that ensures that the PIN value never appears in plain text.

HSMs are held in secure locations within the Data Centres. Corresponding physical security is afforded the encryption units located at the NBE site.

The operation of the translation of the encrypted PIN value conforms to the LINK standard (LINK Switch Service Interchange Standard LIS5 Security Standard). Key management for the HSM is also conformant to the LINK standard.

Key management for the HSM storage master keys is via a standalone Card Loading Workstation which is located in a secure Fujitsu Services facility.

Storage master keys and key management for HSMs is distinct from any other cryptographic keys used for the exchanges between Horizon and the NBE.

11.6 PIN Encryption Key Generation & PINPad Key Loading

To support PINPad initialisation and rollout, secure key management and key handling procedures and processes are established with the Pin Pad vendor.

PINPad key generation and loading is a multi-part process involving both Pathway and the Vendor. Within this process discrete separation of the duties of each party is enforced. In particular, Pathway is responsible for the generation of the keys from which the PIN encryption key is either derived or directly protected.

FUJ00088068

A particular facet of the PINPad loading process applied by the Vendor is the use of MIDU units. A MIDU is a tamper resistant unit that is used for both key generation and other cryptographic functions. The use and algorithms applied by the MIDU's are compliant with ISO 9564 and 11568.

An overview of the sequence of key generation and loading (and the involved parties) is shown in Figure 11.2 below:

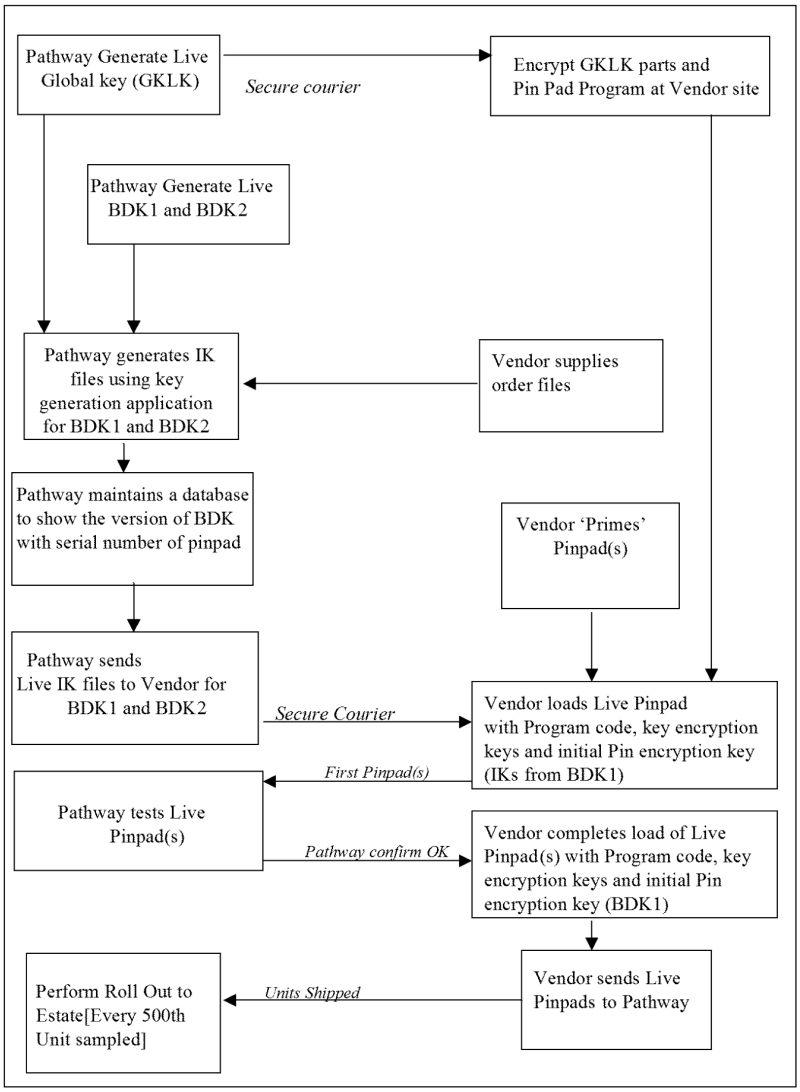

Figure 11.2 Key Generation and Loading

11.6.1 GKLK Generation

The Global Key is generated in a secure Pathway facility using a SCT hardware device. The key is generated in multiple parts and handled, transcribed and stored (separately) by at least

FUJ00088068

two individuals to ensure that no one individual has access to all the parts – and thus the whole key.

