POL00401199

Document Title:	Access Control Policy
Document Type:	Policy Document
Abstract:	This Access Control Policy (ACP) defines the policy for controlling access to resources in the operational Pathway system.

Distribution:		
	Ian Bowen	Mik Peach
	Gerry Boyce	Barry Procter
	Alan D'Alvarez	Martin Riddell
	John Dicks	Glenn Stephens
	Peter Dreweatt	Chris Sundt
	Mark Fisk	Chris Wannell
	Peter Harrison	Frank Womack
	Dave Jones	Horizon
	Graham Lloyd	Pathway Management
	Tom Parker	Pathway library

Document Status:	Approved
Document Predecessor:	-
Associated Documents:	See section 0.2
Author:	Belinda Fairthorne
Approval Authority:	John Dicks
Comments To:	Author, copy to John Dicks
Comments By:	-

POL00401199

0.CONTENT

0.1 Document History

Version	Date	Reason
0.1, 0.2	28/10/96	Initial drafts for review by security team
0.3	7/11/96	Initial Draft for internal Pathway review
0.5	6/12/96	Response to comments; Addition of new information including Pathway Corporate Services domain, Network Management
0.6	4/3/97	Further clarifications in many areas including network, Sequent access, Post Offices
1.0	16/4/97	Terminology changes. Major updates to the Post Office section have been made. Numerous minor changes have been made.
1.1/3		See separate note
2	23/2/98	Draft version of 1.3.
2.1, 2.2	sep/oct 98	See separate note Approval responsibility passed to John Dicks
3.0	18/12/98	Minor updates, see separate note. For approval

0.2 Approval Authorities

Name	Position	Signature	Date
John Dicks	Customer Requirements Director		

POL00401199

0.3 Associated Documents

Ref:	Title	Identifier	Vers.	Date
SADD	Service Architecture Design Document	CR/FSP/004	5.1	23/7/98
TED	Technical Environment Description	TD/ARC/0001	4.2	13/10/98
SPOL	ICL Pathway Security Policy	RS/POL/0002	3.3	23/2/98
SFS	Security Functional Specification	RS/FSP/0001	3.2	5/8/98
CHDM	PAS/CMS Help Desk Call Enquiry Matrix	CS/FSP/0003	2.5	13/10/97
AUDT	Audit Trail Functional Specification	CR/FSP/006	2.2	8/9/97
BS7799	A Code of Practice for Information Security Management	BS7799	1	15/2/95
DSPOL	DSS IT Security Policy (Departmental IT Security Standards)	DITSG/ITSS/0001.04	6.2	3/96
PPOL	Post Office Counters Information System Security Policy	SRR Appendix 4-1		

0.3 Abbreviations

ACP	Access Control Policy
BA	Benefits Agency
BES	Benefit Encashment Service
BPS	Benefit Payment Service
CAPS	Customer Accounting and Payments System
CAW	Certification Authority Workstation
CESG	Communications-Electronic Security Group
CFM	ICL Outsourcing (Client Services Ireland)
CLI	Calling Line Identification
CMS	Card Management Service
CS	Pathway Customer Services
DBA	Database Administrator
DSA	Digital Signature Algorithm
DSS	Department of Social Security
ECCO	Electronic Cash Registers at Counters
EPOSS	Electronic Point Of Sale Service
ESNS	Electronic Stop Notice System
FCMS	Fraud Case Management Service
FRM	Fraud and Risk Management
FTMS	File Transfer Management Service
HAPS	Host Automated Payment Service
HFSO	Horizon Field Support Officer
ISDN	Integrated Services Digital Network
IT	Information Technology

POL00401199

KEK	Key Encryption Key
KMA	Key Management Application
LAN	Local Area Network
MIS	Management Information Services
NAO	National Audit Office
NMS	Network Management Station
NSI	National Sensitive Indicator
NT	New Technology (Microsoft's operating system)
OBCS	Order Book Control Service
PAS	Payment Authorisation Service
POCL	Post Office Counters Ltd
PUN	Pick Up Notice
RDMC	Reference Data Management Centre
RPC	Remote Procedure Call
SMC	System Management Centre
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSC	System Support Centre
TACACS+	Terminal Access Controller Access Control System +
TIP	Transaction Information Processing
TME	Tivoli Management Environment
TMS	Transaction Management Service
TPS	Transaction Processing Service
VME	Virtual Machine Environment
VPN	Virtual Private Network

0.4 Changes Forecast

In some areas of Pathway, design for future releases is not yet finalised or changes or additions to the Pathway solution are being considered. While this document normally states the policy in these areas, details are subject to change as indicated in the relevant section. The main such areas are listed below.

- Changes as the results of new services added or extensions to existing ones
- Some aspects of network access controls
- Cryptography/key management design for later releases
- Some details of support from remote sites
- Some aspects of Pathway system auditing; archives and access to them
- Some aspects of future software distribution and auto-configuration
- Telephone authentication procedures

POL00401199

POL00401199

POL00401199

0.5 Table Of Contents

[TOC \O "1-3" \T "APPENDIX 1,1"]

1.

POL00401199

INTRODUCTION

1.1 Purpose

This Access Control Policy (ACP) defines the policy for controlling access to resources in the ICL Pathway IT system.

Effective control depends on having a clear definition of the roles and responsibilities of all personnel who need some form of access to the system. This document defines the operational, management and support roles required in the Pathway system, and the main functions which people in those roles carry out. It then defines the policies for controlling the access to the Pathway services - both by these people and by other system users.

1.2 Context

This document fits into the structure of documents for Pathway security as illustrated in figure 1-1 below.

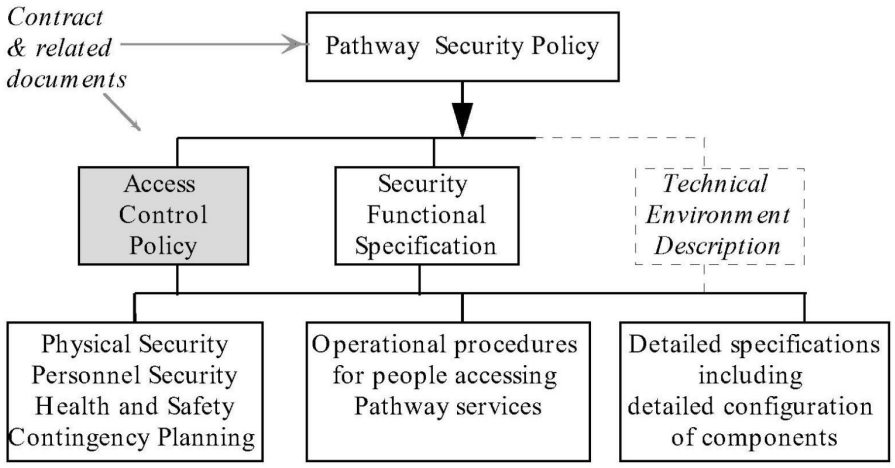


Figure 1 - 1 Pathway's Security Documents

The Access Control Policy defines how access is controlled throughout the Pathway system in compliance with the Pathway Security Policy.

The Security Functional Specification defines the security functionality that will be incorporated into the ICL Pathway system.

The Technical Environment Description describes the architecture and technical environment for the Pathway solution, including the security architecture.

POL00401199

Other security processes define, for example, the physical security of information and machines and personnel security including storage of workstation keys and tokens. Personnel procedures include staff vetting. There are also plans for business continuity after a major incident.

There are also procedures for people using Pathway services. For example, there are procedures associated with entering a site, using the system, safeguarding of manual records and handling security incidents. These will be checked for compliance with the Pathway security policies and specifications by the Pathway Security Manager. Section 3.8 outlines the implications of the Access Control Policy on these procedures and identifies the key ones.

There are also specifications defining how the various Pathway components are configured to meet this policy. These will define, for example, which functions in which applications are available to people in particular roles and the database views available to each role.

1.3 Scope

This Access Control Policy defines how access to information system resources is controlled in the operational Pathway system. It includes:

- General access control policies for Pathway
- The principles of how the access controls should be configured - which roles should be set up with what responsibilities and what categories of functions people in those roles should be permitted to do
- How the security functionality defined in the [SFS] is used to achieve that. For example, how people in different roles are authenticated, how access to the permitted functions is achieved.
  This covers functions performed in the information system as the result of direct user action, and those cases where the user of the system is carrying out a function on behalf of someone else, often as the result of a telephone call requesting use of the system.

This document is concerned with what can be accessed by whom and how within the Pathway information systems rather than the detailed procedures for configuring and running these systems. Separate Pathway documents as described in 1.2 above define these related standards and procedures.

POL00401199

This policy covers the Pathway operational and management systems at the Pathway Data Centres plus closely associated systems. Separate internal Pathway documents cover system development and test systems and other activities prior to the handing over of the software for operational use.

1.4 Access Control Policy Review

This document will be formally reviewed at least annually. It will also be reviewed where relevant after a significant security incident, as part of a more general security policy review, and updated whenever necessary.

Responsibilities for approval, review and issue of this document will conform to the review procedure for Pathway policy and standards defined in the Pathway Security Policy.

1.5 Document Structure

Section 2 of this document identifies the Security Domains of the Pathway system and outlines the main functions in each. It also identifies related internal Pathway systems and other sites which access the Data Centres.

Section 3 specifies the Pathway wide access control policies. It defines the generic roles which should be supported at most of the Pathway systems and the general policies and controls which apply to them all. Configuration of any Pathway platform should conform to this section as well as to the more specific controls in the appropriate later section.

Sections 4 to 8 specify the access control policy for each Domain/sub-domain in turn. For each, it defines the roles with access to services there. Note that some roles are system wide (particularly system management and Pathway corporate ones) so are referred to in each domain where they require access (as the systems there must be configured to support them) but the full definition of these roles is in either the System Management or Corporate Services Domain.

In some cases, the same roles and controls apply to a number of domains. For example, the same Sequent system supports both the PAS/CMS services and other Pathway application hosts so most of the management and support roles are in common for these. In these cases, the roles and access controls are defined once and other sections refer to this definition, though may also have extra roles specific to the particular service or domain.

So the access controls for a particular system are:

POL00401199

- The general controls in section 3 (which apply to all systems)
- The generic controls for that type of system, where relevant (e.g. specific controls associated with Sequent or NT at the Data Centres - see section 4)
- The controls for the particular service/system

Appendix A gives a summary of all the roles with references to the sections where they are described.

POL00401199

2. SECURITY DOMAINS

The Pathway system can be viewed as a number of "domains" which together provide the Pathway solution.

2.1 Domain Definition

A "domain" is a distinct part of the system characterised by the IT services it provides and the components it uses to provide those services. The services offered by several domains combine to provide the end-to-end services, such as the Pathway Benefit Payment Service (BPS).

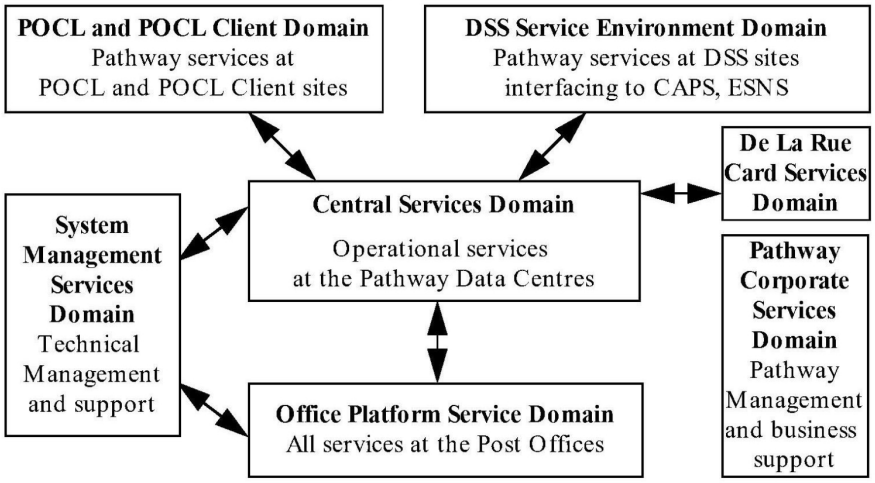


Figure 2 - 1 Pathway Domains

Figure 2-1 illustrates the domains and the primary links between them, except for links with the Pathway Corporate Services. Note that the System Management Domain also has links with all other domains.

2.2 Specifying Access Control Policies

For each domain, or set of domains, the Access Control Policy includes:

- An introduction to the main services provided by the domain - both automated and human initiated ones.
- An outline of the operational, management and support roles of people with access to services in this domain. For each role, there is a description of the main classes of functions performed and the access controls in the information system.
- The access controls resulting from the way the system is configured, for example, providing the base level of controls against general unauthorised access and restricting traffic to that permitted.

POL00401199

2.3 Services involved in Business Operations

The main operational flows of the Benefit Payments Service and other Post Office operations involve the domains illustrated in figure 2-2. These domains are described in the following sub-sections.

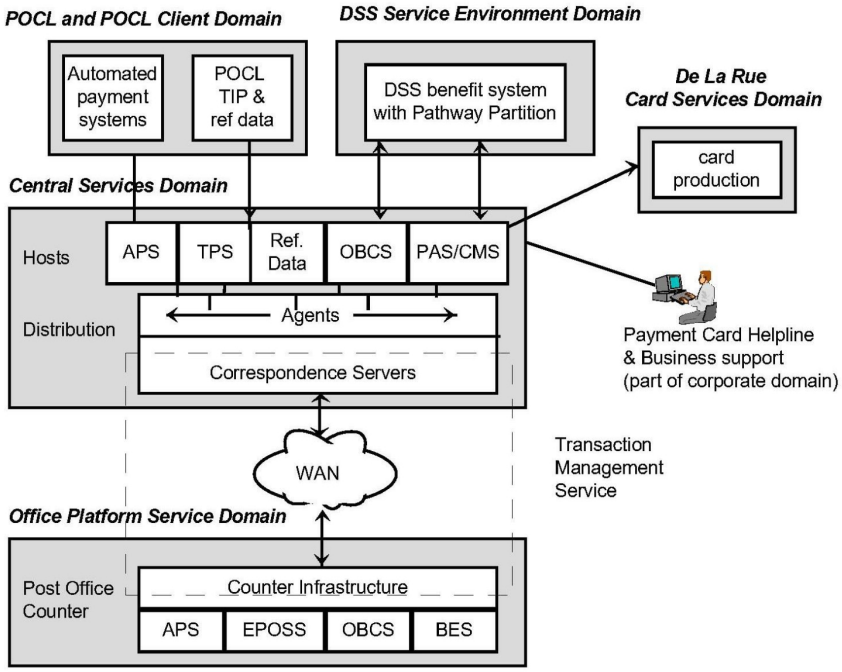


Figure 2 - 2 Domains directly involved in business operations e.g. benefit payments

2.3.1 The DSS Service Environment Domain

The DSS Customer Accounting and Payments System (CAPS) handles benefit payment authorisations. The DSS Electronic Stop Notice System (ESNS) handles Order books for benefits.

Pathway's responsibility in this domain is to accept Benefit related data generated by CAPS (or ESNS) and return data to CAPS (or ESNS) via Pathway software in a partition of the VME system and routers.

2.3.2 The POCL and POCL Clients Domain

The POCL TIP system receives records of transactions at Post Offices. Another POCL system provides reference data for applications such as EPOSS.

The POCL Automated Payments system (or later, POCL Client Systems) process Automated Payments on behalf of POCL Clients.

POL00401199

The Pathway Access Control Policy is concerned only with that part of the interface to these systems which is the responsibility of Pathway.

2.3.3 The Central Services Domain

The Central Services Domain provides the Pathway application hosts at the central Pathway sites to support all the Post Office applications (APS, EPOSS, OBCS). All these run on Sequent machines and use Oracle.

For benefit payments, information is transferred to/from the DSS Services to the Pathway Payment Authorisation Service(PAS) and Card Management Service (CMS). PAS/CMS process the payment authorisations and customer information for forward transmission to the Post Office or Card or Temporary Token Producer as required, and return information on transactions to CAPS.

TMS Agents assemble information from these hosts for distribution to the Post Offices. The Correspondence Servers are the central part of the Riposte Transaction Management Service and distribute information to/from the Riposte journals at the Post Offices. The Correspondence Servers and their associated agents, run on Windows NT platforms.

This domain also includes related services such as the Key Management Service used to generate and distribute keys within the Central Services Domain and to Post Offices.

The Central Service Domain spans two sites (Bootle and Wigan) which are often referred to as the Pathway Data Centres.

2.3.4 The Office Platform Service Domain

The Office Platform Service Domain encompasses all Post Office sites as illustrated in the fourth box in figure 2-2. All services run on Windows NT workstations. The main services supported are:

- The Electronic Point of Sale Service (EPOSS),
- The Benefit Encashment Service (BES),
- The Automated Payment Service (APS), and
- The Order Book Control Service (OBCS).

2.3.5 De La Rue Card Services Domain

The De La Rue Card Services Domain encompasses the facilities used for the production of cards, Pick UP Notices (PUNs) and temporary tokens.

POL00401199

2.4 Other Domains and Related Services

There are two other domains which are concerned with the management of Pathway. Both interact with the services in the operational domains.

- The Pathway Corporate Services domain includes Pathway's own management and business support processes including security ones.
- The System Management and Support Services domain manages the hardware and software systems which make up Pathway.

Some internal ICL systems are also used in support of Pathway operations.

2.4.1 Pathway Corporate Services Domain

The Pathway Corporate Services domain supports Pathway's own management processes such as reporting, accounting, monitoring service levels and Pathway's fraud risk management and auditing processes. It also contains business support processes:

- The Payment Card Helpline, which responds to DSS, POCL and general public queries about benefit cards and payments.
- Pathway Business Support which handles financial reconciliations, for example, of benefit payments after a Post Office problem

This domain includes a Data Warehouse which gathers information from the operational system and a Financials System.

2.4.2 System Management Services Domain

The System Management Services Domain contains the services required to manage and support the Pathway services in the other domains - both during operational running and roll-out of new Post Offices.

System Management facilities include Software Distribution, Event Management, Resource management, Inventory Management and Network Management.

The Tivoli Management Environment (TME) provides the Central System Management co-ordinating input from other management software such as Patrol, which is used to provide event and resource management of the Pathway Sequent systems, and HP Open View (with Cisco Works) which is used for management of the routers.

Roll-out of new Post Offices is controlled by a Roll-out database and associated facilities for auto-configuration of the Post Offices.

POL00401199

Support facilities include technical support of applications and hardware.

The Horizon System Help Desk provides technical assistance on hardware, software and network problems, calling on others when needed. The Roll-out Support Desk supports the roll-out process.

2.4.3 Internal Pathway Services

A number of internal Pathway services interact with Pathway operational and management services at the Pathway Data Centres. These include:

- The Powerhelp and PinICL systems which record and maintain information about calls to the technical Help Desks and their progress. Associated systems are used in support of lost keys and passwords at Post Offices.
- The Dispatch-1 system which holds hardware inventory information

2.5 Pathway Sites and Responsibilities

The main Pathway services run at the secure Pathway Data Centres at Wigan and Bootle. This includes:

- The operational systems of the Central Services Domain including application hosts, agents and Correspondence servers
- The Management Information Services of the Pathway Corporate Services Domain
- The System and Network Management services and services supporting the implementation of the Post Offices.

The main operational and management services can be run at either site, if needed, though there is a prime site for each. Figure 2-3 shows the sites with electronic links to the Pathway Data Centres.

POL00401199

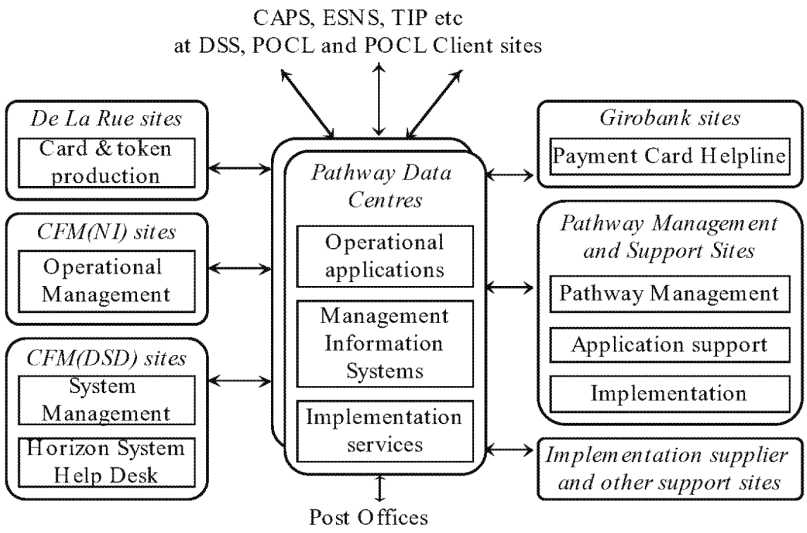


Figure 2-3 Sites with links to the Pathway Data Centres

ICL Pathway has overall responsibility for the design, development, test, implementation and operation of the Pathway services. Specific activities are subcontracted to appropriate organisations as identified below.

- **De La Rue/Thomas De La Rue** manufacture cards, Pick up Notices (PUNs) and temporary tokens, which are subsequently distributed by Royal Mail. De La Rue are located on De La Rue sites (e.g. Tewkesbury).
- **ICL Outsourcing** (Client Services Ireland) is responsible for the operational management of the Sequent and other systems at the Pathway Data Centres. They are also responsible for application support of some applications on Sequent and VME. They are located mainly at Belfast.
  They are also responsible for Network Management, which is done at the Data Centres, though it manages routers on other sites also.
- **ICL Outsourcing (Distributed Services Division)** is responsible for the overall System Management of the Pathway information systems, including software distribution, event and resource monitoring. They are located at Stevenage, Lytham St Annes and one other site.
  The Horizon System Help Desks and associated call handling system and hardware inventory systems are also at ICL Outsourcing sites.
- **Girobank** run the Payment Card Helpline. These are at the Wigan and Bootle sites, but in separate areas from the Pathway Data Centres. Help Desk advisors have interactive access to the PAS/CMS database.