11.6.2 Pin Pad Load Package Generation

Generation of the PINPad Load package is performed in a secure facility at the Vendor's site conducted under the supervision of authorised personnel. The required inputs for the processes are the Global Key and the KAREA index.

The PINPad software and the key parts are input into a stand-alone system and encrypted values of the Pin Pad program and Global Key parts produced. The production of the encrypted components is a serial process whereby each part is submitted, passed to a secure MIDU-A unit for encryption and then copied to a disk before the next part can be introduced. The production of the encrypted parts is a time-bounded process that is controlled by the load production software.

Key parts are encrypted under a randomly generated triple DES key. The PINPad program is encrypted under single DES variant of this key and a random number key is encrypted under the KAREA key. The KAREA key is generated from the KAREA index that is unique to Horizon. (Note: the KAREA key is not available outside of the MIDU-A).

11.6.3 Order File Creation

An Order File containing PINPad Serial numbers and other non-sensitive attributes is created by the Vendor and sent to Pathway.

11.6.4 DUKPT Initial Key Generation

The generation of DUKPT Initial Keys is performed within a secure facility at Pathway on a dedicated stand-alone system running a key generation application.

The global derivation key (BDK) is generated in a using a hardware device (SCT). The key is generated in 2 parts with a KCV (for the whole key). Each Key part and the KCV are generated, handled, transcribed and stored separately by two individuals to ensure that no one individual has access to all the parts – and thus the whole key.

The key generation application uses a two-step process to calculate the unique encrypted initial key (IK) for each PINPad. The separate GKLK and BDK parts are loaded into the HSM where they are encrypted under a randomly generated Triple DES key. The resultant encrypted key values are then stored on the Key Generation PC.

The encrypted BDK and GKLK are then loaded in to the HSM and the records from the Order file are input into the HSM. For each Pin Pad a key encryption key (BKLK) and initial key (IK) is calculated and the encrypted IK is derived. A file record is then output containing the Pin Pad Serial number and the PINPad IK encrypted under the BKLK. The file records are written to CD for subsequent transport to the Vendor.

In operational terms the above process is performed for two derivation keys (BDK1 and BDK2) and the output files are written to separate CDs. The file of IK keys encrypted under BDK1 are used to prime the rolled-out PINPads and the file of IK keys encrypted under BDK2 is retained for those scenarios (e.g. repair) where it would be necessary to change the PINPad keys. The file of encrypted IKs (from BDK1) sent to the Vendor.

(Note: BDK keys never leave the Pathway secure facility.

FUJ00088068

11.6.5 Key Loading

PINPads are primed in three stages in a secure facility at the Pin Pad production centre:

- a MIDU is used to load the Boot processor of the 'bare' PINPad with a Boot Guard Key.
- a Tamper Seal is applied to the Pin Pad.
- a MIDU loader unit is used to load the loader code, PINPad Serial number and an encrypted loader key into the PINPad. The PINPad Serial number and the encrypted Loader key are placed in a special security zone of the PINPad implemented by a combination of both hardware/software design and operation that is only available to the Security Loader in a specific mode.

The loading of PINPad keys is performed in a secure Key Loading Area. The load process requires inputs of the KAREA index, the encrypted Pin Pad program code and GKLK parts, the encrypted IK File and the Pin Pad Serial number.

After entry of the KAREA index and Pin Pad Serial number at the MIDU-A, the encrypted KAREA key is calculated in the MIDU-A and then loaded into the PINPad's security area. A subsequent process then loads the encrypted programs, random number key, PINPad IK and GKLK parts into the PINPad.

After loading the input components the PINPad Security Loader decrypts and stores the program code; overwrites and deletes the random key encrypted under the KAREA; decrypts the GKLK parts and derives the BKLK key – using a DES process and overwrites and deletes the encrypted GKLK parts.