POL00401199

- The ICL **Pathway project** runs Corporate Services including Management, Auditing and Fraud and Risk Management. It also manages implementation of the Horizon system at the Post Offices supported by **Implementation suppliers** from other organisations such as Peritas for training, Workplace Technologies for site preparation and Exel for shipping and installation.
  Pathway project users are mainly at Feltham, though there are also secure sites at Bracknell and Kidsgrove. The Pathway Implementation unit also has Regional offices. Implementation suppliers access authorised implementation systems from their own sites.
- The Pathway System Support Centre - **SSC**, provides 3rd line support for most applications and packages including Riposte. They are located at a secure Pathway site (Bracknell).
- On site hardware support at the Data Centre is provided the appropriate organisations. For example, Sorbus support the NT systems and Sun the Solaris systems. These roles generally do not require on-line access.
- Under exceptional circumstances, ICL Outsourcing or SSC need 3rd or 4th line support from other organisations for software in the Pathway system. For the following support organisations, controlled on-line access from their own sites is being considered:
  - **Sequent** supports the Dynix operating system.
  - **Oracle** provides 3rd line support for Oracle databases and applications.
  - **Cisco** supports the routers.
  - **EMC** supports the Symmetrix discs.
  - **General Signals** provides support for the Symmetrix/Energis link.

  No other organisations will have on-line access to the system. For example, there is no on-line access by Microsoft for NT support or by Escher for Riposte support.
- **Sorbus/Exel** will provide Engineers for Post Office roll-out.
- **EDS** runs the DSS CAPS system and the firewall between it and the Pathway systems
- **Girobank** also perform Fraud Risk management functions.
  This is at Bootle, but in a separate area from the Pathway Data Centre.

POL00401199

The Pathway Access Control Policy covers control of access to resources in the Pathway operational systems by all these organisations. It also covers access to Pathway services by other organisations - particularly Post Office staff accessing the Post Office systems. Other external access includes, for example, by POCL auditors and the DSS Fraud Investigation Team.

Later sections define the permitted accesses between these sites.

POL00401199

3. PATHWAY WIDE ACCESS CONTROL POLICY

This identifies the overall policy and associated procedures and controls which apply across the whole of the operational Pathway system.

Sections 4 to 8 deal with the procedures and controls in different Pathway domains.

3.1 Objectives

The Pathway Security Policy specifies the following IT security objectives for Pathway. This Access Control Policy defines how controls of access to resources are used in achieving the following objectives.

1. Security measures in Pathway's IT systems will ensure appropriate confidentiality, integrity and availability of data, whether in storage or in transit. Maintaining the integrity of the services and software components is also essential.
2. Physical and logical access to the system will be controlled, with access granted selectively and permitted only where there is a specific need. Access will be limited to persons with appropriate authorisation and a "need to know" requirement.
3. Authentication, whereby a user's claimed identity is verified, is essential before any access is granted to the system. Authentication mechanisms are also required to ensure that trust relationships can be established between communicating components within, and external to, the system.
4. All users of Pathway's services will be individually accountable for their actions. Accountability for information assets will be maintained by assigning owners, who will be responsible for defining who is authorised to access the information. If responsibilities are delegated then accountability will remain with the nominated owner of the asset.

The Pathway Security Policy also specifies objectives for auditing, alarms and monitoring of the system. These are only of concern to this Access Control Policy in as much as they are part of the functionality of the system for which access must be controlled.

3.2 Pathway Roles

Responsibility for performing functions within the Pathway system is allocated on the basis of roles. This document identifies the following types of human roles:

POL00401199

- **Operational roles** of the users of the system during normal running. These include, for example, the Payment Card Helpline Advisors and the Post Office Counter Clerks.
- **System** and **Security Management roles**. These are the people who are responsible for maintaining and monitoring the system, including adding new software and users.
- **Support roles** such as engineers and application support

People in specified roles are permitted to carry out defined functions, normally by controls within the Pathway information systems. In a few cases, manual procedures are used to supplement these.

Pathway controls which people can carry out which roles, and therefore perform which functions. However, users are individually identified so that they can be made accountable for their actions.

Roles are defined to support the functions in each of the Pathway domains defined above. Where practical, the same or similar roles are defined for several domains to reduce complexity and make it easier to check compliance with the overall security policy. The following subsections identify roles and major functions used in most Pathway domains. In some domains, several of these functions are available in one role to simplify administration where separation of these duties is not required. This is defined in the more detailed sections of this document about the individual domains. Several domains have specific requirements which require use of particular roles.

A limited number of roles are "pathway wide" and so recognised in most Pathway domains. These are the Pathway management roles which allow auditing and investigation of all Pathway systems.

The Access Control Policy includes all roles for users who have direct access to the Pathway operational systems and the related systems at the Data Centres. In addition, this document includes a limited number of roles of users who cause others to use the system on their behalf, for example in response to a phone call.

Note that as many of Pathway's operations are automated, access by systems entities, for example, particular applications, must be controlled as for human access to the system. This Access Control Policy covers access by such system entities, but does not define roles for them.

POL00401199

3.2.1 Operational Functions

It is Pathway policy to automate the operation of Pathway applications where practical, thus reducing the need for human intervention and associated access controls. Operational applications are automated at the DSS/BA, POCL and Pathway Data Centres, as are transfers of data to/from them and the Post Offices. Processes are initiated as the result of some event such as the receipt of data. In these central domains, no human intervention is required unless some exception condition occurs or a query is received at the Help Desk. Control of access to resources for automated processes results from the way the system is installed and configured.

The operational roles are different in each domain. For example, there are Pathway management functions at the Corporate services domain. At the Post Office, operational roles are the Post Office Manager, Supervisor and Counter Clerk. These should be taken as also referring to the equivalent staff in franchises and Sub Post Offices including Sub Postmasters and their staff.

3.2.2 Common System Management Functions

Functions to manage and administer systems are required in all domains. Note that many such system management functions are done remotely from the systems being managed.

The main management functions for a system in any of the domains (for example, a Sequent machine supporting the PAS/CMS Services or a Post Office set of counters and LAN etc) are as follows:

- **System set-up and installation**: setting up the base and application software on the system and configuring it for live running. On installation of some systems, cryptographic keys will also need to be installed- see security management roles.
- **Software Update**: updating the software and reconfiguring it. Most updates to software are done automatically by system management. However, some base software updates need to be done manually on site.
- **System Management:** monitoring events and resources in the operational system and taking appropriate action to rectify problems. Also, distributing software (complete new packages or patches).

POL00401199

- **Operational Management** (sometimes called **System Administration**): keeping the system running - responding to incidents, keeping it correctly configured (where this is not done by system management). This is mainly concerned with operating system management, but may also involve some database administration.
- **Computer operator**: in most domains, this is a minimal role involving switching on the machine, loading media and similar operations. (Most management of the system is done as part of other management roles.)
- **Package Administration:** Pathway uses a number of packages to handle resources. The key packages and functions associated with them are:
    - **Oracle Database Administration.** This includes administering the database structure set up and maintenance.

      Access to databases is often controlled by packages such as Discoverer and Business Objects which also require administration.
    - **Riposte Administration.** Management of Riposte message stores and groups is largely done automatically.
    - **Tivoli Administration.** This is used to configure what Tivoli manages and set thresholds etc. (Specifying the Tivoli roles and regions etc is also a security management function). See section 8 for more about Tivoli.
- **Application Management**: Managing the running of the applications themselves where human intervention is needed.

Note that some of these functions are carried out in the System Management Domain. Further management functions there are:

- **Network Management**: managing the network, including routers and firewalls, which connects machines and domains together.
- **Implementation management:** managing the roll out of the Pathway solution to Post Offices.

3.2.3 Common Security Management Functions

There are a number of management functions particularly concerned with security. In practice, these will often be performed by people in other management roles, but in that case, are defined as part of the responsibilities for that role. Security management functions are:

POL00401199

- **User administration**: administering user security information such as their authentication information, the roles they can perform and the groups they belong to. It may involve operating systems (e.g. Dynix, NT) and packages (Oracle, Riposte, Tivoli) etc. It may be split into:
  - initial set up of roles/groups and key users
  - individual user management, including removing the rights of users who have changed jobs or left the organisation
  - periodic checks for, and removal of, redundant users
- **Resource access control**: administering who can access which resources in the operating system, database or applications. Unless otherwise stated, human user access to resources is based on role rather than individual user identity. This is generally done as part of the management or administration of the particular system, package or application.

In addition, there are Pathway wide roles for **Security Event Auditing** and **Cryptographic Key Management** (see 3.2.5).There may be local auditing functions in some areas as well as the Pathway wide function.

3.2.4 Common Support Functions

Support functions are primarily concerned with:

- Keeping applications operational
  Application support, including diagnosing application problems at the Post office, is mainly done remotely.
- Training staff to carry out their defined roles.
  On-line training is provided at Post Offices and Payment Card Helpline.
- Keeping all equipment operational. This includes:
  - Running diagnostic applications to check for equipment faults (at the Post Office, done by the Post Office Manager, as well as engineers,)
  - Installing new Post Offices; done by **Installation Engineers**
  - Replacing and reconfiguring hardware; done by **Support Engineers.** This includes network boxes as well as NT and UNIX systems.
  - Technical Help Desks for reporting, and getting advice on, problems

3.2.5 Pathway Wide Roles

People in the following roles have access to several of the domains:

POL00401199

- **Pathway Business Support**. This role supports the business operations. For example, it handles financial reconciliation of payments.
- **Pathway Fraud and Risk Manager** (FRM). Concerned with identifying, monitoring and managing fraud, particularly in benefit payments.
  While much of this is done using MIS systems, FRM staff also access operational Pathway systems such as the TMS journals and PAS/CMS data.
- **Pathway Security Manager:** Responsible for managing security tokens for all Pathway users authenticating using tokens, and also other functions.
- **Pathway Cryptographic Key Manager**: Responsible for generating and distributing keys all cryptographic keys used in Pathway to protect communications links, digitally sign information and encrypt filestore.
  The Key Manager will delegate some responsibility for installing and updating keys to Pathway **Cryptographic Key Custodians** and **Cryptographic Key Handlers.**
- **Pathway Security Event Auditor:** Responsible for auditing all use of the Pathway systems, so requiring access to most of the Pathway systems. (Access to the Post Offices is not required, as TMS provides sufficient records of Post Office activity at the Pathway central site.)
- **Pathway Business Function Auditor:** Responsible for general auditing of the Pathway system focusing on business, rather than security, auditing. Note that the Pathway Security Event Auditor and the Pathway Business Function Auditor access much of the same information (though look at it differently). Therefore the term **Auditor** (meaning both these auditors) is used where both have the same access to systems.

These Pathway Management roles are described further in section 7 on the Pathway Corporate Services Domain.

3.2.6 External Roles

In addition to the Pathway roles defined above, POCL customers use the system indirectly at the Post Office (see section 5).

Some people in POCL, DSS/BA and others also access the system. These are:

POL00401199

- **POCL Auditors, Investigators** and Emergency Managers who can access services at Post Offices as described in chapter 5. They also have access to audit information at the Data Centres via Pathway Auditors - see 7.6.
- **DSS and NAO Auditors** have similar access to central audit information.
- **Benefit Agency staff** use the on-line CAPS interface, for example, to make emergency payments or stop cards or payments.
- **DSS Help Desk** staff are expected to use the on-line CAPS interface for queries e.g. on authorised payments.
- **DSS Fraud Investigation Team** access the FRM database and a limited amount of information in the Data Warehouse - see chapter 7.

POCL, DSS and NAO Auditors also have access to audit information at the Data Centres. Initially this will be provided via Pathway Auditors, rather than by these auditors having direct access to the Pathway systems. Note that in this document, POCL, DSS and NAO Auditors are often referred to collectively as External Auditors and are shown as being subject to the same access controls. However, there are some differences in data available to different External Auditors in line with [AUDT]. For example, DSS staff cannot access POCL specific data.

3.3 Types of Information and its Use

The Pathway Access Control policy protects information in all Pathway systems. For example, benefits information is protected from its receipt from DSS/BA through its processing in Pathway and at the Post offices to the return of transaction information to BA/POCL. This includes protection of information during fault investigations and correction and information retained for auditing and fraud investigation.

Information in the Pathway system includes:

- The business data such as the payment authorisation data to support the PAS system, the reference data to support EPOSS and the transaction data resulting from Post Office counter activities. This is stored at the main operation systems and also in archives. Some data is also available for management services at the Data Warehouse.
- Training information - special business style data used in training sessions
- On-line documentation e.g. Payment Card Helpline procedures, Post Office procedures
- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc.

POL00401199

- Security information about users, keys, security audit logs etc

Most processing of the business information, except at the Post Office, is automated and therefore not subject to human access. Most processing of system data is also automated.

All information is protected in conformance to the Security Functional Specification and Pathway Security Policy.

3.3.1.1 DSS and related business data is classified as RESTRICTED according to the UK government classifications and must be protected accordingly. Access to data with a National Sensitivity Indicator is further limited to authorised staff.

3.3.1.2 Where human access to this information is needed, for example by Help Desks and for system management, the information should only be accessible to those with a need to see it according to their role.

3.3.1.3 Information in transit between systems should be encrypted for confidentiality and/or integrity according to the needs of the particular link as defined in the Security Functional Specification [SFS].

3.3.1.4 Digital signatures should be used for integrity of business information between the Post Offices and other services where required. For example, payment authorisations sent from Pathway are signed; Automated Payments are signed at the Post Office prior to transmission via Pathway to POCL or POCL Clients.

3.3.1.5 System data should also be integrity protected when required. Digital signatures are used for integrity protection of software and scripts distributed to the Post Offices and elsewhere. Appropriate key distribution protocols as defined in [SFS] are used to protect all cryptographic keys.

3.3.1.6 Business information in filestore at the Post Office PCs should be encrypted.

3.3.1.7 Information in relational databases should be accessible only via authorised client "applications" (such as Oracle Forms, Discoverer, Business Objects, Tivoli database interfaces) except where there is a proven need for lower level access. Lower level access will only be granted for agreed operational management and support functions.

POL00401199

3.3.1.8 System Management actions by Tivoli should be activated using pre-defined Tivoli tasks, authorised for use by SMC and the Pathway configuration management and software distribution process. This includes collection of diagnostic information from the Post Office for application support.

3.3.1.9 RESTRICTED data on discs and other media (including printed output) should not be accessible for unauthorised use. For example, archives should be stored securely; information on faulty discs removed from service should be inaccessible.

3.3.1.10 Information should be appropriately separated in filestore, database tables etc. Each data set should be accessible only to those with a need for that access.

3.4 Information System Controls

3.4.1 Implementing Role Based Access Controls

Human user access to the functions of the system is controlled according to the user's role. Authentication procedures prove the user's identity. Authorisation procedures check the user's right to carry out the role. Access controls functions associated with resources will check that the user with this role is permitted to access the resource.

The way roles and the associated access controls are implemented in the information systems depends on the products used. For example, Oracle and Tivoli support roles, so can use roles directly in access control lists (rather than identity). Other products such as Riposte, UNIX and Windows NT support groups which can be used to represent roles.

Implementing role based access control involves:

- Administering information about users including role/group (as well as identity), authentication information (such as passwords) and other security relevant information associated with users in this role such as operating system privileges, database views.
- Authenticating users via the appropriate method for someone in that role at that location. At some locations, such as the Post offices, permitted roles/groups are automatically associated with a user when the user logs on. At other locations, the users are given limited privileges on log-on and have to ask for others, though will still be restricted to authorised privileges. (This particularly applies to some management functions. For example, no user is allowed to log onto UNIX with root access, though may be permitted a controlled change to root access later - see 3.4.2.15.)

POL00401199

- Administering access control information associated with resources e.g. which users in which roles with which privileges can access which resources (files, data and other objects) in which ways.

Roles will normally be associated with major functions. Defining separate roles allows different functions to be allocated to different individuals. However, the actual allocation of roles to individuals is done by administrative action. Some users can be permitted to carry out more than one major function, so are permitted to take more than one "role", but this will not be done where it might undermine security.

The way individuals are allocated to roles depends on the products used in the different Pathway domains and is defined further in the later sections of this document. Some general principles apply:

3.4.1.1 The principle of "least privilege" should apply to restrict the access rights of users.

3.4.1.2 Duties of different users should be separated to minimise the damage that any one user can do to the system or the information in it.

3.4.1.3 If a role at a particular location is allocated to a single person, there should generally be at least one other person who can deputise for that person. (At small Post Offices where no deputy is available, if the Post Office Manager is unavailable, the Post Office will not open until emergency procedures have been invoked.)

3.4.2 Access Controls at Pathway Platforms

Much of the operational Pathway system is automated and does not require human intervention except at the Post Office. The main human users of the central systems are the system management and support users. The Pathway systems are configured to reduce the risks of human users interfering with the automated applications and of these applications interfering with each other.

This section gives the policy for how access controls at all Pathway platforms are configured. It gives the standard policy which applies to all domains and identifies where variants are permitted. In these cases, the variant is defined for the domain in which it is allowed in sections 4 to 8 below. No other variants are permitted.

POL00401199

3.4.2.1 Workstations from which operational systems can be updated should have floppy drives disabled. Servers should have floppy drives disabled at boot time. Booting from CDROM should also be disabled once a system has been configured. In all cases, exceptions to this rule must be agreed with Pathway Security Management and Horizon and be documented.

3.4.2.2 Workstations at the Post Office display sensitive business data (e.g. about payments) as part of normal operation. All other workstations which can display sensitive information should be in physically secure areas.

3.4.2.3 All systems should have the required roles, groups and other privileges set up on installation. It should rarely be necessary to update these. "Guest" users must not be enabled in the installed systems, and where possible, should not be included. Other generic users should not be accessible for user logon except in exceptional circumstances explicitly defined in the appropriate section below.

3.4.2.4 After a workstation is booted up, a log-in screen should be displayed which cannot be by-passed.

3.4.2.5 People accessing Pathway systems are required to identify themselves using hand held tokens if:

- They are at sites remote from the Data Centre and can update operational or MIS systems (for example, to perform systems management actions)
- They can access BA and/or POCL business data (except at Post Offices).
- They are authorised to update system data which can affect the running of the Pathway systems. This includes people who have UNIX root privilege, NT users belonging to the administrators group and database administrators.

3.4.2.6 Where such tokens are used for authentication, the associated PIN must be at least 6 characters long.

3.4.2.7 If a user who authenticates with a token to one system/domain needs to perform an additional authentication to another system, the second authentication should also be a token based one, using the same token. Agreed exceptions to this must be documented.

3.4.2.8 Each user will have an individually allocated token except in emergencies, for example, when a token is lost. In such cases, specific authentication will be agreed.

POL00401199

3.4.2.9 Where passwords are used for authentication, the user is forced to change the initial password before any other access to the system is permitted.

3.4.2.10 Passwords will expire in 30 days unless otherwise stated (in the section on the appropriate domain).

3.4.2.11 Re-use of the same password is not permitted for either a specified time or until at least 3 other passwords have been used.

3.4.2.12 The minimum password length is 6 characters.

3.4.2.13 After 3 consecutive unsuccessful attempts to log-on, the user is locked out unless otherwise stated.

3.4.2.14 People are identified to the Pathway system as individuals. Users with direct access to the system are registered as follows.

- If accessing the system via a package such as Oracle or Tivoli, they are registered with that package.
- Users who require direct access to the operating system are registered with that operating system
- Users requiring token authentication are also registered with the appropriate authentication service.

(The only exceptions allowed to this are the specific cases identified in later sections of this document. In these limited exceptional cases, the user, for example, an engineer, is identified as an individual using manual means prior to using the system in a way specially set up for this, and where the use of the system is suitably monitored.)

3.4.2.15 Users are authenticated with their individual usernames on first accessing the system. A change to use another username, will only be permitted to certain authorised management roles in exceptional circumstances as specified in the appropriate later section (for example, for Sequent systems in 4.2.2). Any change to use another username is controlled (as specified in that section) and audited in a way which will always be recorded.

3.4.2.16 The filestore is structured to prevent interference between users and between applications.

3.4.2.17 Access to shared resources such as filestore is controlled by:

- Access to that filestore being restricted to a specific product which is available only to authorised users. (Most access is controlled this way as most use of the system is automated), or

POL00401199

- Access to those resources being restricted to users in specified roles. (Group ids may be used to represent roles. Access control lists using these will ensure that only authorised people can access the resource).

3.4.2.18 Access to Tivoli and Oracle resources will use role based access controls.

3.4.2.19 Security audit logs are protected from everyone except those permitted to take specified Security Event Auditor roles. Unless otherwise specified for a particular domain (such as the Post offices) , the security auditing role is separate from other roles at that domain.

3.4.2.20 Passwords are stored in encrypted form separately from application data and executable code, except for the specific cases listed in 3.4.3.1.

3.4.2.21 Interference between applications is prevented. For example, at any system, different applications run in their own user names or that of the user calling them (or at the Post Office, in the Riposte username impersonating the user).

3.4.2.22 Packages (such as Oracle and Tivoli) and applications above the operating system must also conform to the Access Control Policy. For example, Oracle should restrict Payment Card Helpline users to the authorised tables and views.

3.4.2.23 Audit records are generated at the server for client-server applications (such as Oracle Forms applications using PAS/CMS) so audit logs do not rely on input from workstations.

3.4.2.24 Where a product is delivered with pre-defined usernames for human users, these should be deleted (or if this is not possible, disabled) once the initial individual usernames for administering the system have been set-up. Usernames should be disabled by changing to a password which is extremely difficult to guess, then storing this password in a safe.

3.4.3 Non Human Users

As much of the operational Pathway system is automated, some users are system, not human users, so there are usernames and passwords for both types of users. In general, system users should be subject to the controls specified above (e.g. for password protection), as such usernames generally cannot be confined to human users only, so human users can potentially access usernames intended for system users. However, some differences are permitted.

POL00401199

3.4.3.1 The username and password used to automate the log-in may be held in clear if it is only accessible to authorised operational management staff for that system and the potential damage from mis-use of that username is minimised.

3.4.3.2 The password may expire less frequently than the 30 days for human users where suitably obscure passwords are used, and the risk of external access to such accounts is very low.

3.4.4 Engineering Access

Where possible, engineering access to the machines, for example, for hardware diagnosis and repair, is subject to the controls specified above. However, in some limited circumstances, for example, when the operating system cannot be booted, special access is needed, by-passing the normal controls. In such cases, any visiting engineer must be subject to the "authentication of visitors" procedures (see 3.5.3) and two people must be present during such access.

3.4.5 Workstation Related Access Controls

The Access Control Policy covers the security of the workstations used by humans to access the Pathway services where this affects the security of the system. The security required depends on the type of access the user has to the system and the security of the route to the system accessed. The following policies are in addition to those in 3.4.2 above.

3.4.5.1 Users with interactive access to Pathway systems should use controlled, NT workstations where the workstation set-up, including services available at that workstation, is controlled by Pathway.

3.4.5.2 Use of other workstations are only permitted when access is constrained to a single system (via network controls), this system does not store sensitive BA or POCL business data and access is limited to agreed types. All such exceptions to the "controlled NT" workstation policy must be authorised and documented in the ACP.

3.4.5.3 Workstations which have access to sensitive data should be on separate networks linked only into the Pathway secure network. Any exceptions to this must be documented in this Access Control Policy. Documentation on exceptions must explain how the sensitive data is protected from other networks accessible from the workstation, including use of routers and firewalls and how these are configured to prevent undesirable traffic.

POL00401199

3.4.5.4 Where workstations and servers require access to both the Pathway Data Centres and other systems, an authorised combination of routers and firewalls should be configured to restrict the traffic to that permitted. All such cases must be documented in this Access Control Policy and are confined to the Pathway Corporate Services sites.

3.4.6 Controlling Traffic between Systems

Pathway controls should restrict who can access what services so there is no unnecessary access to services. This covers all traffic in and out of, as well as within, the Pathway campus. Controls are enforced using a combination of access lists at routers, platform controls on use of ports and other application gateway/firewall controls where needed.

General policies in addition to the workstation related ones in 3.4.5 are given below. More specific policies are in 8.10.

3.4.6.1 All accesses in and out of the Pathway Data Centres should be restricted to the required traffic from/to authorised sources using routers and firewalls. Such traffic should be routed only to the ports at systems which require that traffic.

3.4.6.2 Traffic originating within the Pathway Data Centres is generally initiated by controlled applications. These applications (and the way they are configured in the system) should restrict traffic between systems to that needed.

3.4.6.3 Where there are specific systems subject to higher risks or vulnerabilities in the Data Centre network, additional network controls should be used. All such special cases should be documented in the ACP.

3.4.6.4 Accesses to/from the Pathway Data Centres such as CAPS, TIP and SMC will have well defined, controlled links with cryptographic protection where needed as specified in the [SFS].

3.4.6.5 External support users of Pathway systems should be permitted access to the Pathway Data Centres only from approved remote sites, only when authorised to carry out a specific support activity and only via controlled routes as specified in this Access Control Policy.

3.4.6.6 No other accesses in and out of Pathway should be permitted.

POL00401199

3.5 Other Access Controls

In some cases, the information system cannot provide all the access controls required. For example, telephone contacts cannot use normal IT authentication procedures. In these cases, some other form of authentication is required.

3.5.1 Customer Authentication

Customers authenticate themselves at Post offices using PUN, card and responses to questions - see [SADD] and section 5.

Customers may also need to provide some proof of identity to the Payment Card Helpline, depending on the type of call - see 5.3.5.

3.5.2 Other Telephone Authentication to Help Desks

Apart from customers, Help Desks may receive calls from at least Post Offices, POCL offices, DSS offices and Pathway sites. Many of these calls come from offices and sites known to the Help Desks. In many cases, the request will not be actioned unless the source of the call has been authenticated.

Both the Payment Card Helpline and the Horizon System Help Desk will maintain information on the Post Office and other relevant sites and offices. The caller is asked for information to authenticate the location, and if required, the individual which the Help Desk can verify. The information known about such offices and sites includes the office code, possibly the telephone number, the address and for some sites, the name of the contact.

For certain cases, different (normally extended) authentication is required supported by further information. The methods used for authentication in these cases are included in the definition of the appropriate domain.

3.5.3 Authentication of Visitors

Some visitors to both Pathway and Post Office sites need access to the IT system. Such visitors will have a company identity card which includes their photograph, signature and pass number. Unless otherwise stated, for all such visits, the pass number of the visitor must be notified in advance to the relevant manager; access will not be permitted if this has not been done. However, Auditors will visit Post Offices and other sites without prior notice to the Post Office Manager.

POL00401199

Pathway visitors to Post Offices are subject to Pathway vetting procedures and approval by Horizon. Visitors to Pathway sites are subject to Pathway vetting procedures.

At the Post Office, visitors such as engineers and auditors are not known individually to the system. However, they are known to the Horizon System Help Desk, and authentication includes use of a one-time password which requires calling the Help Desk. In these cases, the telephone authentication procedure described in 3.6.2 is used to identify the site, and is supplemented by verification of the particular visitor, generally including their pass number.

3.6 Key Management

Cryptography is used widely in Pathway as described in the Security Functional Specification [SFS]. For example, it is used for:

- Protecting information on links for confidentiality, integrity and origin authentication in line with the requirements for that link.
- Digitally signing information such as benefit authorisations, automated payments and software in transit across systems.
- Filestore encryption at the Post Office.

This Access Control Policy defines how the required cryptographic keys are protected when in the information systems. As different keys are protected in different ways, general policies are given here, with specific controls defined with the other controls at the appropriate system where needed.

3.6.1.1 CESG approved keys must be protected in line with CESG requirements.

3.6.1.2 Key material (symmetric keys, DSA private keys and DSA entropy) should be held in clear only when in physically secure environments.

3.6.1.3 Public keys (except for the CA's public key) should be held in certificates signed by the Certification Authority.

3.6.1.4 Symmetric keys should only be stored where necessary, and be held securely.

3.6.1.5 Keys (or part keys) held in filestore must be in separate filestore accessible only to authorised key custodians via authorised applications.

3.6.1.6 Keys used for protecting data should not be resident in filestore in clear.

POL00401199

3.6.1.7 Keys should be changed periodically according to CESG policy. Different periods may apply to Symmetric Keys used for encrypting data, Key Encryption Keys (KEKs) used to encrypt other keys and Certification Authority keys.

3.6.1.8 New KEKs should not be distributed solely under the protection of existing KEKs.

3.6.1.9 Key material in transit electronically must be encrypted (except for CHAP keys between the routers within the Pathway Data Centre LAN).

3.6.1.10 Cryptographic keys and Key Encryption Keys are either installed locally at the machine where they are to be used, or are distributed electronically using an approved protocol which protects these keys in transit.

3.6.1.11 Where a key is delivered in two parts (e.g. a red key and a black key), the parts should be delivered by different routes.

3.6.1.12 The key (or part key) to be handled manually must be held in a locked safe when not in use. Access to this must be authorised and recorded in conformance with Pathway procedures.

3.7 Effect on other Pathway Standards and Procedures

This Access Control Policy defines the policy for controlling access to resources in the operational Pathway system. As explained in section 1.2, there are other documents covering detailed configuration of Pathway systems, physical security standards and procedures used when operating the system. The effect of the Access Control Policy on these other documents is:

3.7.1.1 The detailed configurations documents covering the different Pathway systems define how this Access Control Policy is achieved. For example, they should say how the roles defined here are set up to restrict access as required.

3.7.1.2 The roles defined in this document should be used in other security standards and procedures, not just information system controls. For example,

- procedures for controlling access to secure areas must take into account the roles of people and the organisations to which they belong
- where a role requires access to sensitive data, this should be reflected in the level of vetting required for staff in that role.

POL00401199

- users in these roles must be controlled through a formal registration process. Each user must be authorised to take that role by the appropriate authority before being added to the IT system. Records of all persons registered to use the system must be kept, though the way this is done may be role or service dependent.

3.7.1.3 This Access Control Policy depends on Pathway procedures in some places. The key ones are:

- Pathway (and associated) staff visiting other sites must have a identity pass with photograph and signature. This must be from a relevant organisation which gives such passes to suitably vetted staff only.
- Post Office procedures which must include how to add users to Riposte, how to physically protect tokens and passwords, procedures for telephone authentication to Help Desks etc
- Girobank procedures associated with the Payment Card Helpline. These include procedures for telephone authentication and action to be taken on different types of calls. It also includes Girobank procedures need to cover user and system administration in line with this policy.
- Operational management and application support procedures (particularly CFM and SSC). These must detail, for example, how remote access is properly authorised and the lines configured to allow this when needed (see sections 4 and 8).
- System management procedures to authorise, for example, distribution of software.
- Technical Help Desk procedures to ensure all relevant calls are logged with the help desk systems system and properly monitored.
- General procedures for all users of the system. This will include, for example, procedures on password use and incident reporting. For users authenticating using security tokens it will also cover precautions for protecting the tokens and associated PINs.
- Internal Pathway procedures, for example, for authorising software for inclusion in the live system.

The Pathway Security Manager will satisfy himself that the procedures at the various sites are in compliance with the Pathway security policies and specifications.

4.

POL00401199

CENTRAL SERVICES DOMAIN

4.1 Introduction

The Central Services Domain is illustrated in figure 4-1.

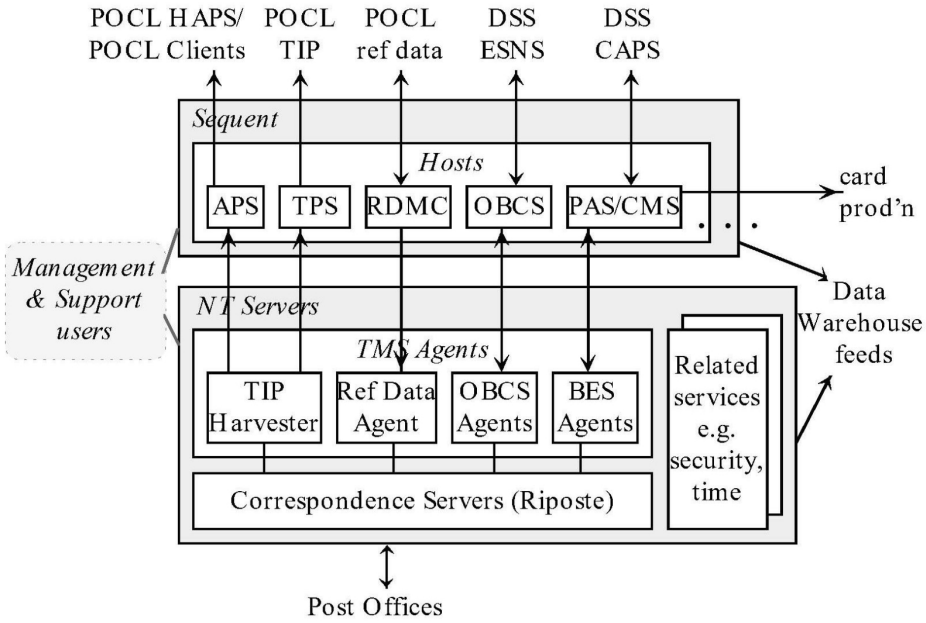


Figure 4-1 Interactions in the Central Services Domain

The hosts at the Central Services Domain are on Sequent machines running Oracle applications. (New hosts, and host ancillary systems may be added.)

The TMS agents interface between the application hosts and the Transaction Management Service (TMS), extracting data from the host and formatting it for transmission to the Post Offices as Riposte messages and vice versa. The agents use SQL*Net to access specific Oracle tables set up for such transfer at the hosts, either to retrieve information to send to the Post office or to update tables as the result of messages received from the Post office. TIP Harvester Agents extract all transactions from the correspondence servers (via the Riposte API) for forward transmission to TIP and elsewhere.

Riposte at the Correspondence servers and Post Offices provide the Transaction Management Service which records all transactions at the Post Office Counters and archives them.

POL00401199

The main operational flows though the hosts, TMS Agents and TMS are automated (as is most System Management).

4.2 Sequent Systems with Oracle Databases

All the host systems in this domain run on the Dynix operating system on Sequent and use Oracle databases, though the Access Services, which feed information to and from the applications, in some cases hold data in flat files. Interactions with Sequent systems are illustrated in figure 4-2.

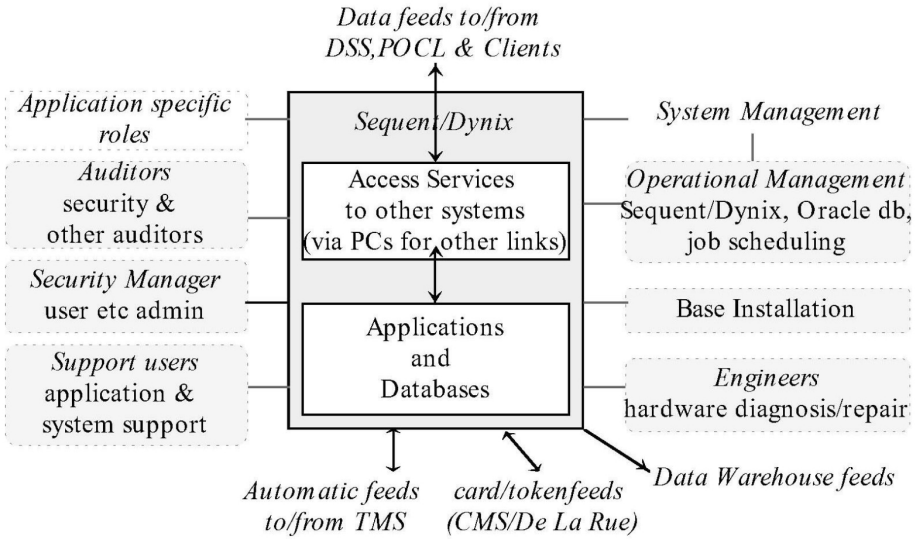


Figure 4-2 Interactions with Sequent systems

Processing on the Sequent systems is normally initiated automatically as the result of files being received or at a particular time. So the main processing is controlled purely as the result of the way the system is set up, not by controlling human access to the system. Similarly, where practical, system management is done automatically (see section 8). As the results of monitoring the system, the need to take some remedial action may be recognised. Only where this action cannot be taken automatically is human intervention required.

Direct users of the Sequent system are defined in 4.2.1. The main users are:

- Security managers who manage security information about users and their privileges, groups etc.
- Operational Managers/System Administrators managing the Dynix operating system and Oracle databases. The normal role here is

POL00401199

monitoring the system. More active use of the system occurs as the result of incidents.

- Application support people diagnosing software faults and engineers diagnosing and clearing hardware faults
- Security and other Auditors
- Application specific roles as detailed in 4.3 below.

4.2.1 Roles

People in the following roles have direct access to the Sequent machines.

Role	Main classes of functions
Computer Operator	Physical operations e.g. media handling, and the ability to run pre-defined jobs, such as back-ups.
System Monitoring	Monitoring the operational system using Patrol.
Database monitor	Monitoring Oracle databases
Operational management/ System Administrator	Management of Dynix including any action needed concerned with replication between campuses and local archiving. Operational monitoring/management using Patrol workstations. Job scheduling (Sequent & NT) using Maestro workstation. Code updates when required quickly (prior to update via configuration management) and authorised
Operational manag't/ Database administrator	Oracle database administrator for database structure - setting up views, space allocation etc.
Secure menu administrator	Configuration of the secure menu system, including addition of new functions
Security Management	Administering UNIX user information, including group membership for all users of the Sequent system. Administering Oracle database administrator (DBA) users and associated roles and privileges. Administering users rights in the Secure menu system Security monitoring
Dynix 3rd line support	Operational management of Dynix by Sequent staff when CFM cannot cure problem.
Database 3rd line support	Operational management of Oracle when CFM cannot cure problem. This may sometimes require updating the database.
Application support user	Supporting applications on Sequent - both Oracle applications and Access services.
Application support manager	Supporting applications as above, plus correcting data when required and authorised.
Application support - VME applications	Using Sonnet on Sequent to access the Pathway partition on DSS VME systems for application support
Application 3rd line support	Supporting Oracle applications
Engineer	Hardware diagnostics and repair
Base Installation and	Initial installation and configuration the base system -

POL00401199

Role	Main classes of functions
configuration	Sequent and Oracle databases. Later updates to these.
(Business Function and Security Event) Auditor	Access to audit trails, when these are not available elsewhere

The Sequent operational system uses symmetrix discs. These are linked across Data Centres via the Energis network. The roles and associated access controls for supporting the symmetrix disc controller and the network box which connects these discs to the Energis network are covered in 8.8 below.

4.2.2 System Access Controls for Human Roles

As for all domains, system access controls conform to the policies in section 3.

Users access the system at the operating system and/or Oracle level - many of the roles above require both levels of use.

Note that users of specific host applications only (see 4.3) should be Oracle users, not operating system users.

4.2.2.1 System Level Access Controls

System level access controls at the Sequent system are enforced using Dynix facilities with some additions. All users requiring UNIX level access to the system will access it using a Secure Menu System. This constrains the functions called depending on the user's role and audits all functions performed by that user. Most management activities should be done using specific functions on the menu. Where the function requires a change of username, that will be done automatically by the menu system and audited. Changes to username will also cause a Patrol event. For emergency use, the menu will include an item which provides root access and use of UNIX commands.

Engineering access when the operating system cannot be fully booted, is via "single user mode" under controlled conditions (see 3.4.4). Single user mode should only be used when more controlled methods are not possible.

4.2.2.2 Oracle Application Access Controls

Oracle users can access Oracle applications and databases in several ways:

POL00401199

- Oracle applications or other tools on the user's workstation, accessing the database via SQL*Net.
- SQL*Plus and other facilities on the Sequent system, called via the secure menu system above. (SQL*Plus should **not** be used in client-server mode.)
- System management tools using system management protocols

Database administration functions should use:

- Patrol for monitoring the database
- Pre-defined Discover queries to examine the state of the database. (Discoverer should be configured to restrict access to the tables and views needed for the task and audit actions.)
- Pre-defined, authorised SQL*Plus for database updates (which should include auditing)

Application support should use:

- Discover queries to examine the data
- Pre-defined forms for correcting standard types of data problem
- Pre-authorised SQL*Plus scripts for correcting other data problems

Pre-defined forms and pre-authorised scripts should audit the correction made.

Note that application support users also need system level access, for example, for access to code.

Human users of an Oracle database or application, are registered with the particular Oracle database server as users of specific Oracle roles. The following Oracle roles should be defined for all Oracle applications. (This section includes only those roles which are supported for all Oracle databases - specific roles for specific applications are defined in 5 for PAS/CMS and 4.3 for other applications). Note that in some cases, people with different human roles may have the same access to the same Oracle role.

Oracle role	Functions, and roles
MONITOR	Read only access to application data in this database - used by Auditors, FRM, application support etc
AUDITOR	As MONITOR plus access to audit information - used by auditors
CFM_DBA	Full dba privileges
SSC	As for MONITOR, plus limited updates, implemented by pre-defined, authorised forms

POL00401199

Note that there are also roles for non-human users such as system management tools and TMS agents.

4.2.2.3 Table of Access Controls by Role

The following table specifies for each role how users access the system (workstation type and location), how they are authenticated and where defined and what resources are available to people with this role. Note that some of the operational and system management users have access to a number of systems and are described more fully in section 8. Information in this section is limited to their use of the Sequent system.

Role	Workstation type and Location	Authentication method & where user defined	Resources available
Computer Operator	console	UNIX/secure menu with token	Predefined jobs in secure menu system only
System Monitoring	X terminal (or emulator) at Data Centre and CFM site	token authentication	Resources as available via Patrol
Database monitor	NT workstation at secure CFM site	UNIX/secure menu with token	Read only use of SQL*Plus, svrmgr
Operational Management/ System administrator	NT Workstation (X terminals or emulators for Patrol & Maestro) CFM secure site	UNIX/secure menu plus token authentication (see note 3).	Functions as on menu. This can allow use of root and UNIX commands and Oracle dba functions.
Database administrator	NT workstation at secure CFM site	UNIX/secure menu using token authentication; Oracle user registered with associated role for dba functions	Functions as on menu - this can allow Oracle dba functions for specified applications (CFM_DBA role)
Secure menu administrator	NT workstation at secure CFM site	UNIX/secure menu using token authentication;	Defined functions for menu admin
Security Management	NT workstation on secure LAN CFM site	UNIX/secure menu and token (see note 3). Oracle user registered as above	User information in UNIX, secure menu system and Oracle
Dynix 3rd line support	NT workstation. Secure site (see notes 6 and 7)	UNIX/secure menu plus token (see notes 5 and 6)	UNIX, which can include root access
Oracle db 3rd line support	NT workstation. Secure site (see note 6)	UNIX/secure menu plus token (see notes 5 and 6)	Read only access; Oracle dba, & limited UNIX functions.
Application Support user	NT workstation at secure Pathway site	UNIX/secure menu plus token; Registered Oracle	Read only access to event logs and other

POL00401199

Role	Workstation type and Location	Authentication method & where user defined	Resources available
		user	relevant files and databases; Oracle MONITOR role
Application support manager	NT workstation at secure Pathway site	UNIX/secure menu plus token; Registered Oracle user	As above, plus controlled write access to application data - Oracle SSC role (see note 9)
VME application support	NT workstation at secure site	UNIX/secure menu at Sequent (also VME user)	Sonnet, for VME access
Application 3rd line support	NT workstation at secure site (note 6)	UNIX/secure menu/Oracle application plus token	Read only access to application; Oracle MONITOR role
Engineer	computer console. Data Centre	UNIX with engineer password (see notes 5 & 7)	Access to diagnostics and, if needed, data on suspect hardware
Base Installation	computer console Data Centre	UNIX	most
Auditor	NT w/s on secure LAN; Pathway site (Feltham)	UNIX/secure menu/Oracle and token authentication	Audit logs - platform, secure menu, database, application; includes Oracle AUDITOR role

Notes:

1. Wherever possible, responses to events are automated, to prevent the need for human interaction.
2. Wherever possible, responses to events which require human interactions are performed using pre-defined functions, rather than command line access to the system.
3. Operational management staff always authenticate under their own names to UNIX and perform functions wherever possible without superuser/root privileges (see 3.4.2.15). If root is needed, the appropriate menu item on the secure menu system will be used to switch users. This will be audited and an alert sent to Patrol so a record remains available even if the audit log at the UNIX machine is subsequently corrupted.
4. Emergency operational management is currently expected to be from the CFM secure site at Belfast.
5. All visiting staff are subject to manual procedures on entering the secure Pathway site to authenticate who they are and authorise their access to the computer room - see 3.5.3.