11.6.6 Pin Pad Verification

Pathway verifies and validates the initial PINPads produced by the vendor using a PINPad Proving System. This is a dedicated stand-alone system within a Pathway secure facility that validates by functional testing the key usage and functions of the PINPad. This includes PIN processing (and the MAC) by the HSM. If the test is successfully completed the Vendor ships the loaded PINPads.

For each shipment of Pin Pads received, Pathway will sample every 500th unit and verify the Pin Pad set-up using the Pin Pad proving system.

11.7 Audit and Alarms

11.7.1 Audit

Network Banking audit requirements are detailed in the Audit Trail Functional Specification (CR/FSP/006).

FUJ00088068

The statutory requirement for certification in accordance with the relevant sections of PACE (s69 and s70) no longer exists but Pathway ensures as far as possible that relevant information produced by the system at Post Office Ltd's request is admissible in support of prosecutions.

The confidentiality and integrity of sensitive data (e.g. PIN value, Card discretionary data) is maintained within the audit archive by retaining the encrypted value of the data which can be used in support of investigations and/or evidence for the resolution of disputes and prosecutions.

Pathway retains securely copies of the following encryption keys in compliance with the requirements of RIPA (2000):

- network encryption keys;
- the cryptographic session key used to encrypt the sensitive customer card details within the Horizon environment.

PIN encryption keys or any other key that directly or indirectly reveals plain text PINs are never revealed – not even in support of investigations or evidence.

11.7.2 Alarms

In the event of a suspected key compromise, of any NBS related key (HSM master keys, ZMKs, PIN Pad initialisation keys etc.), key change mechanisms will be called into force.

Where a key is suspected of compromise, it will be changed such that the suspect key gives no information about the replacement key. In addition, any key directly or indirectly protected by the suspect key will also be treated as suspect.

The timing of any key change will take into account the nature of the security breach giving rise to the key change, its impact on system availability, and the presence of any compensating controls.

Where a suspected compromise affects the Horizon environment an enhanced capability of the existing KMA and manual procedures will be used to change keys within the Horizon system.

Where a suspected compromise affects the NBE PIN Translation Key, then key changes will be applied at the NBE. A procedure will be agreed between Post Office Ltd. and Fujitsu Services to co-ordinate the changes at the Horizon - NBE interface.

Post Office Ltd. will allow access to Pathway representatives to apply key changes to the encryption units at the NBE site.

FUJ00088068

12.0 Debit Card (DC) – Additional Features

Debit Cards supports several on-line counter transaction types, each being initiated by the presentation of a debit card. Customer verification is via a visual check of the customer signature by the Post Office clerk. Dedicated DC Agents within the POL Central Service Domain exchange data with the MA. The Debit Card Authorisation Agent links through a dedicated Firewall to an external router. The router is configured for dial out only (to the MA). The links between DCA and Router utilises TCP/IP. The link on from the router to the MA utilises X.25. The router performs the protocol conversion from/to X.25. Communications between the DCA and MA are not encrypted.

The Debit Card Manager links through a dedicated Firewall to a second external router. The link on from the MPPE Server to the MA shall be encrypted using Microsoft Point-to-Point Encryption (MPPE).

The encryption key for MPPE is established from a shared password/passphrase. Procedures for the establishment, key length, exchange and frequency of change of the password/passphrase are to be agreed between Pathway and Post Office Ltd and then documented in the OLA entitled DC operational Level Agreement.

The RAC model of transactions and data flow has been adopted to support communications with the Merchant Acquirer. The counter application is generic and supported by POL Reference Data.

This section deals with the additional security enforcing features and components introduced as a result of Debit Cards.

12.1 E2E Security Domains

The 'end-to-end' involvement and interaction of domain boundaries for DC are shown in Figure 12.1 below.