POL00401199

6. Where Sequent and Oracle staff provide 3rd line support, this may be from Sequent and Oracle sites. In this case, access is from a secure area using a secure NT workstation on a secure LAN via encrypted links to the Data Centre - see 8.2.1 and 8.10. Call in procedures are as in 8.2.2.
7. As Sequent require root access, an independent monitoring system will be used where all key strokes on the Sequent workstation are captured and echoed on a CFM workstation.
8. Visiting engineers are subject to manual procedures as in note 5 above.
9. Application support managers can correct application data subject to authorisation procedures - see 8.7. For Oracle applications, this should, where-ever possible, be via functions available to Oracle SSC role. In exceptional circumstances, use of SQL*Plus scripts will be authorised after checking. For Access and other services, this may involve updates to flat files. In all cases, corrections to the data are audited.

4.2.3 Dynix and Oracle Access Controls

The Dynix operating system should be set-up according to the access control policy in 3 above. For example, Security Audit Logs (both Dynix and Oracle ones) should only be accessible to Security Event Auditors, for Oracle, where there is more than one database on the same machine (e.g. OBCS, APS, PAS/CMS), these will run under separate user names.

All loading/unloading of data to/from Oracle databases should be done by automated processes. Separate interface tables should be used to restrict the damage possible due to failures during automated processes.

The set-up of the system should be regularly monitored, for example, to check for dormant accounts and to review any changes made to important system files.

4.2.4 Control of Connections to the System

Links to the Sequent systems are controlled by routers and by configuration of applications and the use of Sequent ports. These restrict access to the Sequent system from other services at the Pathway Data Centres and elsewhere. These should permit the traffic required to support the roles above and the Pathway application traffic, for example:

- Telnet, X-terminal and token authentication traffic for operational management, 3rd line support, job scheduling and Security Event Auditors

POL00401199

- OSI traffic to VME (FTF and MAC) to support file transfer to DSS systems and management
- SQL*Net access to Oracle databases from Girobank Help Desks and agents extracting data from the databases for transfer to the Post offices, to the Data Warehouse, to archives and exceptionally for Fraud Risk Management
- File transfer of business data to PCs en route to/from POCL and De La Rue

4.3 Access Controls for Specific Host Applications

All host application are Sequent/Oracle ones, and are therefore subject to the controls defined in 4.2 above. Each has some differences in the automated feeds into/out of the application. For example, PAS/CMS has feeds about payment authorisations with CAPS and about cards with the De La Rue services. OBCS communicates with the DSS ESNS e.g. to find what Order books have been stopped. The RDMC service accepts feeds of reference data from POCL (and potentially elsewhere). The TPS feeds Post Office transaction information to the POCL TIP system. Access controls for all applications conform to the general policies in 3.

All these applications support the standard Oracle roles (CFM_DBA, AUDITOR, SSC and MONITOR) for database administration, auditors, application support managers and people with only read access to the database (application support users, system monitoring) - see 4.2 above.

In addition, there is a BSU role (for Business Support) for some applications, including PAS/CMS - see below.

The MONITOR role is also used by the other human roles for read only access - both Pathway and Girobank Fraud Risk Managers have this role in PAS/CMS, APS, OBCS and TPS.

In addition, PAS/CMS and RDMC have further application specific roles.

4.3.1 PAS and CMS

Information comes from the CAPS system, is processed by PAS/CMS and sent either to the TMS for forwarding to the Post Offices or to the Card or Temporary Token Producer to generate cards and PUNs. Information is returned from both these sources, processed and returned to the CAPS system. The main processing is done automatically without human intervention. Track and Trace information is also received from the Royal Mail.

POL00401199

Specific PAS/CMS roles are:

- Payment Card Helpline Advisors using Oracle Forms applications to access PAS/CMS and Helpline Security Managers maintaining user information about them at the PAS/CMS database. See also 7.4 for Helpline roles.
- DSS/BA benefit staff doing on-line transactions via CAPS e.g. emergency payments and DSS Help Desk staff enquiring on PAS/CMS data, also via the CAPS on-line interface.
- Business Support users accessing PAS/CMS when required for financial reconciliation (see 7.5)
- Fraud Risk Management staff accessing PAS/CMS data when required information is not available via the Data Warehouse or archives.
- The Cryptographic Key Custodian installing/updating the encryption key needed for the CAPS to PAS/CMS link.

Note that the operational management role includes generating contingency payment authorisations when CAPS is down according to agreed procedures.

The following table shows the system access controls associated with the PAS/CMS roles (apart from the Cryptographic Key roles which are as defined in 7.7.1). All users in the table access PAS/CMS information via Oracle tools.

Role	Workstation type and location	How authenticated to PAS/CMS (& where user defined)	Resources available
Helpline Advisor	NT Help Desk workstation in Girobank area at campus	Oracle username, password (Oracle user associated with Oracle role)	Particular PAS & CMS tables as required for the authorised Oracle Forms (with sufficient write access to allow cards to be stopped, update call logging tables and change password.)
Helpline Advisor (NSI)	as above	as above	As above, plus can handle data with a Nationally Sensitive Indicator.
Helpline Supervisor	as above	as above	As a Help Desk Advisor, plus the ability to handle NSI data and other more restricted dialogues.
Helpline Security Manager	as above	Oracle username, password (Oracle user associated with Oracle role)	Oracle user and role tables via authorised Oracle Forms; access as Helpline Advisors plus privilege to create users and assign/re-assign them to Helpline roles.
DSS/BA staff	DSS/BA terminal and site	Authenticated to DSS system, identified to P'way by transaction id.	Particular PAS tables as required for the authorised transactions from the Oracle client applications on VME. (The Oracle POLI system

POL00401199

Role	Workstation type and location	How authenticated to PAS/CMS (& where user defined)	Resources available
			username.)
Business Support	NT at secure Pathway site	NT user with token and Oracle user (BSU role)	Read only access via pre-defined forms to PAS/CMS for reconciliation
Fraud Risk Manager	NT secure sites G'bank, P'way	NT user with token and Oracle, UNIX? user	Read only access main database in exceptional circumstances

There is a separate username for the Cryptographic Key Custodian. Filestore accessible only to that user holds the cryptographic key.

4.3.2 Reference Data Management Centre

Reference data can be associated with particular applications (e.g. the price of stamps in EPOSS) or be more generic (e.g. Post office details). It may come from POCL, POCL Clients and Pathway. Data fed into the RDMC is classified according to whether it should be used to update the RDMC and Post Office counters automatically (class 1) or whether some human intervention is needed. For the main feed from POCL, new reference data and its class is agreed in advance of the data being fed to the RDMC.

All reference data fed to RDMC is validated. If validation fails, the data is returned automatically to POCL without human intervention. Reference data for counter applications is distributed via the associated RDDS and the TMS system to the Post Offices. Reference data is also fed to the Data Warehouse.

For reference data of class 2 and above, the data is held at the RDDS until the dependencies for its use have been satisfied. For example, the software needed to process it must be available and shown to work with it. Some reference data comes from the Pathway project and supplied to RDMC via Configuration Management as for other software updates - see 8.6.2.

Application roles supported at the RDMC are:

Role	Main Functions
Reference Data Change Manager	Kick off the transfer of validated reference data of classes 2 to 5 to TMS when all required dependencies have been met. (Oracle role: user_change_control)
RDMC Loader	Manually initiated load of reference data files to RDMC (Oracle role: user_loader)
RDMC user	Query and report on reference data, so read only

POL00401199

Role	Main Functions
	access (Oracle role: user_reports)
RDMC access administrator	Sets up users and assigns them their roles (Oracle role: user_administrator)

All these users access the RDMC from a controlled NT workstation on a secure LAN from a secure Pathway site via encrypted links. Authentication to NT uses a token allocated to the individual, they also authenticate to the Oracle application. Oracles roles control this access. There are no human roles at the RDDS.

Note that the security management role in 4.2 includes user management of the core users of the system, including the RDMC users. Application support in 4.2 includes support of the RDMC.

4.4 Windows NT Systems

There are several different types of NT systems in this domain. For example, the TMS Agents are generally on separate NT servers from those used for the Correspondence Servers and there are also NT servers supporting security services, the time service, the PCs providing the interfaces to transfer files to De La Rue, POCL etc.

All of these NT servers have common management and support users and may have specific operational users as illustrated in figure 4-3.

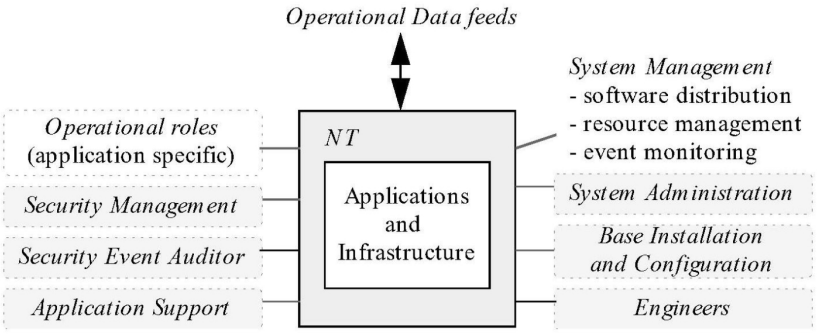


Figure 4-3 Users of NT systems

As for the Sequent systems, most of the use of the NT systems is automated so human intervention is an exception - mainly for system management and support. Different NT servers support different applications, so there are some differences in the access controls required at different servers. However, management of all NT servers in this domain is done in the same way.

POL00401199

- The NT servers are managed using Tivoli and NT administration. Events and resources are monitored via Tivoli (see section 8) and appropriate remedial action is generally taken automatically. Security management (e.g. administering users) is done using NT utilities.
- Software and configuration information is distributed to these systems via Tivoli (see section 8).
- NT servers also have local consoles for use by engineers when diagnosing and repairing faults and for any other management action required locally.

The common roles for all NT servers are described in [REF _Ref401984526 \n * MERGEFORMAT]. Specific roles for particular NT servers are included in section 4.5.

4.4.1 Roles

People in the following roles have access to all NT systems in this domain.

Role	Main functions
Computer Operator	Physical operations e.g. media handling, but no on-line use of the system. This includes the Legato tapes used for archiving
Operational management	Any residual management of NT (not done by SMC e.g. via Tivoli).
Security Manager	Administering NT user information, including group membership.
Security Event Auditor	Use of audit logs in monitoring security and tracing incidents
Application support user	Supporting applications on NT platforms.
Application support manager	As above, but also able to correct some data
Engineer	Hardware diagnostics and repair
Base Installation and configuration	Initial installation and configuration the base system - NT etc Later updates to this.

Note that relational databases are not supported at most NT systems, so NT database administrator roles are defined only at relevant NT systems (e.g. the roll-out/auto-configuration system - see 8.6.)

4.4.2 System Access Controls for Human Roles

Access controls associated with these roles are defined in the followed table.

Role	Workstation type and location	Authentication method & where user defined	Resources Available
Computer	no w/s; on site at	none, as no access	Media only

POL00401199

Role	Workstation type and location	Authentication method & where user defined	Resources Available
Operator	Data Centre		
Operational Management	NT w/s at secure Pathway site	NT with token (defined at appropriate domain)	Administrator rights
Security Manager	NT workstation at secure Pathway site	NT with token (defined at appropriate domain)	User administration, security policy administration etc
Security Event Auditor	NT workstation at secure P'way site	NT with token (defined at appropriate domain)	Read only access to audit logs only
Application Support user	NT workstation at secure P'way site	NT with token (defined at appropriate domain)	Read only access to event logs, registry and relevant files.
Application Support Manager	NT workstation at secure P'way site	NT with token (defined at appropriate domain)	As above plus some data correction
Engineer	Pathway campus; no remote access	NT with controlled password/token	Administration
Base Installation	Pathway campus	NT with password	Administration

Notes:

1. Engineers have controlled access c.f. Sequent. They are accompanied by CFM staff when using the system
2. There is a specific variant of the administration role for administration of the Primary Domain Controller of an NT domain.
3. Application support managers correcting data are subject to the same controls as on Sequent and elsewhere (see 8.7) - all updates must be pre-authorised, and the update method used must audit the correction.
4. Apart from event logs etc which are relevant to all NT systems, application support users should access application databases via relevant tools, rather than just operating system facilities.

4.4.3 System Set Up

System access controls must conform to the policies in 3.

All NT servers are set up with a group and template user for each of the roles above (plus any other defined for the particular NT system). These templates are used when a user is assigned to a role to set up that user with the required user profile providing access to only those tools needed to carry out the role.

POL00401199

NT systems belong to domains with a primary domain controller and backup domain controllers so users only need to be administered at one place for access to all systems at that domain. Users in most roles can logon once to all NT Pathway domains with trust relationships constraining resources available between domains. However, some roles (Engineer and Key Custodian) will always be defined as requiring the user to be local at the machine. Policies for the structure of NT domains are in 8.11.

4.4.4 Control of Connections

The following traffic is generally permitted to NT systems at the Data Centre:

- Telnet and token authentication traffic for NT management, security auditor access etc
- NT domain traffic
- Maestro job scheduling (at Agents)
- Tivoli traffic for event management, software distribution etc
- File transfer traffic using FTMS
- Client access to applications. Different types of access are used for different applications

However, the NT server supporting the KMA has more restricted access (for example, no Maestro scheduling). Also, many of the NT systems have application specific traffic such as SQL*Net access to access Oracle database tables, Riposte RPC traffic to link to Correspondence Servers.

4.5 Specific NT Servers (except security ones)

NT servers are used to support many of the Data Centre business services used during normal operation. These include:

- The **Correspondence Servers** where Riposte, together with the Riposte infrastructure at the Post Office, form the Transaction Management Service which handles all the operational traffic to and from the Post Offices. (Note that there is other traffic between the Pathway Data Centres and the Post Offices for System Management traffic and Key Distribution.)
- The **Agents** which transfer data between the hosts and the Correspondence servers. There are different agents which handle traffic for different links.

POL00401199

- The **PCs which handle file transfers** between the Pathway Data Centres and POCL, De La Rue, and potentially other POCL clients sites in future. (The PCs at the POCL and De la Rue sites are controlled as described in sections 5 and 8)
- **Related supporting services** such as the Time Service, Archive Service, Host Ancillary services.
- **Security services** such as the Entropy Servers used in signing benefit payments, the Key Management Service used to generate and distribute keys and the Authentication Service used for token authentication.

All these NT servers are subject to the controls described in [REF _Ref401738027 \n * MERGEFORMAT] above. In addition, there are also service specific access controls on some of these systems. This section describes these controls for all these NT servers except the Security Services ones which are described in the next section.

There are also a number of NT systems used for system management, software distribution and Post Office implementation. These are covered in section 8.

4.5.1 Roles

Operational use of these services is automated, so does not normally require any human intervention apart from the management and support roles defined in [REF _Ref401738027 \n * MERGEFORMAT] above. There are the following specific roles at these NT servers.

Role	Main Functions	NT Servers where applicable
Riposte Management	Residual Riposte management which is not automated e.g. setting Riposte neighbours. (Setting up Correspondence servers as members of Riposte groups when new Post Offices are added is done by the auto-configuration application.)	Correspondence servers
Business Support	Access to TMS when needed to support reconciliation	Correspondence servers
Pathway FRM	Access to TMS journals in exceptional circumstances, when needed to support investigations.	Correspondence servers (and their archives)
Auditors	Access to TMS journals when needed to when investigating security incidents	Correspondence servers (and their archives)

POL00401199

Role	Main Functions	NT Servers where applicable
Legato Adminstration	Managing the audit archives	Archive server
Crypto Key Custodian & Key Handler	Installation and update of keys and re-installation when needed e.g. on machine reboot. (These roles are defined in 7.7.1)	BES Agents, PC for De La Rue link

Notes:

1. The BES Agent requires installation of a DSA private key for protecting payment authorisations. (and associated public key certificates etc).
2. The De La Rue link PC requires installation of a Red Pike key.

Access controls for these roles are as defined in the following table.

Role	Workstation type and location	Authentication method	Resources available
Riposte management	NT at secure site (see 8.2)	NT domain user with token	Appropriate Riposte utilities
Business Support	NT at secure Pathway site	NT domain user with token	Controlled read only TMS access
Pathway FRM	NT at Pathway secure area	NT domain user with token	Limited read only TMS access (see note)
Security Event Auditor	NT at Pathway secure area	NT domain user with token	Audit logs and limited read only TMS access
Legato Administration	NT at Pathway secure area	NT domain user with token	Legato archivies via Legato client

Notes:

1. Business Support, FRM and Auditor access to the operational Correspondence servers is allowed in exceptional circumstances for limited amounts of data (as otherwise, the performance of the system could be impaired). In all cases, access is controlled, and limited to use of a specific Riposte Query tool.
2. Access controls associated with cryptographic keys are covered in 7.7.1

POL00401199

4.5.2 Other Access Controls

The network and platform set up should restrict the traffic to that required to operate and manage the system. At all platforms, the required system management traffic is permitted. In addition, the traffic needed to support the operational and MIS process must be permitted. For example:

- At Correspondence servers: data transfers to/from Agents using Riposte RPC and to/from Post Offices using TMS via specific routers
- At Agents in general: SQL*Net links to the appropriate host application on Sequent (PAS/CMS, OBCS, APS, TPS or RDMC) and links via the Riposte API using RPC for distribution to/from TMS. Note that the TIP harvester acts as the Agent for both APS and TPS and also supplies the TMS journal information to the Data Warehouse.
- At BES Agents: links to an Entropy Server on a separate NT server to obtain the entropy needed for signing payment authorisations using DSA and to the KMA for distribution of some key material using key distribution protocols which protect keys in transit

4.6 Security Services

Pathway uses cryptography for integrity and sometimes confidentiality protection of all or selected data on certain links and sometimes filestore. To support this, Pathway has the following security services:

- A **Key Management Application** (KMA) which (generates and) distributes cryptographic keys to Pathway services and the Post Offices. An associated **Certification Authority** (CA) generates public key certificates and **Entropy servers** which generate DSA entropy for digital signatures.
- The **VPN servers** used for protection of the traffic to Post Offices
- An **Authentication Service** to support token authentication.
- The **cryptographic boxes** used for link level encryption of some links.

(This is in addition to the software security services to protect data in transit on particular links. For example, encryption on the CAPS and De la Rue links, digital signatures for payment authorisations send to the Post Office. Also, there are signing servers to sign software and auto-configuration information sent to the Post office - see 8.6.)

POL00401199

4.6.1 Key Management and Associated Services

Interactions with the Key Management Application (KMA) and Certification Authority Workstation (CAW) are illustrated in figure 4-9.

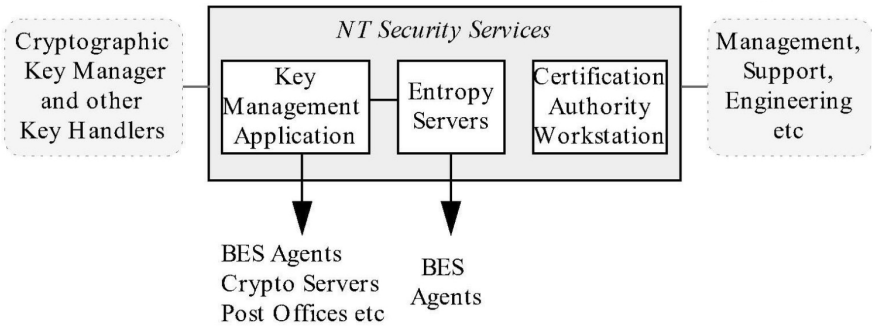


Figure 4-4 Interactions with the Key Management Service

The **Key Management Application (KMA)** is used to (generate and) store cryptographic keys and is also used when distributing initial and updated keys to the Post Offices, routers etc. Keys handled include the CHAP keys for Post Office authentication and Post office filestore encryption key. The KMA also uses the **Entropy Servers** to provides the entropy needed for DSA signatures.

An off-line **Certification Authority - the Certification Authority Workstation (CAW)** is used to generate public key certificates used when verifying digital signatures.

People in the following roles have access to these services (in addition to the NT operational management and support roles defined in 4.4).

Role	Main functions (system accessed)
Cryptographic Key Manager	Generating keys and initiating distribution of these; viewing current situation re keys (KMA) Generating certificates to certify keys (CAW)
KMA Data Manager	Maintain validity of data within KMA database e.g. specify new client where key to be sent (but no key management roles)
Cryptographic Key Custodian and Handlers - see 7.7.1	Installing, updating and re-installing keys.
PO key recoverer (part of SMC Team Leader role)	Initiating recovery of a Post Office key for a Post Office Manager who has lost his card or PIN after authentication of the PO caller to the Help Desk - see 8.3, 8.9.

Notes:

POL00401199

1. Access controls for the Key Custodians and Handlers are defined in 7.7.1
2. Access controls for the PO key recover are defined in 8.3.
3. The Key Manager and KMA Data Manager roles are Oracle users, so log-on to Oracle (after NT workstation, token logon). This gives access to specific functions only
4. There are also Database administrator and security manager roles for the underlying database c.f. Oracle roles for host applications.

4.6.2 Authentication Service for Authentication using Tokens

Authentication using tokens will be supported by an **Authentication Service** at each Data Centre. The Authentication Server at one Data Centre will be the master, generally used for all authentication, with the other acting as a slave to provide resilience.

The Authentication Service holds information about:

- Tokens, and when, and to whom, they are assigned; also the PINs associated with these tokens
- Users of these tokens
- Clients who initiate authentication when users access the system. These may be on NT and UNIX systems and on routers.
- Audit logs of authentication and administrative activities
- Configuration options such as the type and size of PINs permitted, Client retry interval, master/slave information

The main roles at this system are:

- Installation and configuration of the Authentication Service - part of the operational management role of the Solaris system on which the service is installed - see 4.7.
- Administration of tokens and users for all Pathway users who require authentication via tokens - see 7.7.2.
- Auditors - the Authentication Service has real time monitoring tools for this (as well as providing audit trails to the Audit Service).

All these users access the system from controlled NT workstations on a secure LAN in a secure area linked to the Data Centre over an encrypted link. After initial installation of the service, they authenticate using tokens.

POL00401199

4.6.3 Cryptographic Boxes

Zergo boxes are used to provide link level encryption on a number of links. These are government approved point-to-point encryption devices using Rambutan and access controls are as specified by the manufacturer.