FUJ00088068

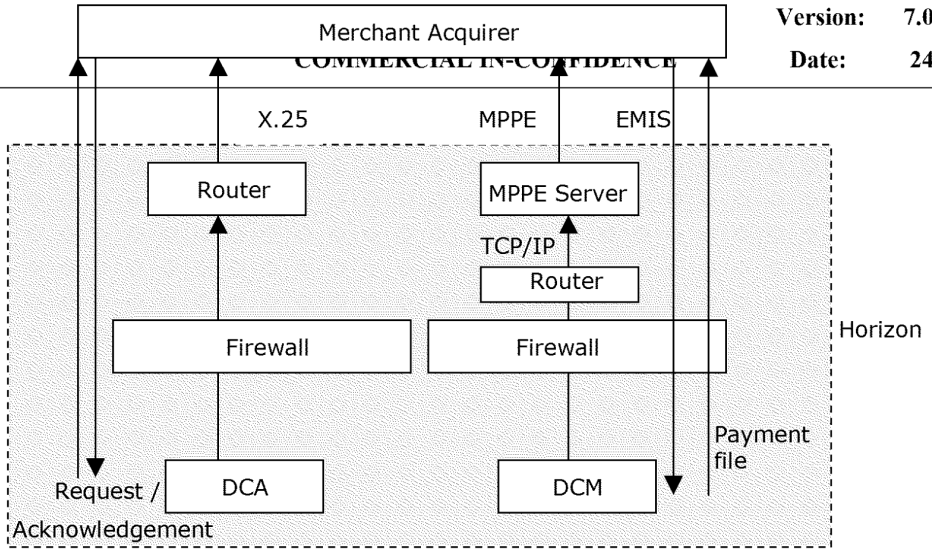

Figure 12.1 DC Domains and boundaries

The figure identifies the domain boundaries that equate to the operational, management and contractual responsibilities of the two participants.

DC, like NBS introduces real-time interaction as opposed to message exchange but neither alters the basic security posture of the Horizon system. DC is afforded the existing security protection of the Horizon infrastructure whilst within the POL Central Service Domain. Primary changes are related to the links between the POL Central Service Domain and the Merchant Acquirer.

12.1.1 Security Components

For DC, Pathway provides additional facilities that ensure amongst other things:

- The integrity of DC data between POL Central Service Domain and the Merchant Acquirer;
- The confidentiality of sensitive DC data between the counter DC application in the Office Platform Domain and the DC is maintained. Sensitive data is defined as discretionary data held on the magnetic card tracks 1 and 2, or card details entered by the Counter Clerk;
- Separate key management scheme used to protect the sensitive data;
- The encryption of EMIS and payment files through the communications networks, between the POL Central Service Domain and the Merchant Acquirer;
- The authentication and integrity of information exchanges with the Merchant Acquirer;
- That only authorised services and protocols operate between the POL Central Service Domain and the Merchant Acquirer;
- The installation and configuration of dedicated firewalls at the interface between each Data Centre and the Merchant Acquirer supported by log analysis software.

12.2 Office Platform Service Domain

All Horizon based transactions for DC will require authorisation and will be referred to the MA. No locally delegated authorisation procedures will be supported within the Horizon Domains.

FUJ00088068

The counter clerk will enter the request for authorisation at the point of customer service (counter) and convey it to the point of authorisation. The MA will undertake the authorisation decision and the details of the decision will be returned to the customer service point. The counter clerk will confirm the decision and undertake any associated processing to ensure the transaction outcome is aligned at the counter with the MA decision. This follows the RAC model used within the financial services industry.

The confidentiality of any sensitive data within DC Requests, Authorisations, Confirmations passed between counter and the data centres shall be achieved by encryption. This is via the Horizon Sensitive Data Key that is distributed and managed by automatically by KMS. DC Requests, Authorisations, Confirmations passing between Counter and the Data Centres shall be digitally signed.

12.3 POL Central Services Domain

The Debit Card Authorisation Agent and Debit Card Manager at the Data Centres shall be built with filestore encryption for selected files, i.e. those that contain sensitive DC data and swap files. The DCA and DCM shall verify/sign the digital signature of all messages exchanged with the Counter. The use of digital signatures for all communications between POL Central Service Domain and the Office Platform Domain ensures authenticity, integrity and non-repudiation of all exchanges between the counter and the interface to the MA. This protection is in addition to the VPN encryption deployed at the Outlet LAN and the Wan between the Outlet and the Data Centres.

Key management of signing keys between the outlets and the agent in both directions is automated via KMS. Associated key encryption keys are manual distributed. .

The origin of correspondence server DC messages are validated to ensure that they originated at the counter and duplicate responses received at a counter are ignored thus protecting against replay.

12.4 Horizon - MA Interface

Firewalls are used to mediate the communications between the Horizon data centres and the MA. The use of a combination of firewalls and routers to screen protocols and services across the interface provides a DMZ (De-Militarised Zone) to protect Horizon Components that interface directly with the MA.

Messages and files exchanged between the Debit Card Manager and the MA are encrypted with Microsoft Point-to-Point (MPPE) encryption to protect their confidentiality. Key management and key change frequency for the MPPE are undertaken with accordance to ISO 8732 and ISO 11568. MPPE is established from a shared password/passphrase. The secure procedures for establishing, exchanging and frequency of change shall be agreed by Pathway and Post Office Ltd and documented in the OLA entitled '*DC Operational Level Agreement'*

Pathway is entitled to close down, so they are not available for use, the connections to the communication links between a single data centre and the MA for the purpose of maintenance, support, upgrade, repair or replacement of any equipment used to provide or support those links. Scheduled maintenance of any component of the data centres, which provide on-line service shall be carried out outside of the core hours of business.

FUJ00088068

Pathway is entitled to close down, restrict or prevent communications between both data centres and the MA subject to the DC MoP Functional Description, Section 12 Service Interface to MA as agreed with Post Office Ltd. in the OLA entitled '*DC Operational Level Agreement'*.

12.5 Audit and Alarms

12.5.1 Audit

Debit Card audit requirements are detailed in the Audit Trail Functional Specification (CR/FSP/006)

The statutory requirement for certification in accordance with the relevant sections of PACE (s69 and s70) no longer exists but Pathway ensures as far as possible that relevant information produced by the system at Post Office Ltd's request is admissible in support of prosecutions.

The confidentiality and integrity of sensitive data (e.g. DC Sensitive data) is maintained within the TMS journals on the audit archive by encrypting the value of the data. DC sensitive data extracted by Record Query and provide to Post Office in support of investigations and/or evidence for the resolution of disputes and prosecutions shall be in the encrypted form in which they are held by the TMS journal.

Pathway retains securely copies of the following encryption keys in compliance with the requirements of RIPA (2000):

- network encryption keys;

12.5.2 Alarms

In the event of a suspected key compromise, of any DC related key, key change mechanisms will be called into force.

Where a key is suspected of compromise, it will be changed such that the suspect key gives no information about the replacement key. In addition, any key directly or indirectly protected by the suspect key will also be treated as suspect.

The timing of any key change will take into account the nature of the security breach giving rise to the key change, its impact on system availability, and the presence of any compensating controls.

Where a suspected compromise affects the Horizon environment an enhanced capability of the existing KMA and manual procedures will be used to change keys within the Horizon system.

FUJ00088068

13.0 Administration of Security

Administration of security is largely concerned with management and operational controls but there are also supporting technical controls that are implemented.

System management facilities preserve the integrity of the system and contribute towards achieving high system availability. The software distribution facilities, in particular, incorporate mechanisms for integrity protection of all files/modules distributed to end systems.

User management is distributed because the bulk of the user population is managed as small groups local to each Post Office Outlet.

13.1 Management Roles and Responsibilities

Pathway's Security Policy [SECPOL] contains a definition of responsibilities for security within Pathway.

The Pathway Access Control Policy [ACCPOL] contains a detailed definition of roles and responsibilities for all personnel who have any kind of access to the services provided by Pathway.

The following subsections provide a simplistic overview of the operational, system management and support roles.

13.1.1 Operational Roles

The operational roles comprise the "users" of the system in its operational state, as follows:

- Post Office Manager (Post Office Ltd.), and
- Post Office Counter Clerks (Post Office Ltd.).

A distinction is made between the Post Office Manager and Post Office Counter Clerks.

13.1.2 Systems Management Roles

The system management roles ensure the system is running for the "users" in the operational roles. In simple terms, these are the roles for which Fujitsu Core Services have main responsibility, as follows:

- System Manager (Fujitsu Core Services),
- System Operator (Fujitsu Core Services),
- Database Administrator (Fujitsu Core Services/Oracle),
- Network Manager (Fujitsu Core Services), and
- Encryption Key Custodians (Fujitsu Core Services).

Encryption key custodians have responsibility for the use and safekeeping of encryption keys. These keys are used to enable the Rambutan based encryption devices at each site. For simplicity, Fujitsu Core Services manage all keys used in the central Data Centre site.