4.7 Solaris Systems

Solaris systems are used for a number of services at the Data Centres including:

- A Solaris system supporting the PAS/CMS training database. This is used by the Payment Card Helpline for staff training and supports the same Oracle Forms applications as used for the operational system, but with training (and therefore not sensitive) data.
- The Network Management Station at each Data Centre- see 8.5
- The Solaris system at each Data Centre supporting Security token management (see 4.6 above) and the Firewall Enterprise Centre (see 8.5)

All of these Solaris servers have common management roles as follows:

Role (and organisation)	Main functions
Computer Operator (CFM)	Physical operations
Operational management	c.f. Sequent operational management
Security Management (CFM)	Administering user information
Security Event Auditor (Pathway)	Access to audit logs
Engineer	Hardware diagnostic and repair

Access controls associated with these roles are defined in the following table:

Role	Workstation type and location	Authentication method	Resources available
Computer Operator	no w/s; on site at Data Centre	none, as no access	media only
Operational management	? (is this NT, Belfast)	UNIX with token	UNIX administration
Security management	see above	UNIX with token	user/security administration
Security Event Auditor	NT workstation; Feltham	UNIX with token	read only access to logs, relevant files
Engineer	Pathway campus, no direct access	UNIX with controlled password/token	required UNIX facilities

POL00401199

Note: this section is not yet complete, as roles have still to be discussed and agreed.

5.

POL00401199

OFFICE PLATFORM SERVICE DOMAIN

5.1 Introduction

The Office Platform Service Domain is illustrated in figure 5-1.

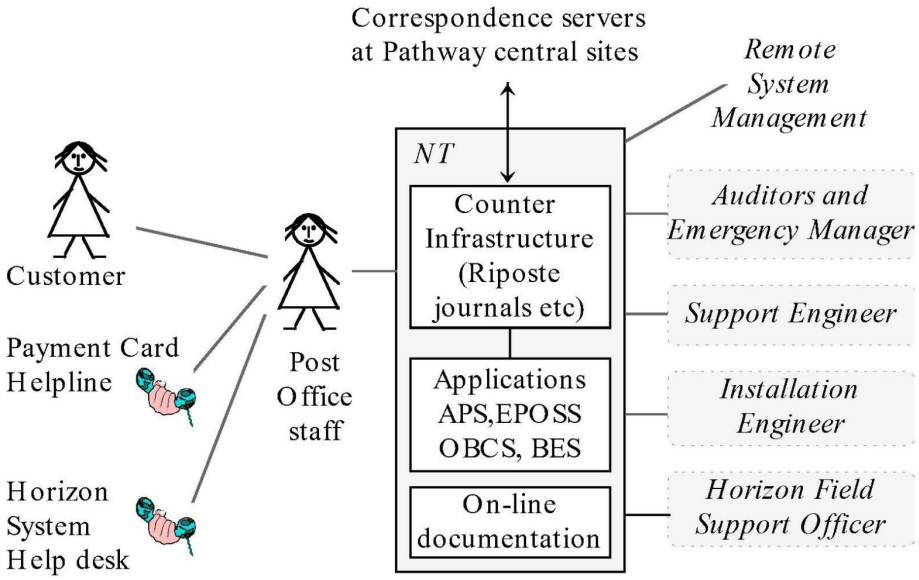


Figure 5 - 1 Interactions in the Office Platform Service Domain

Information about BA payments and cards and also about APS, EPOSS and OBCS is distributed using the Riposte Transaction Management System which includes the Riposte journals at the Post Office.

Customers pick up Benefits cards and use these to prove their identity when receive payments or use the existing style of Order Books and Girocheques to get payments. They may also use other Post Office services such as Automated Payments and purchase many types of items.

Counter clerks handle these transactions using the applications at the counter. In exceptional circumstances, they may ring up the Payment Card Helpline, for example, to confirm whether a payment should be made or the Horizon System Help Desk for advice on other applications. Post Office Managers act as local system manager and report faults via the Horizon System Help Desk.

Engineers install the Pathway service to Post Offices, provide updates and handle faults in the system by replacing components of it. The Horizon System Field Officers (HFSOs) handle migration of existing Post Office data.

POL00401199

Post Office Systems are monitored and managed via System Management Services using Tivoli. These are used to distribute software and scripts to initiate management actions to Post Offices. Software distribution can include updates to the Tivoli Agent and to Riposte and NT as well as applications. Tivoli tasks are also used to extract diagnostic information from the Post Office counter systems for use in application support - see 8.3 and 8.7.

5.2 Roles

All direct users of the NT Workstations at the Post Office are local.

Although there are potentially several separate functions which in a larger organisation would be allocated to separate people, only the following roles are identified for Post Office staff:

- The **Post Office Manager** who is responsible for all the management of the Post Office system including setting up workstations, introducing users, doing accounts.
  "Manager" is a generic term here - meaning the person in charge of the Post Office. The person taking the role may be a sub-postmaster or agent.
  Post Office Managers may allow other staff to deputise for them, and so take this role.
- **Counter clerks** who run the APS, EPOSS, OBCS and BES applications.
- **Supervisors** who can perform all Counter Clerk functions and may also do other functions such as view stocks.

The Post Office Manager acts as the Security Manager at the Post Office (rather than this being a separate role as in other domains); in many Post Offices, there are insufficient people to justify a separation role for this.

Customers are also recognised at the Post Office, though they do not access the system directly, so do not have a role in the system.

POCL Auditors have access to Post Office services. The normal POCL Auditor will have read only access to the system. One of the Auditors may take the role of an Emergency Manager who may take over from the Manager after suspected fraud or when a Post Office is closed down or transferred to a different Manager. POCL Investigators have the same access rights as normal POCL Auditors and are not distinguished from them in the IT system.

POL00401199

Horizon Field Support Officers (HFSOs) handle the migration of Post Office data to Horizon - either manual records on from ECCO equipped Post Offices. Other Pathway staff such as Security Event Auditors do not have access to the Post Office system.

The following table shows the main classes of functions of people in the identified roles. (There is also a Support group used in emergencies - see 5.4)

Role	Main classes of functions
Manager	Key (and memory card) custodian - installing, changing and recovering keys. User management (of local post office staff). Stock unit management (including allocation to clerks) Specific management applications, for example, balancing Post Office accounts. Run diagnostics to check system and peripherals are functioning correctly. All counter clerk functions.
Counter Clerk	System boot-up using the memory card. (At some Post offices, this may be restricted to more senior staff.) Run applications BES, EPOSS, APS, OBCS. Contact the Payment Card Helpline when required. Stock unit balancing etc.
Supervisor	As Counter Clerk plus viewing stock, users.
Clerk using training mode	As Counter clerk functions with special training data (counter clerk also uses special training benefits/APS cards so does not need a customer present)
Installation engineer	Roll-out of new Post Offices including setting up Post Office personality.
HFSO	Migration of data, particularly stock units from existing Post Office systems onto Horizon
Support engineer	Replacing peripherals etc and running diagnostics to check functioning correctly. Adding new workstations, peripherals.
Auditor	Production of reports as done by Post Office manager and viewing and/or printing selected log of events.
Emergency Manager	As normal auditor plus all Post office Manager functions including user administration.

5.3 Control of Connections to the Systems

A multi-counter Post Office has a network of NT workstations, one of which is the gateway with a link to the Pathway Data Centres as illustrated in figure 5-2.

POL00401199

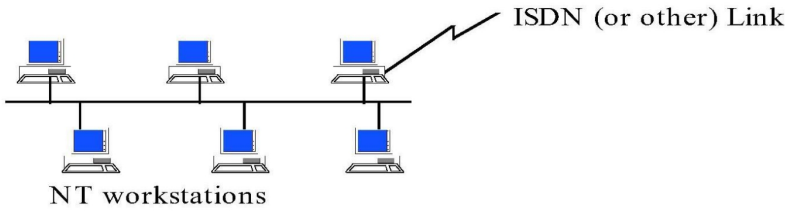


Figure 5-2 Post Office Configuration

In some cases, the ISDN link is replaced by a different form of link, but this does not affect the Access Control Policy.

In a single counter Post Office, the link is to the only workstation, which may be at the Post Office site or may be portable. In a multi-counter Post Office, not all workstations need have all the same peripherals, so some transactions can only be done at certain counters.

The link to the Pathway campus is protected using VPN as defined in [SFS].

The following table shows which services are permitted on this link.

Service	Type of access
Auto-configuration on Post Office roll-out	Transfer of auto-configuration information e.g. from Boot server - see 8.6.
Key distribution from KMS	Key management protocols protect keys in transit as defined in [SFS]
Transfer of business information to/from correspondence servers	Automated using Riposte TMS features
Distribution of help documentation and training mode data	Via Riposte TMS
System management via Tivoli including software distribution	Automatic using Tivoli. Scripts and software are signed for integrity protection.
Gathering diagnostic data for application support	Read access only to required data (NT event logs) via Tivoli.

5.4 System Delivery

As the result of Factory installation, Post Office workstations have NT, Riposte, applications and file encryption software installed. There is also a "failsafe" version of NT included in the installation which will not be updated by changes distributed via Tivoli. However, there is no specific information or code for a particular Post office. Personalisation information is added during installation.

POL00401199

At this stage, the filestore is not encrypted, though the directories are set up correctly for standard running.

The Riposte user groups are set up. The Manager, Supervisor, Clerk, Engineer and Auditor groups are used by people in those roles. The AuditorE group is used by Emergency Managers. The Support group is used for emergency procedures such as the Manager forgetting his password. The Engineer, Auditor, AuditorE and Support groups are set up to require one-time password authentication.

Usernames are set up in Riposte and NT for an Engineer, an Emergency Manager, a Support user and for a number of Auditors (enough to allow an auditor at each counter of the largest Post Office). There will also be a special Set-up Manager user used during Post Office installation - see 5.6. These users are associated with the relevant Riposte groups. (The Post Office Manager will introduce further users later.)

Some standard keys are included in this installation as defined in [SFS].

When leaving the factory, the only application which can be run is the Auto-configuration one (see 8.6). It is not possible to log-on to NT or Riposte.

5.5 System Installation/Reconfiguration

The Auto-configuration application at the counter is run by the installation engineer on the gateway workstation when the counters are first installed and after major configuration changes. It (together with the auto-configuration facilities at the Data Centre - see 8.6) sets up the link with the Pathway Central Services and installs the Post Office personality, and registers this Post Office with the Central Services.

When this has been done, the workstation is rebooted and the Post Office Manager takes charge.

5.6 Booting the System

When the system is rebooted after installation, the Manager puts a blank Memory Card in the reader and a PIN is generated for it (and printed unless there is a fault) and key material put on the card. The security initialisation process establishes the keys to protect the link and encrypt the filestore. The Manager then starts up each workstation for normal running.

POL00401199

From this point on, whenever any Post Office workstation is rebooted, the Memory Card is used for starting up the workstations securely as described in [SFS]. The start up process completes in the display of the Riposte log-on screen. No direct access to NT or Windows is possible at any time, even for engineers.

On first installation of the Post Office, the Manager logs in under the Set-up Manager username to create his individual username as a Manager for future use. On first installation, existing stock units need to be migrated to the Pathway system. This is done one of two ways:

- For Post Offices with manual records, the HFSO uses the MiMAN (Riposte) application under the PO Manager control. The PO Manager checks the bona fides of the HFSO and creates a migration user, including the HFSO's name in it, and with the role MIGRATION which only has access to the MiMAN application. The HFSO will logon (using a shared HFSO password) and input the required stock unit information. After migration, the Post Office Manager and HFSO check the name details are correct and the Post office manager deletes the migration account.
- For Post Offices migrating from ECCO equipment, the HFSO uses a laptop to read ECCO disks, and create Riposte attribute grammar records from them. These are then fed to the Correspondence server records for the Post Office via the Post office gateway and the Migration server at the Data Centre - see 8.6. As for manual migration, this is under Post Office Manager control. After migration, the ECCO disk is invalidated, so it can no longer be used and the Migration server will not accept another attempt at migration from this Post office.

If there is a failure on booting the counter systems after installation of a new package, the Manager, supported by the Horizon System Help Desk, reverts to the Failsafe version of NT.

5.7 System Access Controls associated with Human Roles

As for all domains, system access controls conform to the policies in section 3. The following specialisations of the general policies apply at this domain.

- A password cannot be re-used for 18 months.
- The password is checked to conform to quality standards as follows:
    - passwords cannot contain spaces
    - there cannot be more than two consecutive identical characters

POL00401199

- the password cannot be the same as the username
- the password cannot be one of an agreed "excluded passwords" list.

- The PIN used for the Post Office Manager's memory card is a 15 character alphanumeric value
- After a period of inactivity at a Post Office counter, the session will time out, but can be resumed on entry of the password. After a longer period of inactivity, the user is forcibly logged out.

The following table shows how access controls associated with human roles are enforced at the Post Office counters after installation and migration.

In NT and Riposte, there is no direct support for roles, so these are represented by user groups - see 5.4. Users are maintained using Riposte, which causes equivalent users to be maintained in NT.

Role	Function	Where users defined	Authentication needed	Resource access controls
Installation Engineer	Start up Post Office	Not in system	Manual procedures (see note 1)	Auto-configurer application only
Post Office Manager	Post Office installation	Not in system	Manual procedures	Memory Card and set up application only (see notes 2-4)
	Normal functions and key changes	Riposte user; in Manager group	Riposte username and password (see note 5)	Relevant Riposte applications only
	Emergency procedures (see note 5)	Riposte user in Support group	Riposte username and one-time password	All Riposte Manager functions
Counter clerks and Supervisors	All functions	Riposte user in relevant group	Riposte username and password	Relevant Riposte applications only
	training mode	Not separately defined	no separate log-on from live application use	Relevant Riposte applications with training data
All permitted PO roles	Workstation start up	Not in system	Memory Card and PIN (see notes 2-4)	Workstation start up only
Support Engineer	running diagnostics installing new hardware	Riposte user	generic Engineer Riposte username & one shot password (see note 6)	Relevant Riposte diagnostic application only. Auto-configurer application
Auditors	All functions	Riposte user	generic Riposte Auditor username	Relevant Riposte applications only.

POL00401199

Role	Function	Where users defined	Authentication needed	Resource access controls
			with one time password (note 6)	
Emergency Manager	Workstation start up	not in system	Memory card and PIN (see note 7)	Start up application only
	other functions	Riposte generic user	One time password	Riposte applications only

Notes:

1. The installation engineer will have an Id card with a photograph and signature and the Post Office will have been informed of his visit.
2. Memory Card use on installation and workstation startup is further defined in [SFS]. More information about Roll-out is included in section 8.6.
3. The Post Office Manager is expected to secure the Memory Card and PIN for it in separate places.
4. If the Manager looses his card or PIN, procedures require the Manager to get an emergency recovery key from the Horizon System Help Desk.
5. If the Manager loses his password, he logs in under a Support username, using a one-time password (see note 6), to reset his password on his normal user name. In the Manager's absence, this function may also be performed by an authorised deputy.
6. For authentication by one-time password, the Post Office System generates a value. The user then phones the Horizon System Help Desk with this, which provides a check value (after authenticating the user's identity). The check value is typed in to provide access to this username. For Engineers and Auditors, the pass number will also be typed in, so individual users can be identified in the log.
7. If the POCL Emergency Manager takes over a Post Office when the Manager is unavailable or unco-operative, he may need to use the Manager emergency recovery procedure to boot up the Post Office PCs - see note 4.
8. If the Post Office counter fails to boot, the Manager needs to revert to the failsafe version of NT. This is controlled by a one-time password, with the Horizon System Help Desk providing the check value as for Auditor authentication (see note 6).

After a user has logged on using Riposte, the Riposte desk top allows access to only those items available to people in the user's role. The user cannot call any other applications or NT or Windows functions.

POL00401199

The application called from the desk top runs in the Riposte user name but has limited privileges. It accesses filestore and other resources by calling the Riposte API to the privileged Riposte Service - it cannot access the files itself. The Riposte Service "impersonates" the user to access any user related resources. [Some access to print spoolers do not use Riposte, but are available to relevant applications.] The Riposte account (used for the desktop and message service) does not have administrator privilege.

All Riposte transactions, including user administration, are logged in the Riposte journals. On adding a new user, a full name must be supplied.

5.8 Other Access Controls

The Customer is an indirect user of the system who needs to be authenticated as defined in [SADD] for example:

- The customer brings a Pick-up Notice (PUN) with a bar-code as identification when collecting a Benefits card (or brings an existing card due to expire to collect a new card)
- The customer brings the benefit card as identification when picking up a payment. Extended verification is used on transactions particularly at risk of fraud such as foreign encashments.

Post Office staff may contact Pathway Help Desks and will need to authenticate to them as defined in the section 5.3.5 (for the Payment Card Helpline) and in 8.9 (for the Horizon System Help Desk).

6.

POL00401199

INTERFACE DOMAINS

The ICL Pathway project interfaces to systems run by other organisations at their sites as part of normal operation. These are:

- The DSS Service Environment Domain, where Pathway components at DSS sites interface to the DSS CAPS Service for payment authorisations and to the DSS ESNS Service for stopping order books.
- The POCL and POCL Clients Domain, where Pathway components at POCL sites interface to POCL services for handling reference data feeds to Pathway, Post Office transaction data to POCL and to support Automated Payments (which in future, could interface directly to POCL Clients).
- The De la Rue Card Services Domain, where Pathway components at De La Rue sites interface to the De La Rue services for card, temporary token and PUN production.

In all cases, the Pathway components are concerned with providing the interface between the Pathway Central Services and the other organisation's services. They do not provide significant independent application functionality.

In all cases, routers are managed by Pathway Network Management (see 8.5) and interface PCs are managed using Pathway System Management (see 8.3).

6.1 DSS Service Environment Domain

The DSS Service Environment Domain is illustrated in figure 6-1.

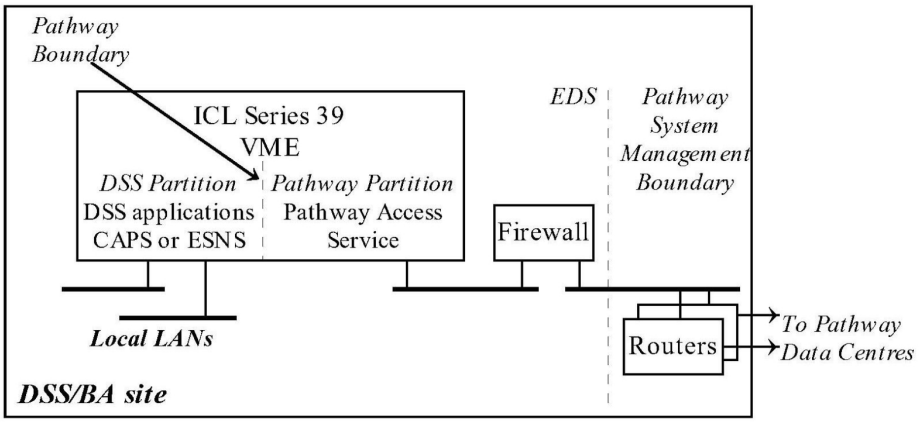


Figure 6 - 1 DSS Service Environment Domain

The DSS Service Environment Domain provides the interface between Pathway and the Benefit Agency's CAPS and ESNS systems at DSS sites.

POL00401199

In both cases, applications in the Pathway partition of the VME machines (the VME part of the CAPS and OBCS Access Services) handle:

- The transfer of information to/from the DSS partitions. An exchange of information about the files transferred (or on-line transaction) across the interface is used to check that the data sent is what is received.
- The transfer of information between the Pathway Services on VME and the Service at the Sequent operational system at the Pathway Data Centres.
- On-line transactions from DSS/BA staff to PAS.

These interactions are automated, so do not require human intervention in the Pathway partition of the VME machine. For on-line transactions from CAPS, the CAPS transaction is passed to an Oracle client in the Pathway partition which in turns calls PAS/CMS on Sequent in the Pathway Data Centre.

As well as the Pathway partition of the VME platform, this domain includes the Pathway routers used to route traffic to/from the Pathway Data Centres. These are managed by Pathway Network Management as described in [REF _Ref401824719 \n * MERGEFORMAT].

6.1.1 Roles

The DSS VME systems are run by EDS, so EDS are responsible for the main systems administration of them (including their split into partitions and resources allocated to these partitions) and the engineers analysing/repairing hardware or base software errors including those which involve the Pathway partition. This is not a Pathway responsibility, so is not covered by this Access Control Policy.

DSS BA and DSS Help Desk staff are indirect users of the Pathway VME partition. The CAPS on-line transactions pass through to PAS/CMS, though have no access to facilities at the Pathway VME partition. These users are authenticated to the DSS systems; Pathway accepts and carries out these transactions without further authentication of these users. (Pathway trusts any on-line transaction from DSS via the agreed interface. The DSS system will have performed the required access controls for these users, for example, to ensure DSS Help Desk staff are restricted to enquiry only access.) At the interface, the DSS/BA member of staff is identified by a transaction id which is used for Pathway auditing.

Pathway roles at the VME partition are:

POL00401199

- Operational management and application support roles for the VME partition, including monitoring. This is carried out from a secure Pathway site using interactive (MAC) access via Sonnet on Sequent. The users will have been authenticated individually to others systems - see section 8.
- The Key Custodian who installs and updates the Red Pike cryptographic keys used to protect the transfers of information from CAPS to the Pathway Data Centres (at least the trailer record giving the file totals and the checksum). This role is done by EDS at the local DSS site.

All users of the VME Pathway partitions will individually identified and authenticated using the VME Enhanced Security Option.

6.1.2 System Access Controls

The Pathway VME partition has its own filestore separate from other partitions. This filestore is set up to separate data with different access requirements and profiles are also used to restrict access as needed to conform to the policies in section 3. Transfer of data between the Pathway partition and CAPS/ESNS is restricted to transferring files to/from the special transfer usernames using the XPERT product.

6.1.3 Control of Traffic between VME and the Data Centres

All traffic between VME and the Pathway routers is OSI based so the routers handle bridged OSI traffic. The router LAN interface should be configured with Access Lists at two levels. The first should provide a MAC filter, so that only the Ethernet address of the EDS firewall router and the other router are allowed as source addresses. The second should provide an IP filter, so only the IP address of the other router is allowed as a source (for network management traffic).

Permitted connections between Pathway Data Centres and the DSS site are:

- File transfer between the relevant VME service and PAS/CMS and OBCS on Sequent.
- SQL*Net traffic supporting the CAPS on-line service
- Interactive (MAC) access for management, support and auditing
- Network management traffic to the routers.

6.2 POCL and POCL Clients Domain

Pathway has links to POCL and POCL Client systems. These are:

POL00401199

- The POCL TIP system to which records of transactions at Post Offices are sent. This link is also used for Royal Mail traffic
- The associated POCL system which provides reference data about Post Offices and for EPOSS applications and shares the TIP link.
- The POCL Host Automated Payments Service (HAPS) which processes Automated payments on behalf of POCL Clients. This will be replaced in future by:
- Links to POCL Client systems for automated payments.

At each site, there are Pathway PCs and routers connected to the POCL or POCL Client systems there as shown in the following diagram.

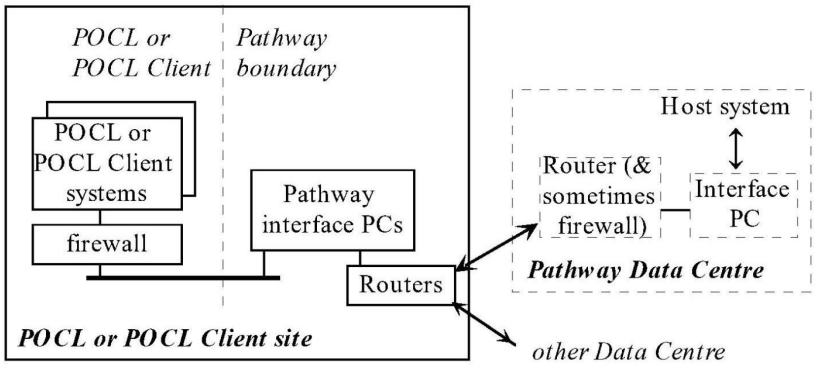


Figure6-2 Pathway components at POCL Sites

The Pathway PCs at the POCL and POCL Client sites handle file transfer to and from the Pathway Data Centres. Differences between these sites are:

- The TIP/Reference data link is via the Energis network
- the HAPS link is a leased line with protection provided by encryption boxes
- The POCL Client links are expected to be ISDN ones with an ISDN card in the Pathway interface PC, rather than a separate router.

Cryptographic protection of the links is outlined in 8.10 and defined in [SFS].

6.2.1 Roles

Once configured, the PCs and routers at these sites will not normally have any human access as applications are automated and the PCs are managed remotely using Tivoli. Pathway roles supported are:

Role	Main function
Key Custodian	Installing new keys and changing keys (for systems

POL00401199

Role	Main function
(Pathway)	where file transfers are encrypted)
Key Handling (POCL or POCL Client)	Re-installing keys on re-booting PCs (for systems where file transfers are encrypted)
Operational management	Limited, local system administration functions
Engineer	Installing or replacing PC. The PC will not be repaired when configured into the operational system.

6.2.2 Control of Connections to the Pathway Data Centres

Traffic is permitted between the Data Centres and these sites is:

- The file transfers between Pathway hosts (TPS, Reference Data and APS) and the POCL/POCL Client systems
- System Management traffic to manage the PCs using Tivoli
- Network management traffic for router management

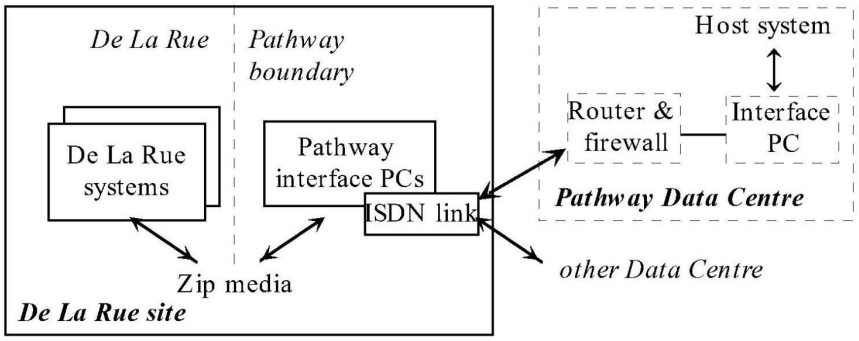
In all cases, traffic is controlled by routers (and firewalls for ISDN links) at entry to the Data Centre which will restrict the traffic to that permitted. The Pathway router at the POCL sites accepts only this traffic.

6.2.3 Control of Connections to POCL Systems

Access from the POCL systems is by file transfer. Controls at the PC will ensure separation of incoming and out going files so that all files supplied by Pathway are read only for POCL access. In addition, files for different systems (e.g. TIP, Royal Mail and Reference Data) are separated.

6.3 De La Rue Card Services Domain

The De La Rue Card Services Domain is illustrated in figure 6-3.



POL00401199

Figure 6-3 De La Rue Card Services Domain

Files of data for card, PUN and temporary token production are transferred from CMS on the Sequent machine at the Pathway campus to a PC at the campus. They are then encrypted and transferred via ISDN to the Pathway PC at the De La Rue sites where they are decrypted as described in [SFS]. Information is transferred between the Pathway PCs and De La Rue systems by being written to/read from Zip drives to provide a secure air gap between the systems.

De La Rue operations take place using secure systems in a secure site. De La Rue information system controls and procedures protect the information there.

6.3.1 Roles and System Access Controls

Roles supported on the Pathway PCs are as in 6.2.1 above (plus the operator who physically moves the tapes). De la Rue perform the Key Handler role.

Control of traffic between the De La Rue site and the Data Centre is as in 6.2.2 above.

7.

POL00401199

PATHWAY CORPORATE SERVICE DOMAIN

7.1 Introduction

This domain contains Pathway's own processes for managing and supporting the business. These include:

- Fraud Risk management (FRM) - both Pathway and DSS
- The Payment Card Helpline which supports users, POCL, DSS and customers, by handling calls about cards and payments
- The Business Support services which handle financial reconcilations
- Business Function and Security Event Auditors
- Security Management
- Other management processes such as accounting, monitoring service level agreements and asset management.

Management Information Systems support many of these management processes. However, some of these Pathway Corporate users also require access to other systems. This section covers, therefore both the Pathway Corporate users (and their access controls) and the Management systems which support them (and how they are controlled).

7.2 Workstation Controls

Most business management and support users are located at a Pathway management site (such as Feltham), except for some FRM staff, the Payment Card Helpline and key custodians and handlers. Workstation controls at management sites are shown in the following diagram.

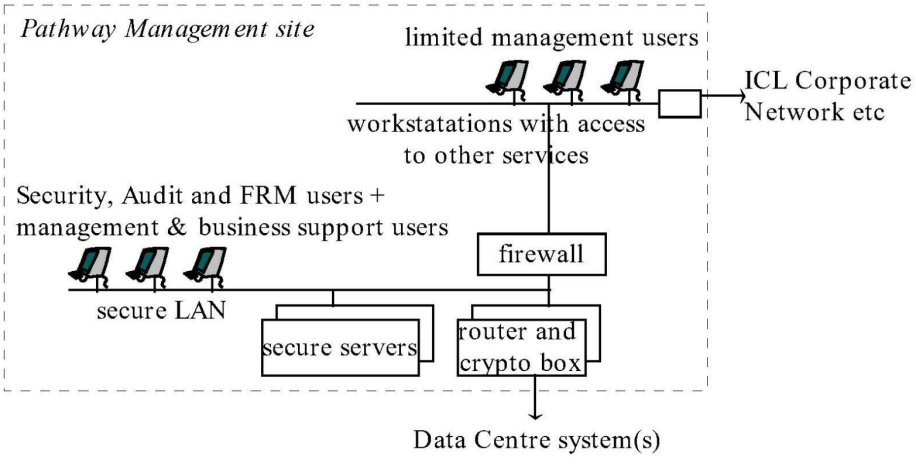


Figure 7-1 Management user workstation controls

POL00401199

7.2.1.1 All users who have access to sensitive data at the Data Centre or update any information there (e.g. Management support users updating Business Object Universes) must access the system from the secure LAN which is in a physically secure area restricted to permitted users.

7.2.1.2 All such users should authenticate using a token.

7.2.1.3 All workstations on the secure LAN at the Pathway management site are controlled NT workstations set up to Pathway standards. These restrict access to permitted functions for that user and have floppy/CD drives disabled for booting, except where exceptions are agreed.
The current agreed exceptions for management and support users is that some of these users have write access to CDs to allow information to be put on CD for transfer to DSS and/or POCL. This is permitted for the Management support role (see 7.8) for providing agreed warehouse data, for the FRM supervisor (for providing information to DSS FIT) and for the Business Function Auditor (for providing information to external auditors)? *[In future, some transfers of data, e.g. to DSS FIT, may be via an encrypted link, not CD.]*

7.2.1.4 Limited (read only) access by some management users is permitted from the main Pathway network at the management site to management services, such as the Service Level Agreement Monitoring system (SLAM), at the Data Centre. This is subject to controls at the Feltham network (see 8.x) and is restricted to where the services at the Data Centre are not on the main operational or warehouse machines and the firewalls and routers restrict this access to the required services on the particular management machine.

7.2.1.5 Where users (particularly the Payment Card Helpline and Girobank FRM) are located at the Pathway Data Centre sites, the links to the Data Centres do not need to be encrypted, as the users are not remote.

7.2.1.6 DSS FIT staff may access the FRMS service from their own site. Remote access should be from a secure DSS area, using controlled NT workstations, via an encrypted link.

7.2.1.7 Servers at the management site which require strong security, such as the CM signing server and reconciliation database, should be on the secure LAN

POL00401199

Sections 7.3 to 7.8 outline the access controls for Pathway Corporate roles which involve systems other than MIS ones. Note, however, that controls for a user at a particular service or system are defined in the section for that service. Section 7.9 below gives the access controls associated with the Management Information Systems.

7.3 Fraud Risk Management

Fraud Risk Management is concerned with identification, monitoring and management of fraud associated with/relevant to the ICL Pathway system. Both the Girobank Fraud Risk Management (FRM) staff at Bootle and the ICL Pathway FRM staff at Feltham use the same services i.e.

- Regular reports on aspects of the system which are relevant for fraud e.g. weekly trend analyses and daily exception reports and ad hoc selective reports according to agreement.
- Access to the Fraud Case Management System (FCMS), both to create and maintain cases originated by Pathway and to read case data about cases originated by DSS Fraud Investigation Team (DSS FIT)

Most FRM access to Pathway is to the Data Warehouse and the FCMS applications. In exceptional circumstances, FRM staff may require access to other Pathway systems in order to investigate a potential fraud. These are currently expected to be:

- The PAS and CMS data. This is expected to be mainly to the archives, not the operational system, except in exceptional circumstances.
- The TMS journal of Post Office activity
- Data transfer logs

DSS FIT staff can create and maintain their own cases in the Fraud case database and have read access to cases originated by Pathway FRM staff. Any other information they require is obtained by the Pathway FRM staff - both regular reports and specifically requested information.

The following table lists the FRM Roles.

Role	Functions
Pathway FRM Manager	Investigating fraud cases using FCMS, Data Warehouse information, and where needed, operational systems including TMS and PAS/CMS. Supervisor of FCMS and also FRM Business Object universes, so create/expire users in FCMS Setting flags for transactions in FCMS (code user).
FRM Analyst (an ICL Pathway	Investigating fraud cases as FRM manager (including access to Data Warehouse, TMS etc)

POL00401199

Role	Functions
role)	FRM supervisor functions as FRM manager
FRM users (ICL and Girobank FRM staff)	Handling fraud case information in FCMS Read only access to Data Warehouse information in support of investigations.
DSS Fraud Investigation Team (DSS FIT)	Read and update access to cases initiated by DSS FIT; Read only access to cases initiated by Pathway FRM staff. Access to extracts of Data Warehouse information (extracted by Pathway FRM staff.); no direct DW access

Access controls at the various data centre systems are in the appropriate section - 7.9 below, and also parts of section 4, when they have access to central services. All these users access the system from controlled workstations on protected links - see 7.2. In some cases, FRM Manager and Analyst may use facilities similar to the Business Function Auditor.

Fraud investigations will also include collection of evidence. Some evidence will be collected by requesting information from other users, rather than direct FRM staff access.

7.4 Payment Card Helpline

The Payment Card Helpline is run by Girobank at the central Pathway sites. It handles the following types of calls:

- Calls from Post Office counter clerks about payment authorisations and cards. Some of these can initiate changes to the PAS/CMS database, for example, to stop a card, encash a payment (under the responsibility of the Post Office clerk)
- Calls from customers about card problems (some of which could result in stopping cards), and more general queries
- Calls from DSS/BA, some of which can result in stopped payments, stopped cards
- General calls from the public, for example, reporting finding a card

Helpline Advisors use the PAS/CMS database when responding to telephone calls. (They also have access to local on-line documentation, such as the procedures they must follow, from local Helpline NT servers.)

7.4.1 Roles and Associated Controls

People in the following roles have access to PAS/CMS:

- Helpline Advisors using authorised transactions in response to calls

POL00401199

- Helpline Advisors (NSI) who can handle data with a National Sensitivity Indicator
- Helpline Supervisors who can act as advisors, but also perform extra transactions (and have extra local functions)
- Helpline Manager who can perform the same role, but has further local functions
- Helpline Security Manager who maintains information about the Helpline users both at PAS/CMS and at the local system

In all cases, Helpline users with access to PAS/CMS use controlled NT workstations with floppies disabled. They log onto the local Helpline controlled NT domain with an individual username and password and local profiles control what local functions they can do according to role. This controls which Helpline staff can use which Oracle Forms applications for accessing PAS/CMS. These workstations also provide access to some local functions (e.g. viewing on-line documentation), but not to external services.

Access to PAS/CMS is also controlled by the PAS/CMS servers (see 4.3.1) which require the users to log-on to Oracle and then restrict what tables Helpdesk users can access. Note, however, that as Helpline users have update access to some PAS/CMS data, the controls on the Oracle Forms applications at the workstations are needed to prevent update access to other data in those tables.

A set of dedicated workstations are used for training activities accessing the training database at the Data Centre.

7.4.2 Other Access Controls

The Helpline system is a controlled network with routers controlling all access in and out. This is limited to:

- the Pathway Data Centres - for PAS/CMS access and information about telephone calls to the Data Warehouse
- between Helpline sites and
- to the Rockwell ACD and associated servers. (Information is fed from the Rockwell ACD to a specific PC on the helpline network so that telephone traffic may be monitored.).

POL00401199

7.4.3 Authentication of Callers

Contact is made with the Helpline Advisors from Counter clerks, the Benefit Agency and customers by phone as detailed in the call matrix in [CHDM]. There will generally be a need for the caller to provide some level of authentication that they are who they claim to be.

Note: the procedures for handling telephone authentication are not yet finalised in all cases.

Contacts with these people are shown in the following table.

Contact	Function	How authenticated
Customers	Queries and reports about cards, PUNs. e.g. card lost or damaged.	Response to a number of verification questions asked by the Helpline Operator as specified in [SADD].
Members of the public	Reports such as found card	No caller individual authentication normally (as the caller may not be known to the system). However, the caller may be asked further verification questions depending on the type of call.
Staff at Post Office	Get payment details and extended verification e.g. for foreign encashment. Reporting on failures & anomalies	Correct responses to questions based on information held at the Helpline about Post Offices - see section 3.5.2.
PO staff on behalf of customer	Queries and reports about cards etc	As above for verification of Post Office staff plus customer verification information.
DSS/BA	Enquiries on cards, payments. Request to stop cards, payments etc	Correct responses to questions based on information held at the Helpline about DSS sites/people.
BA for customers	As customer queries and reports	See above for verification of BA staff, plus customer verification information

7.5 Business Support

Pathway Business Support staff handle financial reconciliation when there is a Pathway problem, for example a service breakdown. There are two types:

POL00401199

- Reconciliation incidents for DSS benefit payments.
  This role requires access to information about customer payment authorisations and Post Office transactions at operational services. (Where larger volumes are concerned, relevant data may need to be downloaded at the request of Business Support to the SSC reference system (see 8.7) and a flat file of transaction adjustments generated there for forward transmission to the Data Centre and back to CAPS by SSC.)
- Reconciliation incidents for in the Automated Payments Service for other POCL clients.

The same BSU staff handle both sorts of reconciliation incidents. Roles are:

Role	Functions and resources accessed
Business Support Analyst	Investigating incidents, and inserting or adjusting payment records (but not finally authorising them.) Analysts therefore have access to PAS/CMS, TPS etc and also to the reconciliation (RED) database - a secure server at the management site.
Business Support Manager	Inserting or adjusting payments and authorising them, subject to agreed procedures. The BSU Manager has access to all the systems available to the Analyst

Notes:

1. BSU staff are located at a Pathway management site and access the Data Centre systems via secure workstations using tokens - see 7.2. All update access is via specific Oracle forms applications.
2. These same controlled workstations should also be used for access to the RED database, as this holds DSS Restricted data
3. Services accessed for DSS payment reconciliation include PAS/CMS and OBCS, and TMS
4. Services accessed for APS reconciliation are APS and TPS

7.6 Auditing

Pathway activities are audited to ensure they are functioning correctly, for example, that the controls in the system are working effectively. Within the Pathway project, two types of Auditors are distinguished:

- the Pathway Business Function Auditor responsible for overall auditing of the system
- the Pathway Security Event Auditor

POL00401199

The external (POCL, DSS and NAO) Auditors are mainly concerned with auditing the business transaction of the system such as the processing of payment authorisations and customer information and the transactions at the Post Office. The Pathway Business Function Auditor provides the interface to external auditors for access to Pathway Data Centre systems, accessing these systems on their behalf to provide the information they need.

7.6.1 Overview of Audit Information Accessed

Auditors requires access to information in the audit tracks defined in [AUDT]. Security Event Auditing is concerned with auditing all access to the Pathway systems, including that by Pathway operations and management staff. The main activity is monitoring, though on occasions, more active investigations are expected. Business Function Auditors also have access to audit logs, though they will be looking at different information in them.

Audit logs include:

- Operational and management logs of business transactions such as the Riposte journal which records events at Post Offices and the PAS and CMS logs (including records of Payment Card Helpline transactions)
- Logs recording system level activity at Pathway Data Centre systems such as user logon and administration and other security relevant events including system, network and firewall management.
- Logs at relevant Pathway internal systems.
- Archives of these at the archive server retrieved from the Legato tapes there
- Manual records associated with IT access.

Many events are collected centrally using Tivoli (via Patrol and Openview where needed). The technician monitoring the systems management workstation will alert the Security Event Auditor of specified types of significant events. However, some event records will remain in local audit logs.

The Security Event Auditor will need to be able to access/extract audit data from all these - see the following diagram.

POL00401199

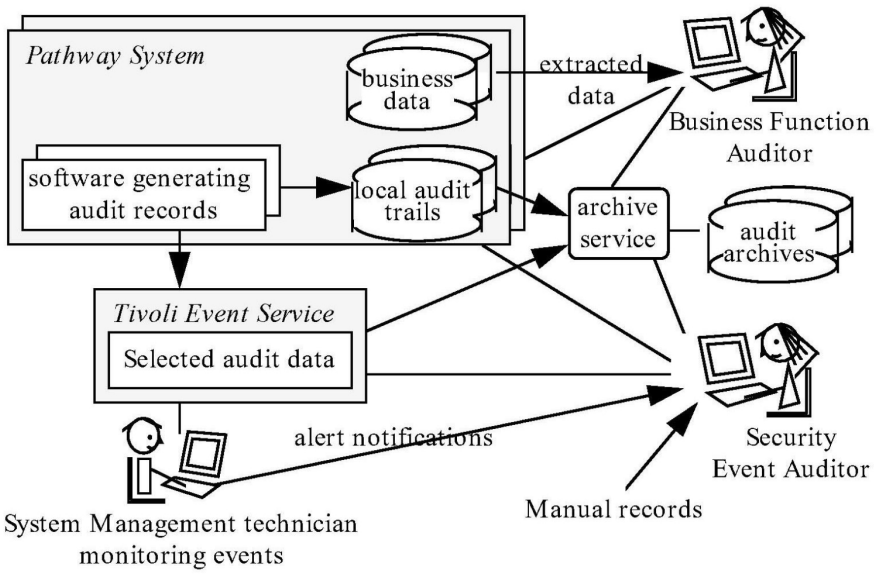


Figure 7-2 Auditor access to audit information

The Business Function Auditor mainly uses information to the archive server and to information extracted from other systems, though has limited access to other systems.

7.6.2 System Access Controls

Auditors can access the logs at Pathway systems described above by tools/clients at the audit workstation. The auditors are registered at each system/domain accessed and can access only the audit logs there as included in the relevant sections. Note that Auditors will not have direct IT access to:

- Post Office systems: however, all Post Office transactions (including user authentication) are recorded in the TMS journal and other relevant system events are picked up by the Tivoli Event system or
- The Payment Card Helpline systems: all interactions of the Help Desk users with the Pathway systems are recorded in the Oracle logs on Sequent.
- The interface PCs at POCL and De La Rue sites: management of these will be recorded in the Tivoli logs

Both Business Function Auditors and Security Event Auditors access the Data Centre systems via controlled workstations on the secure LAN in Feltham (see 7.2 above) or a similar workstation at the Data Centre.

POL00401199

7.7 Security Management

Pathway Security Management are responsible for Security Event Auditing of Pathway (see 7.5 above) and also:

- Management of the cryptographic keys used in Pathway
- Management of the Security tokens used for authentication of some users (see 3.4.2.5)

and other security matters.

7.7.1 Cryptographic Key Management

Several of the Pathway systems require a cryptographic key to be installed and periodically changed. These keys are used to encrypt/decrypt or sign/verify data in transit between sites. Some keys are generated by the Pathway Key Management Service (see 4.6). Others are obtained from CESG.

Keys may be distributed electronically (for example, to Post Offices). However, at some systems, the cryptographic key (or part of it) must be installed manually. This is the case, for example, on the following systems:

- The BES agents. These have the private key for signing payment authorisation for transmission to the Post Offices.
- Systems using Red Pike encryption of data on links e.g. the Sequent system for the link to CAPs and the PCs handling the links to De La Rue.
- The Zergo boxes used to encrypt certain links such as the Data Centres to Pathway sites such as Feltham and Stevenage.

All keys are managed in accordance with the policies in 3.6.