FUJ00088068

13.1.3 Support Roles

The support roles are primarily concerned with keeping all equipment operational. These activities, which include monitoring and exception handling, are supported (primarily by Fujitsu Core Services) as follows:

- Support Manager,
- Support Engineer,
- Support Help Desk, and
- Installation Engineer.

13.2 Systems Management Components

Systems management services are based upon three main products, namely:

- Tivoli (with Software Distribution, Event Console, Platform and Inventory),
- HP OpenView, and
- Patrol.

Tivoli handles all services on NT systems and central event management services.

HP OpenView (with Cisco Works) provides network management facilities and all services to the router community.

Patrols used to manage all Sequent systems and the Oracle applications that run on Sequent platforms.

13.2.1 Tivoli

The Tivoli Management Environment (TME) is a management environment used to provide application services and applications for client/server systems management.

Within TME, Tivoli provides applications that support:

- deployment management - involving installation, configuration, and control of all resources,
- availability management - involving local monitoring and local automation, and
- centralised event-based operations management - that enables system-wide monitoring, job scheduling, and system backup.

The foundation of TME is the Tivoli Management Platform (TMP) that provides all the common services and integration between TME applications via an open API.

FUJ00088068

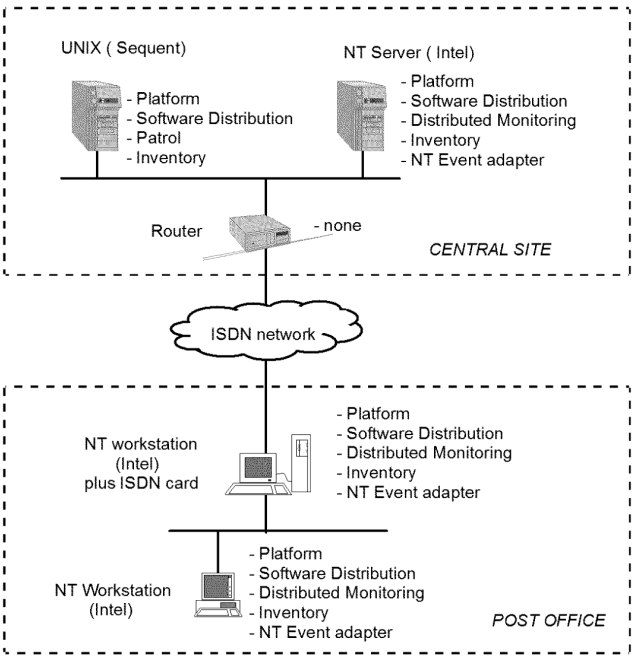

Figure 13.1 Deployment of Tivoli Products

Tivoli products are deployed as illustrated in figure 13.1.

13.2.1.1 The System Management (SM) infrastructure, provided by the Tivoli platform, is Object Management Group (OMG) Common Object Request Broker Architecture (CORBA) compliant.

A Tivoli event adapter is used to map Simple Network Management Protocol (SNMP) traps to the central Tivoli Event server. Similarly, a Patrol Tivoli Event Adapter maps Patrol events to the Tivoli Event server. Event management on Oracle uses Patrol.

13.2.2 HP OpenView

HP OpenView is used to provide the network management service.

13.2.3 Patrol

Patrols used to manage the Sequent platforms and the Oracle applications that run on those platforms.

13.3 Systems Management Services

The services provided includes:

- Software Distribution - using Tivoli Software Distribution,
- Event Management- using Tivoli Event Console and Patrol,
- Network Management - using HP OpenView,
- Resource Monitoring - using Tivoli Distributed Monitoring, and

FUJ00088068

- Inventory Management - using Bespoke Inventory.