The cryptographic key management roles are as follows:

Role	Main functions
Cryptographic Key Manager	Generating or obtaining cryptographic keys and organising their distribution.
Cryptographic Key Custodian	Initial installation of cryptographic keys where this needs to be done manually. Periodic update of these keys.
Cryptographic Key Handler	Handling part of a split cryptographic key when this needs to be re-installed e.g. when a system is rebooted.
PO key recoverer	Initiating recovery of a Post Office key from the Help Desk after it has been lost.

POL00401199

The Cryptographic Key Manager and PO key recoverer roles access the IT system at the central security services only, so their access controls are described in 8.3.

All Cryptographic Key Custodians and Key Handlers access the systems in a similar way as defined in the following table.

Role	Workstation type & location	Authentication method	Resources available
Key Custodian	console at the platform with key	NT (or UNIX) with token	Functions to install and change key
Key Handler	None	None	Media containing key during re-installation of key.

7.7.2 Management of Security Tokens

There is a single role here - the **Pathway Security Manager** (PSM) who maintains the records of tokens, PINs and users.

The PSM uses a controlled NT workstation on the secure LAN at the Pathway management site (see 7.2) and has access to the Token Authentication Service at the Data Centre (see 4.6.2). Functions available to the PSM are:

- maintaining information about tokens and their associated PINs, and whether, and to whom, they have been allocated
- maintaining information about users who have tokens

The PSM is also responsible for the procedures to handle tokens which have been lost, stolen or withdrawn from use, and procedures for the security of handling PINs, so these do not allow unauthorised access to the system.

7.8 Other Management Users

The following Pathway general management users have access to MIS systems (see 7.9), and no other, Data Centre systems. Their access controls at those systems are therefore included in that section. (Their workstation controls are in 7.2 above).

Role	Main Functions
Pathway Management support	Managing the set-up of the management information services (e.g. setting up Business Object Universes and associated controls). Providing information to other Pathway Management users on request

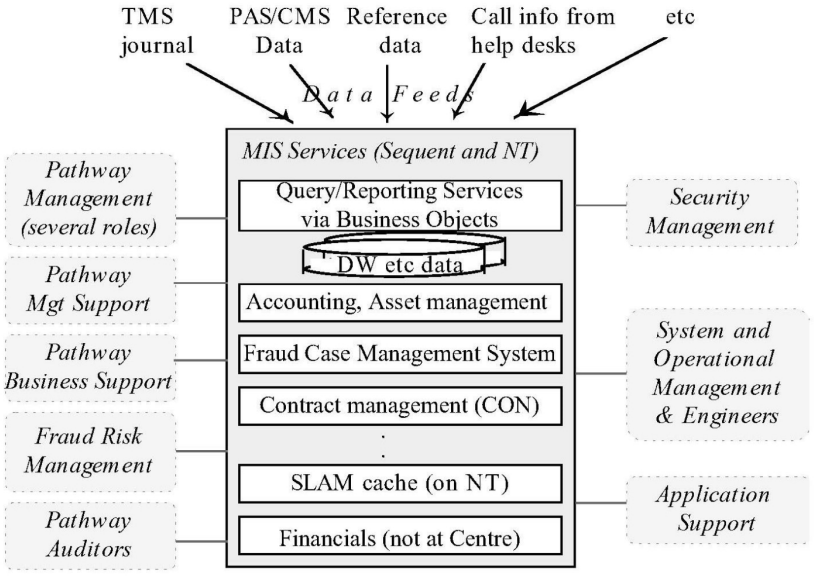
POL00401199

Role	Main Functions
	Also, providing the POCL and the DSS/BA interfaces for management information - including provision of management data regularly and on request.
Pathway Financial Management	Use of finanical management information in the Common Charging System (CCS) and elsewhere
Pathway Contract Management	Use of contract management information in the Contract Management system (CON)
Pathway Reference Data Management	Use of reference data in the Data Warehouse
Pathway Customer Support (CS) Managers	Access to the SLAM cache on NT
Pathway Business Development	Use of selected Data Warehouse information in development of the business

All users except CS managers use controlled NT workstations on the secure LAN at the Pathway management site - see 7.2. Pathway Management Support users have writable CDs for generating information for POCL and DSS.

7.9 The Management Information Systems (MIS)

There are two Sequent platforms at the Data Centre supporting Management Information Services; one is the Data Warehouse - the main information repository for Pathway corporate services. There is also an associated NT server. These MIS and Fraud Risk Management services are illustrated in figure 7-3.



POL00401199

Figure 7-3 MIS Systems

The Pathway Management Services include generating invoices for the Contracting Authorities (using information derived from the operational system), monitoring Service Level Agreements on the performance of the Pathway solution, business development applications (providing aggregates and summaries to identify sales trends and customer habits) and Accounting and Asset management.

Data is fed automatically from other Pathway systems to the Data Warehouse including:

- Data from TMS journals about Post Office transactions (see 4.8).
- Data from the Reference Data Management System (see 4.7)
- PAS/CMS data (see 5.2)
- Information on calls to the Payment Card Helpline. This consists of Rockwell ACD data (see 5.3) and Mercury data.
- Information on calls to the Horizon System Help Desk. This consists of Mitel ACD and BT data.

Much of the output of this system is by using the particular services. These provide the management information required by Pathway and the outputs required by DSS and POCL. There are automatic feeds from Data Warehouse Services to the EIS/Financial service and to the Service Level Agreement Monitoring service (SLAM cache) which is on an NT system at Wigan.

7.9.1 System Access Controls

Both Sequent MIS systems are managed in the same way as the other Sequent systems at the Data Centres, though there is some differences in support due to the different applications run on the MIS systems. So the roles defined in 4.2. above (operational management, database support, application support, auditors etc) are also used here, except for the VME related roles in 4.2. Note that some of these include application/database roles, for example, for Auditors.

The NT server is managed as other NT servers at the Data Centre (so supports the roles defined in 4.4) except for management specific roles and data flows.

POL00401199

Database roles with appropriate database views/tables are used to separate what data is available for what use. Information available to people doing ad-hoc queries is further constrained using the Business Object "universes" to provide restricted views of the Data Warehouse and other MIS Oracle applications.

The following table shows the application specific roles for the MIS systems. In all cases, users have authenticated to their local NT systems prior to access to the MIS system.

Role (and section where defined)	Authentication method at MIS	Resources available
FRM Manager (7.3)	Oracle/Business Objects	Access to all FCMS case information; create/expire users (FCMS supervisor), setting FCMS codes (FCMS code user). Access to Data Warehouse information, both predefined and ad-hoc queries. Administration of FRM Business Object universes (see 7.3)
FRM Analyst (7.3)	As above	Full access to FCMS except code user. Access to Data Warehouse information as for FRM Manager
FRM User (7.3)	As above	Access to FCMS case information; Read only access to Data Warehouse information
DSS FIT (7.3)	As above	Access to case information (but not Pathway specific information) Access to extracts of Data Warehouse information (extracted by Pathway FRM staff, and made available to DSS FIT) - no direct Data Warehouse access.
Pathway Management Support (7.8)	Token plus application authentication	Business Object Universes (including supervisor functions); Read and update access to agreed MIS data including CON, SLAM, BPS; Data required for download to workstations for reports (pathway, POCL, BA)
Pathway Financial Management (7.8)	As above	Access to Common Charging System (CCS) and other financial information
Pathway Contract Management (7.8)	As above	Access to CON service
Pathway Ref. Data Management (7.8)	As above	Access to DW reference data
Pathway CS Managers (7.8)		Read only access to SLAM cache on NT only

POL00401199

Role (and section where defined)	Authentication method at MIS	Resources available
Business Development (7.8)	As above	DW: read only access to Post Office information

7.9.2 Control of Connections

All access to the MIS systems at Wigan from outside the campuses is by encrypted links.

Access to the system is constrained to the agreed data feeds, management and audit use and output to the EIS/financials system.

8.

POL00401199

SYSTEM MANAGEMENT SERVICES DOMAIN

8.1 Introduction

This Domain includes services for:

- Management of the systems in all Pathway domains. There are two main types of system management:
    - Managing the Post Office systems and related Data Centre NT systems (mainly using Tivoli products)
    - Managing the Sequent Data Centre systems (and the Pathway VME partition). While this mainly uses Patrol and other tools, events can still be reported into the Tivoli management system.
- Network Management - managing the routers and firewalls which control traffic into, out of and within the Pathway network. Routers are managed using Open View at the Network Management Station and firewalls managed by the Enterprise Centre.
- Software and Configuration information distribution, both for roll-out and auto-configuration of new Post Offices and release of software updates from the Pathway Configuration Management system to all systems including Post office and Data Centre ones.
- Application support for services in all domains (though access controls for particular services and systems are given with the controls for that system).
- Support of specific hardware not covered by other sections such as symmetrix discs.
- The Technical Help desks which support this - the Horizon System Help Desk which is the main technical Help Desk and the Roll-out Support Desk supporting the Implementation process.

Access controls associated with each of these are covered in the following subsections. The last subsection describes the network access controls which the system/network management achieves. It outlines the network and the positioning of controls in it, and then the access control policies for it.

8.2 Outline of System and Network Management

The following diagram illustrates the main components of system management during operational use of the system. (Roll-out is covered in section [REF _Ref401847521 \n * MERGEFORMAT]).

POL00401199

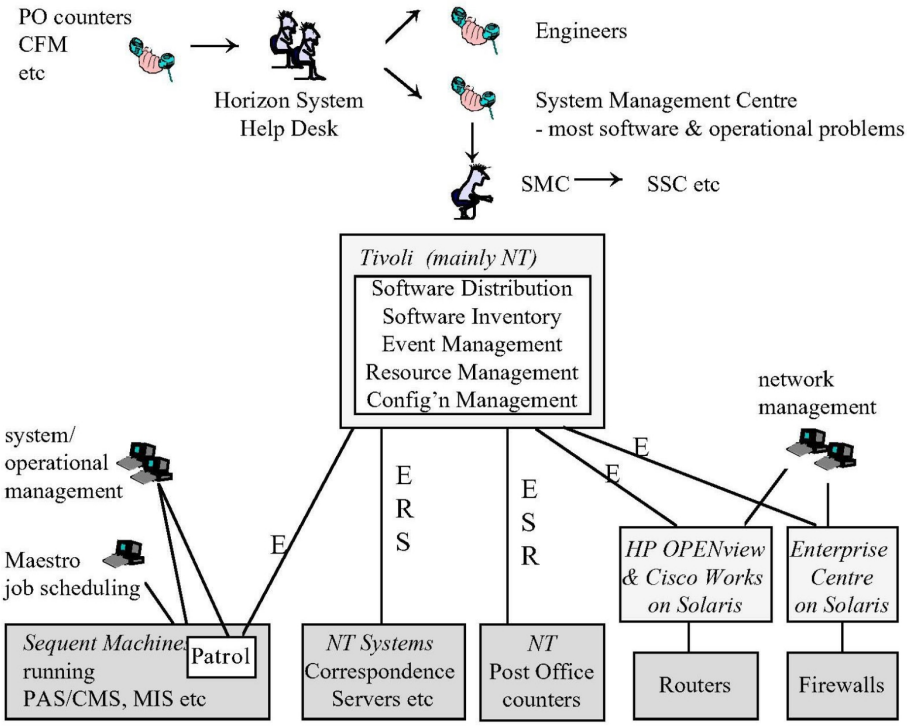


Figure 8 - 1 System Management Service Domain

In the figure,

- E - shows event management - Tivoli manages events either directly (as with the Correspondence servers and Post Office counters) or indirectly (via Patrol at the Sequent systems)
- R - shows resource management such as performance and capacity monitoring (for Sequent, inventory management)
- S - shows software distribution from the Tivoli server. (Distribution of software from the Pathway Configuration Management system is in 8.6.)

The Tivoli Management Environment (TME) provides Event Management, Resource Management and Software Distribution. In some cases, this is done directly by Tivoli at the Pathway Operational systems. This is the case for the Correspondence servers, for all Tivoli servers (some of which are on UNIX systems) and other NT boxes at the Pathway Data Centres. However, for the Sequent machines (both operational and management ones), most management is done using Patrol with events selectively being passed onto the Tivoli Event Management System. Similarly, Open View and Cisco works are used to monitor and manage the routers, but send events selectively to Tivoli.

POL00401199

Management actions may be initiated automatically by System Management software detecting threshold conditions and automatically taking remedial actions. System management staff initiate actions as follows:

- For planned activities such as distribution of a new software version.
- Where monitoring the events in the system shows action is needed.
- When a Technical Help Desks receives a call from external people (e.g. Post Office staff) or Pathway staff (e.g. CFM operational management staff) requiring action

8.2.1 System Management Workstation Controls

System management technicians have access to the Pathway Data Centre systems in order to manage them. In doing this, some will have the capability to update the systems (and potentially disrupt the Pathway services). Some technicians will also have access to DSS data where this is needed to investigate a problem.

Many of these technicians also need to use the call recording and management systems used to record to process of technical incidents from initial call to the Help Desk, through calling in the required experts to investigate the problem to the final completion of any remedial action to rectify the problem. The key tools used here are the Powerhelp and PinICL systems.

Thus these users normally need access to both the Data Centres and internal ICL systems. In this case, their access to the systems is as shown in the following diagram:

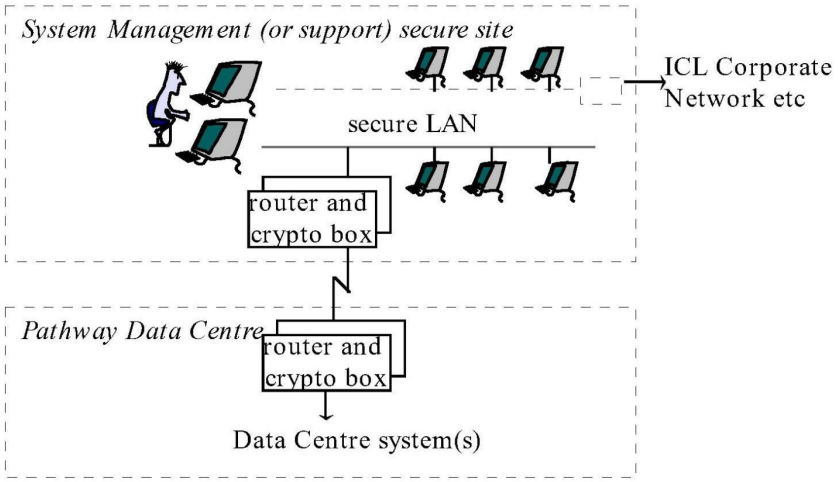


Figure 8-2 system management workstation/network controls

POL00401199

The technician often has two workstations connected to separate networks:

- an NT workstation configured to Pathway standards and connected to a separate secure LAN. Apart from other management workstations for other technicians, this LAN is connected only to the Data Centres via routers and cryptography boxes. All traffic between the secure LAN and the Data Centres is encrypted. The NT workstations have floppy drives disabled.
- if needed, a workstation connected to other systems such as the Powerhelp and PinICL systems used for tracking technical incidents.

  Where the incident tracking systems use networks outside the Pathway controlled area, for example, the ICL corporate network, information recorded on it associated with an incident may refer to a particular record of DSS customer data, but will not include such DSS data, unless adequately protected, for example, by encryption.

System management and support technicians work in physically secure areas.

In the rest of this section, only the controls associated with the NT workstations which can access the Data centres are included.

All system management users managing Data Centre systems authenticate using a token.

8.2.2 Procedures for getting in Support Staff

A number of problems can lead to staff being required to support the system. This could be CFM or SSC staff coming in to support the system from their normal support sites. However, it could also require support staff from other organisations such as Oracle or Cisco. CFM is generally responsible for the call out procedures.

8.2.2.1 All requests for technical support should be made to the Horizon System Help Desk. The identity of the caller requesting support (if by telephone) should be verified to ensure the call comes from an appropriate source, so should be acted on. The Help Desk will pass on the call to the appropriate unit in line with Help Desk Procedures using the call handling system.

8.2.2.2 All support calls should be recorded in the call handling system and their progress reported there, including who was called out and the actions taken.

POL00401199

8.2.2.3 Routers will by default be configured to prevent access from support organisations other than the standard ICL Outsourcing sites supporting Pathway. When support is required from another authorised site (e.g. Oracle or Cisco), a router should be configured to allow this access, and then re-configured to disallow it after use.

8.3 System Management of NT Systems

System Management of NT systems is done using Tivoli. This includes managing the Post Office counters, NT servers at the Data Centres and interface PCs in interface domains. Support is also provided for special Post Office cases such as lost passwords. Other Pathway people such as auditors and application support also access Tivoli for information. The main interactions of the people involved are illustrated in figure 8-2.

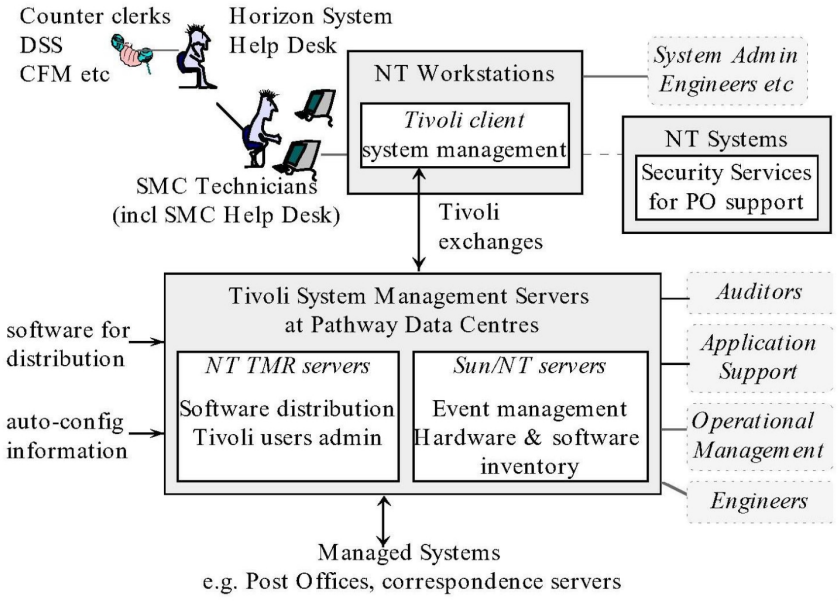


Figure 8-3 Interactions for Tivoli System Management

SMC technicians perform system management activities because:

- System management actions have been planned, for example, the distribution of software or the implementation of Post Offices.
- Monitoring of the system identifies some action is needed.
- The Horizon System Help Desk passes on a call about a technical problem which requires resolution.

Software is sent to Tivoli from the Configuration Management system; Post Office configuration data comes from the Auto-configuration database (see 8.6). In both cases, SMC technicians control onward distribution of the data.

POL00401199

SMC technicians have two workstations - one with access to the call handling systems including Powerhelp and a second which provides access to Pathway system management services.

SMC Team Leaders also handle calls from the Horizon System Help Desk to authenticate users at the Post Office using one-shot passwords and to assist in key recovery as described in 5.7.

8.3.1 SMC and Roles at Tivoli Servers

The SMC system management roles with access to the IT systems are:

Role	Main Functions
SMC technician or technical specialist	Monitoring the system - software distribution, the auto-configuration process and other system management events. For software distribution, select targets for distribution from those authorised and report of progress. Run pre-defined, pre-allocated tasks. Raise alarms on pre-defined conditions
SMC technical team leader	For software distribution, authorise targets for distribution, change priorities or cancel distribution and report on progress. Other system management tasks as SMC technician. Authenticating users at the Post Office using one-shot passwords as described in 5.7. Assisting in Post Office key recovery - see 5.7 and 4.6.
SMC MSS technical support	Handle receipt of software and auto-configuration information. Configure Tivoli event management - configure the view of events by others and task event relationships and add new Sentry monitors. Create Tivoli tasks and allocate to SMC technicians. System administration of the SMC workstations and Tivoli servers (NT and UNIX systems) including backup/recovery.
Security Manager	User administration - adding SMC and other users to the SMC domain and to Tivoli. Allocating users' rights e.g. roles, groups.

Pre-defined Tivoli tasks can be used for a variety of system management tasks including Riposte administration at the Correspondence servers.

There are associated manual processes to authorise some of the actions above and to liaise with other Pathway units involved in software distribution and auto-configuration. For example:

- Team Leaders and SMC Managers can authorise software distribution.
- Only SMC Managers Can authorise creation of new Tivoli tasks.

POL00401199

- All changes distributed via Tivoli first go through the standard Configuration Management system with its associated processes for change control, testing and authorises release

In addition to the SMC technicians listed above (and operational management and engineer roles), other users have access to the Tivoli servers as follows:

Role	Functions
Pathway Auditor	Monitoring the Pathway systems; Security Event Auditors tracing security incidents in Tivoli or reported via the Tivoli event system using the Tivoli event archive database.
Pathway application support (SSC)	Support of Post offices counter applications using events collected via Tivoli.

8.3.2 System Access Controls

The SMC workstations with Data Centre connections are in a secure area on a secure LAN with floppy and CDROM drives disabled - see 8.2.1. All SMC staff using these workstations are authenticated to the SMC NT domain and use a token. Authentication results in display of a desktop which contains only those applications available to this user. SMC technicians using Tivoli also authenticate to Tivoli (though this results in use of NT authentication).

Other users of Tivoli servers such as Auditors and SSC application support staff use workstations in different NT domains.

All users of Tivoli are registered at the Tivoli server and associated with the appropriate roles, groups (and regions) to restrict their access to facilities which they are permitted to access.

The operational management and engineering roles are as for other servers at the Data Centre (see section 4), so is not included in the following table.

Role	Workst'n & Location	Where user defined; Authentic'n needed	Resources available
SMC technician, tech specialist, and team leader	NT - SMC secure area	NT and Tivoli user; NT authentication with token	Tivoli/Oracle facilities for authorised functions. (No NT/UNIX tools)
SMC team	as above	NT with token at	PO recovery

POL00401199

Role	Workst'n & Location	Where user defined; Authentic'n needed	Resources available
leader: PO key recovery		SMC; also user of KMA	application at KMS
SMC team leader: one-shot password auth.	Specific security system	NT user at specific system.	Specific application only
SMC MSS technical support	as above	as SMC technician above	Tivoli/Oracle facilities for authorised functions. Authorised NT/ UNIX tools.
SMC Security management	as above	as SMC technician above	Tivoli and OS user and role administration
Pathway Auditor- see 7.6	NT at Pathway corporate site	NT and Tivoli user; NT authentication with token	Read access to audit information via web interface- platform audit logs, Tivoli notices, Tivoli events collected for auditing
SSC application support - see 8.7	NT at P'way secure site (Bracknell)	NT and Tivoli user; NT authentication with token	Pre-authorised Tivoli tasks to extract diagnostic information from the Post Office.