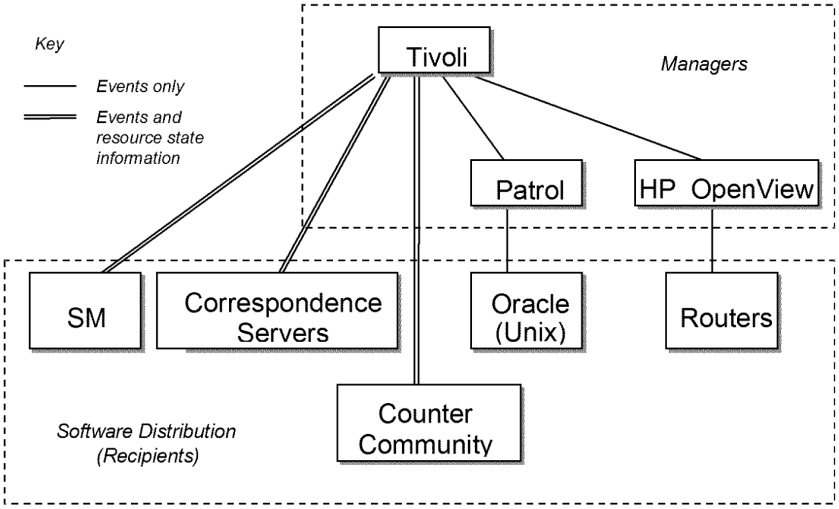

Figure 13.2 System Management Components

The three system management products (described in section 13.2) are combined as illustrated in figure 13.2

13.3.1 Software Distribution

The task of managing a distributed, multi-platform system requires an efficient method for distributing, installing and controlling software throughout the network.

The Tivoli Software Distribution management application provides the means of managing and distributing software across a multi-platform network that includes Windows NT platforms.

13.3.1.1 The software distribution system is used to manage end systems in order to distribute, activate and delete software products.

13.3.1.2 Tivoli runs within the authentication and access controls specified in this document.

13.3.1.3 Tivoli Software Distribution provides a full audit track of all distributions.

This indicates whether distributions are successful and whether any failures occurred. The time of successful distributions/failures also included together with identification of the individual who initiated the distribution.

Pre-requisites for software distribution, to maintain system integrity, are:

- a naming scheme for identifying the product(s) concerned,
- the ability to define a software product in terms of its constituent files,
- scripts to perform the installation (and removal) of the product,
- criteria by which it can be asserted that a software product is installed,

FUJ00088068

- a clear definition of the managed system(s), and
- identification of the managed network routes to the system(s).

This supporting infrastructure also provides:

- a scheduling infrastructure enabling operations to be executed at a defined time, and
- a reporting infrastructure to inform the central systems of the outcome of operations.

The four stages in the release management process, which includes package distribution, are illustrated in figure 13.3

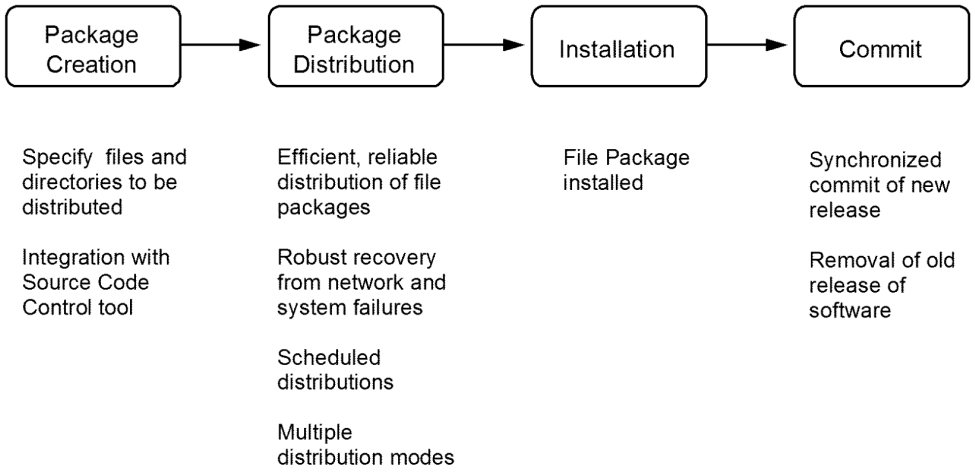

Figure 13.3 Release Management Process

Tivoli Software Distribution provides the ability to run programs:

- before or after distributing new software,
- immediately (when Commit is specified), or
- after removing old software.

These features are used to provide efficient and reliable installation of new software releases.

13.3.2 Event Management

Event Management is the ability to take events from one or more sources, use defined rules to establish whether local actions need to be taken and/or whether notification is to be forwarded to central event servers. Sources of such events include applications and the operating systems.

13.3.2.1 Wherever possible, existing technology for handling events are used, with the events mapped into a normalised form for handling by the central event manager.

13.3.2.2 The event logs used by Windows NT are integrated with the system management components.

FUJ00088068

13.3.2.3 Network components, which emit events as Simple Network Management Protocol (SNMP) traps, are integrated with the system management components.

13.3.3 Network Management

Network management runs from a central service providing facilities for:

- reporting and diagnosing network events,
- consolidating and interrogating statistics, and
- controlling the configuration and parameter settings on network devices.

The global system is divided into three levels for network management purposes:

1. The backbone network - comprising the LAN hubs and LAN attachments at the Pathway central sites, the links between the Pathway sites, links to Post Office Ltd., with associated routers.
2. The branch Fujitsu Core Services network - terminated at the central routers and at the gateway PC at each outlet.
3. The office LAN at each outlet - comprising the PC LAN attachments and local Ethernet hub (present where three or more PCs are installed).

Management of the underlying ISDN switched circuit network are provided by Energis. The implementation of Network Management includes interfacing to the Network service supplier to obtain a structured data feed regarding the state of the whole network including ISDN.

The network management facilities are based primarily upon the use of SNMP mechanisms, with additional facilities provided across the ISDN network at platform level via the Microsoft NT event system and associated middleware.

13.3.4 Resource Monitoring

13.3.4.1 The resource monitoring facilities are used to establish criteria for monitoring an individual resource.

13.3.4.2 When resource monitoring criteria are met, they will trigger pre-defined local action and/or generate an event.

Typically, notification would be provided when available free disk space has reached an appropriate threshold.

13.3.5 Inventory Management

13.3.5.1 Bespoke Inventory applications are used to manage the software and hardware inventory.

13.3.5.2 A central repository holds persistent records identifying the software products installed on each managed node.

13.3.5.3 The data recorded is obtained by evaluating the software signature for each software product on the nodes.

FUJ00088068

13.3.5.4 The central repository holds persistent records identifying the hardware associated with individual managed nodes and its attached peripherals.

13.3.5.5 Where appropriate, asset numbers are held for the individual components.

13.4 User Management

The user management facilities provided by Riposte, and its associated applications, are used to manage all Post Office Outlet users within the OPS Domain. For all other users, facilities provided by the standard COTS products will be used for administration tasks.

13.4.1 Administration of User Accounts

The majority of users are Post Office staff within the Office Platform Service Domain.

Each Post Office Manager manages the small group of Post Office Counter Clerks within their Post Office Outlet as a local community. The interface used provided by Riposte maps to the underlying Windows NT functions.

Within the central sites, Pathway's system administrators are responsible for managing user accounts on the Sequent (Dynix), Windows NT platforms and routers using the standard facilities.

13.4.2 Administration of Access Controls

Access controls are configured in accordance with [ACCPOL] using the facilities outlined in section 6.0.

FUJ00088068

APPENDIX A WINDOWS NT AUDIT EVENTS

Windows NT provides essentially the same audit capability for both workstations and servers. The audit and alarm events selected, however, depend upon the usage of platform.

Windows NT File and Directory Access

Table A-1explains how each type of access is interpreted in terms of Windows NT files and directories.

Type	File Access	Directory Access
Read	Displays the file's data	Displays names of files in the directory
	Displays the file attributes	Displays directory attributes
	Displays the file's owner and permissions	
Write	Changes the file	Changes directory attributes Changes sub-directories and files
Delete	Deletes the file	Deletes the directory
Change Permission	Changes the file's permissions	Changes directory permissions
Take Ownership	Changes the file's ownership	Changes directory ownership
Execute	Runs the file	Displays the directory's owner and permissions

Table A-1 Windows NT File and Directory Access

FUJ00088068

Windows NT Registry Audit

The Windows NT Registry Key Auditing dialogue box can be used to select the auditable event categories defined in table A-2.

Registry Audit Option	Audit events that attempt to:
Query Value	Open a key with Query Value access
Set value	Open a key with Set Value access
Create Subkey	Open a key with Create Value access
Enumerate Subkeys	Open a key with Enumerate Subkeys access (i.e. events that try to find the subkey of a key)
Notify	Open a key with Notify access
Create Link	Open a key with Create Link access
Delete	Delete the key
Write DAC	Determine who has access to a key
Read Control	Find the owner of a key

Table A-2 Interpretation of Windows NT Registry Audit Options