8.3.3 Controls on Connections

The NT workstations and networks which are used by SMC technicians for managing the operational Pathway system are controlled as in 8.2.1. (Tivoli integrity features will also be used to protect Tivoli traffic on the link).

All software, Tivoli scripts, configuration files etc sent by Tivoli to the Post Offices are signed for integrity.

8.4 Sequent and Oracle Management

The components involved in the management of the Sequent systems at the Pathway Central sites are illustrated in figure 8-3.

POL00401199

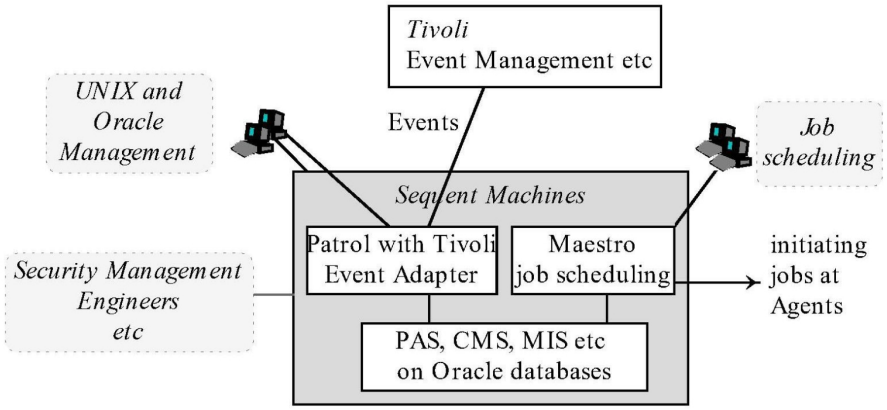


Figure 8-4 Sequent, Oracle and VME management

Patrol is used for system management of both Dynix and Oracle. Most management is automated and so does not require human intervention.

More "hands-on" operational management of the Sequent machines (including direct UNIX and Oracle access) as introduced in 4.2 above is used only when the automated management and Patrol cannot cope.

Maestro schedules jobs on both the Sequent machines and the TMS Agents (when these are not scheduled as the result of data received). The associated Maestro workstation is used for monitoring this and taking action if needed. Most job scheduling is automated and so does not require human intervention.

8.4.1 Roles and System Access Controls

System management related functions are system monitoring and management using Patrol, Sequent system/operational management and job scheduling and monitoring via Maestro. All these roles, and associated access controls, are defined in 4.2 as they affect management of the Sequent systems.

People carrying out these management functions from a remote site use secure NT or Sun workstations via encrypted links, tokens etc as defined in 8.2.1.

Access for staff on call is according to the procedures in 8.2.2 above.

POL00401199

8.5 Network Management

8.5.1 Introduction

The Pathway network routers are managed using HP Open View with Cisco Works as illustrated in figure 8-4 below.

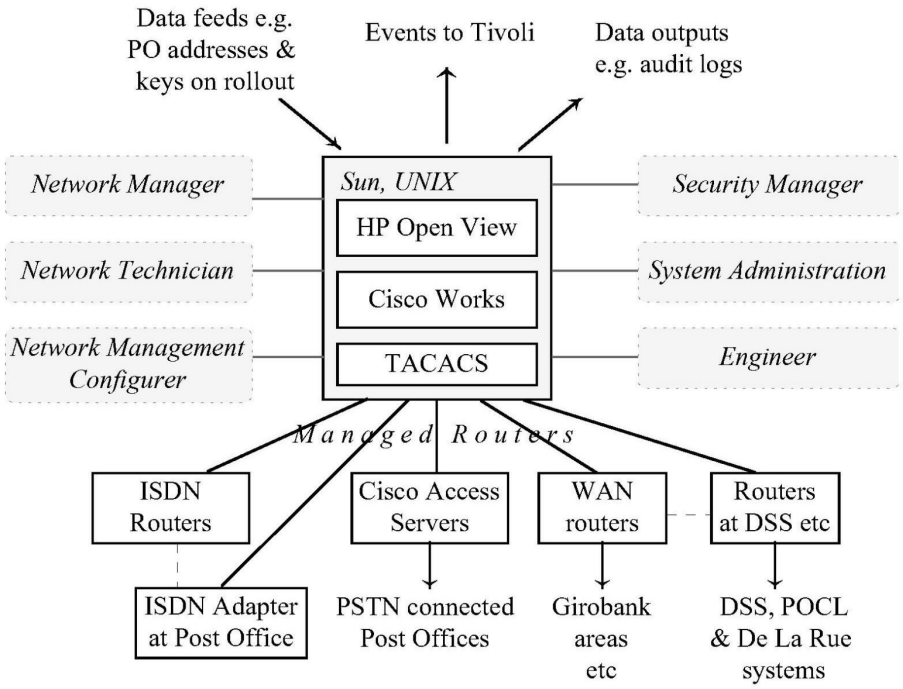


Figure 8-5 Network Management

All routers illustrated are managed using HP Open View. The solid lines show the managed routers, rather than physical connections (dotted lines show how routers outside the Data Centre are connected to it).

Some events are automatically passed on to Tivoli so that the SMC system management knows about the current state of the network. However, this is for monitoring - Tivoli is not used to cause management actions at the routers.

Audit logs are generated during normal running and provided to the audit service.

On new Post Office roll-out, the (ISDN) addresses of the Post Office to be rolled out soon are fed to the routers.

The main roles are:

POL00401199

- Network Manager responsible for configuration and management of the routers
- Network Technician monitoring the routers
- Network Management Configurer responsible for the configuration of the Network Management Station itself, such as Open View configuration. This role is carried out by the Network Management team before live running.
  The configuration will be validated by more than one CFM technician and signed off by a senior CFM person before use.
- Cisco router support.

There are no on-line application support roles. Support of Open View, Cisco Works etc is done off-line.

There is a single Network Management Station (NMS) at each Pathway Data Centre.

In exceptional circumstances, network staff can use router facilities directly via telnet, not going through Open View, and therefore not subject to its controls. In this case, the user is authenticated using TACACS on the NMS and auditing will still be carried out on the NMS - see 8.5.4 below.

Engineers may also require direct access to routers - see 8.5.5.

There are also firewall management staff - see 8.5.6 below.

Zergo encryption boxes for protecting data on links are covered in 4.6. Hardware and other support of the General Signals system to connect the Symmetrix discs to the Energis network is given in section 8.8.

8.5.2 Roles at the Open View System

The following table lists the roles of people with direct access to the Network Management Station.

Role (Organisation)	Functions
Network Technician (CFM)	Monitoring the network
Network Manager (CFM)	Monitoring the network. Updating router configuration information e.g. - Post Office information e.g. ISDN address - Access Lists of permitted addresses, protocols, ports. Updating information about routers available when needed (including confirming bringing a mended one back on line - see 8.5.5 below)

POL00401199

Role (Organisation)	Functions
Network Management Configurer (CFM)	Configuring Open View e.g. - what to display to whom - actions to be taken on certain events Configuring Tivoli Event Adapter
Security Manager (CFM)	Maintain user information for those users permitted to use this system - both UNIX users and Open View users. Local auditing of network management activities at this system
System Administration (CFM)	Any administration/configuration which cannot be done using the Open View, or Cisco Works This is expected to include operating system set up, changes; software updates.
Engineers	Diagnosing, repairing hardware faults

Note: Pathway auditors access audit information from the NMS via audit records sent through to Tivoli and extracted audit logs.

8.5.3 Access Controls associated with Human roles

People in all these roles use the console at the machine for all access to the Network Management Station. The following table shows how the users defined above access the system and what is available to them.

Role	Workstation type/location	Authenticat'n method & where user defined	Resources available
Network Technician	console at NMS	OpenView userlogon	Specified Open View and Cisco Works functions only
Network Manager	as above	UNIX & Open View as individual user	Open View and Cisco Works network management functions (no direct UNIX access)
Network Manag't Configurer	as above	as above	Open View configurer functions
Security Manager	as above	as above	User information and resource access controls
System Administration	NT at Belfast	UNIX after NMS configured to stop managing the network	All UNIX facilities

POL00401199

Role	Workstation type/location	Authenticat'n method & where user defined	Resources available
Engineer	console at NMS	UNIX via special password c.f. Sequent systems	No UNIX/Cisco works access

Notes:

1. The Network Management workstations run 24 hours a day. However, at the end of the shift, the existing user logs out and the new user logs on to give individual accountability. Other users of the system must also authenticate themselves e.g. prior to doing configurer or security management functions.
2. All users (except possibly engineers) are individually identified to the system and logon under individual user names.
3. Engineers identify themselves at the secure site and have supervised accessed to the system - see 3.6.3.

8.5.4 Telnet Access to Routers

Pathway routers are normally controlled from the Network Management Station as described above. There are exceptional cases where more direct access to the routers is permitted using telnet. The only cases permitted are:

- CFM senior network management staff accessing the routers in exceptional circumstances (for example, for fault resolution requiring use of the debug facility, in times of excessive network workload or during fault conditions)
- CISCO staff supporting the routers from a remote CISCO site

No Telnet access to routers is permitted without authorisation by a member of the Telnet authorisation list. Manual records are kept of this authorisation each time Telnet access is used.

All users of Telnet access to routers authenticate using TACACS+. All Telnet access is audited at the NMS. The audit trail contains the TACACS+ authentication entries and configuration etc changes resulting from the Telnet access.

Authorised CFM Network Managers use Telnet access to routers from a specific dedicated NT system on the Operational Bridge area of the Network Centres.

POL00401199

Cisco staff access the router needing support via a separate gateway router dedicated for Cisco use. This gateway router will be configured to permit Cisco access only when Cisco support is needed - see 8.2.2. A different TACACS username and password will be used on each occasion and these will only be valid for the particular session. The standard Cisco engineers will have read only access to the routers. Named and authorised senior CISCO staff (NSA Engineers) may have "enable" mode, as that is needed for reviewing configuration files and debugging. CISCO are not permitted to make changes to the routers (a manual, not IT control).

8.5.5 Direct Access to Routers

The only direct access permitted to routers is for engineers investigating hardware problems. In this case, access will always be done locally at the router using a console.

In normal running, the routers will not have consoles attached, though console access is enabled. Any attempt to use console access will be flagged at the NMS.

If a router has a fault, it will be configured out of the network and then a console physically taken to the router and plugged in. The router engineer can then log onto the router to diagnose and repair the fault. The router is then connected back into the system. The configuration of the router is checked and the Network Manager asked to confirm acceptance before the router is configured for normal use as part of the operational system.

The password used for direct console access is changed via the NMS every 28 days and also immediately when an engineer requires access. (There is a two level password system for console access.) Engineers are not individually known to all routers and need to ask the Network Manager for today's password. (The engineers will have identified themselves manually on entry to the secure site.)

Further details of these procedures will be in the CFM Pathway procedures manual.

8.5.6 Firewall Management

Pathway firewalls are managed using Firewall Enterprise Centres, one at each Data Centre. These reside on Solaris systems (shared with Security token management), which conform to the set-up, operating system roles and access described in 4.7.

POL00401199

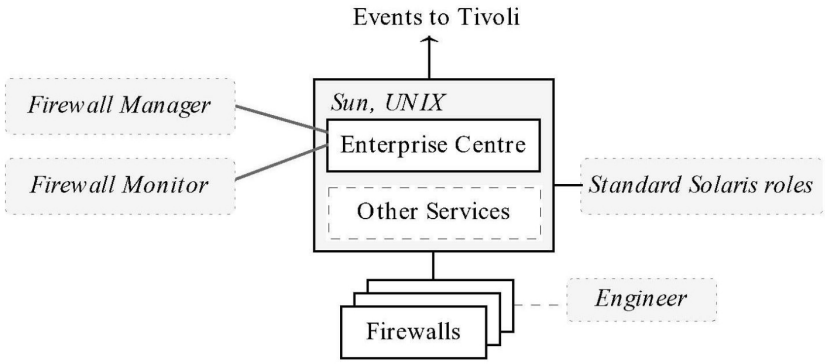


Figure 8-6 Firewall Management

All access to the firewalls is via the Enterprise Centre, except for hardware maintenance. As for routers, in normal running, firewalls do not have consoles attached - they are only attached for hardware maintenance after the firewalls has been configured out of the system. Firewall audit logs are sent to the Enterprise Centre.

All configuration changes are made via the Enterprise Centre and logged via Tivoli. There are no on-line application support roles.

People with the following roles have access to the Enterprise Centre:

Role	Main Functions
Firewall Manager	Maintains the firewall configuration and policy data
Firewall Monitor	Read access to alerts, logs and the rule base

Access controls associated with these roles are defined in the following table:

Role	Workstation type and location	Authentication method & where user defined	Resources available
Firewall Manager	Either: Controlled NT workstation at secure site, or Local UNIX console	Defined as UNIX & Enterprise centre user; Authenticated with token (to NT, and/or UNIX, depending on workstation)	See above
Firewall Monitor	As above	As above	See above

8.5.7 Access controls configured in Routers and Firewalls

Access Lists in the routers define the traffic to be permitted or denied by that router specifying IP addresses and associated IP protocols (ip, udp, tcp, icmp) and port numbers. Only traffic associated with IP addresses that are explicitly defined in Access Lists will be permitted.

POL00401199

Firewalls control the use of other application protocols also, though controls are different for different firewalls, depending on traffic permitted - see policies in 8.10 below.

8.6 Software/Configuration Distribution and Implementation

Pathway releases software and/or configuration information in two cases:

- Implementation of new Post Offices, including migration of in-office data. The Post Office counters are delivered with a standard configuration which needs to be personalised and updated when installed. This process is mainly automated and involves initial set up of IP addresses, routers and cryptographic keys. This implementation process may also be used for certain types of major changes to Post Offices.
- Release software and other configuration updates to existing Post Offices (and related systems). This covers software release to the Post Offices and to systems in other domains.

In both cases, the process includes authorising the release, digitally signing the information, distributing it, and, at the receiving system, using the digital signature to check the information is correct and from the right place.

8.6.1 Post Office Implementation

This Access Control Policy is concerned only with those parts of the implementation mechanisms which affect the operational system. These are illustrated in figure 8-6.

POL00401199

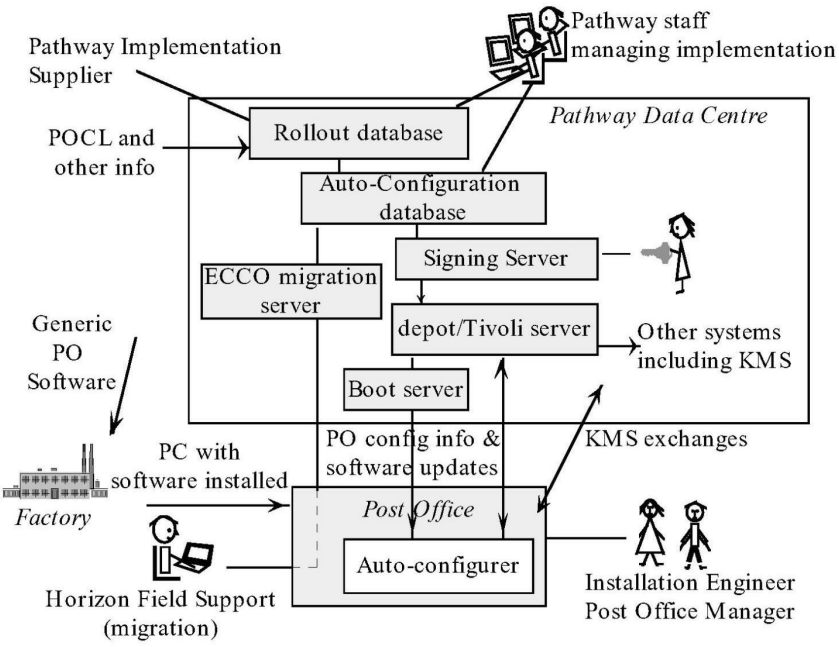


Figure 8-7 Interactions on Post Office Implementation

The information about implementation of Post Offices is managed in the Roll-out database which takes input from POCL and other sources.

Pathway suppliers can also access this database (via bulk transfers) - both to view and update information.

Information about Post Offices to be installed soon is transferred to the Pathway Auto-configuration database. The Auto-configuration initiates the Auto-configuration process which sends information to the Central Pathway services as required to handle the new Post Offices. Configuration information for each Post Office/counter is also generated. This is digitally signed by the Signing Server and sent to Tivoli to distribute.

The PCs are delivered from the factory with software, including an Auto-configurer application, installed. The installation engineer uses this to configure the PCs. During this process, changes needed to the delivered software and configuration are sent to the Post Office. For ECCO equipped Post Offices, a Horizon Field Support Officer (HFSO) handles migration of data from ECCO to the Horizon system using a laptop at the Post Office linked to a migration server at the centre. (Manual migration is also handled by HFSOs, but at the Post office only.)

POL00401199

When the Post Office Manager takes over and first boots up the Post office, the keys for standard running are delivered from the KMS.

8.6.1.1 Implementation Roles

Application roles are:

Role	Functions
Roll-out/RODB users	Implementation staff viewing information in the roll-out database (RODB)
RODB data administrators	Implementation staff as above, but also able to update RODB data, for example, change the date for a Post office installation.
Roll-out support/help desk advisors	Handle calls from Pathway suppliers and Post Offices - forwarded from Horizon system help desk. Queries and limited updates to RODB depending on call
Auto-configuration user	Implementation staff managing the data going through the auto-configuration database (ACDB). This includes some update access.
ACDB data administrator	Administering the central services site information in the ACDB
Horizon Field Support Officer	Handling migration - two roles for manual and ECCO migration
Application support manager and user	Supporting applications

In addition, there are:

- The standard NT roles defined in 4.4. These include the standard operational management roles, and auditor roles. It also includes a dba role for each application
- Key custodian and key handler roles at the signing server - see 7.7.1

System access controls for people in these roles are:

Role	Workstation type/ location	Authentication method	Resource available
RODB user	NT workstation at Pathway site or regional office (see note 1)	Token authentication to firewall, then password to SQL server	Read only access to RODB
RODB data administratio n	NT workstation at Pathway site	As above	Query and update access permitted by RODB/client
Roll-out	NT workstation	As above	Query and update

POL00401199

Role	Workstation type/ location	Authentication method	Resource available
advisors	at Pathway site		access as allowed by RODB client
Auto-config user	Controlled NT workstation at Pathway site	Token to NT workstation, and via domain trust, to Data Centre	Query access plus update as allowed by ACDB/client
ACDB data administration	NT workstation at Pathway site	As above	Query access plus update as allowed by ACDB/client
HSFO - ECCO migration	Laptop linked to Post Office system	NT log at lap top; then NT logon to migration server domain, both using password	Job to transfer ECCO data to TMS journal
Application support	Secure NT support workstation - see 8.7	Token authentication at NT workstation	Access to required files, databases

Notes:

1. RODB users at regional offices dial-in, with routers at the office connecting to the Data Centre firewalls
2. ACDB users have controlled workstations, not on the Pathway LAN, and linked by ISDN to the Data Centres
3. Once initial roll-out is complete, management of implementation of new Post Offices will switch to CFM, so workstation types and authentication methods for those roles will change to the standard CFM ones - see 8.2.1
4. The NT logon to the migration server for ECCO migration is to establish the laptop access to this server. The HSFO uses applications at the laptop only, so is not a direct interactive user of the migration server
5. Manual migration is a Post Office only role, so covered in 5

8.6.1.2 Other Access Controls

The RODB takes traffic from external locations, which do not conform to the standard secure controlled systems used for most Data Centre access. The NT server supporting the RODB is therefore firewalled from such external access, with controls at the firewall restricting traffic i.e.:

- Implementation staff in regional centres connecting to the RODB via modems will be restricted to read only SQL access to the RODB.

POL00401199

- Implementation suppliers will be restricted to (FTMS controlled) file transfers between a Pathway PC at the suppliers site at the RODB.
- ECCO migration laptops can only connent to the migration server at the Data Centre

The RODB server is also separated by firewalls from the main Data Centre systems.

8.6.2 Software Updates

This Access Control Policy is concerned with software updates (new software and fixes) after the software is available in the Configuration Management system and has been authorised for release by the CS Release Manager. This is illustrated in figure 8-7.

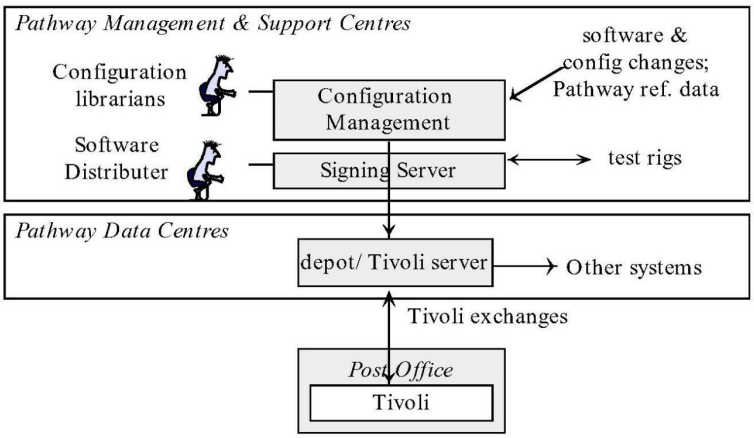


Figure 8-8 Software Release

When authorised by the Release Manager, the CM Software Distributer initiates signing and distribution of the software. It is first made available for testing, for example, at the test rigs in SSC (see 8.7). Once testing is complete, and all other checks made, the Release Manager authorises distribution of the software. The Software Distributer then initiates transfer of the software to the depot in the Data Centre for distribution to the operational system.

From the depot, the software is distributed via the appropriate route to the target system e.g. Tivoli distributes software to the Post Office.

Software distribution to the Data Centre is done by the Pathway Configuration Management unit (CM). Onward distribution from the depot/Tivoli is controlled by CFM - see other sub-sections above.

POL00401199

In exceptional circumstances, where this is not fast enough, authorised code fixes may be done directly by CFM.

All human users of the configuration management system log into it as NT users with passwords.

The usual key custodian and key handler roles are supported at the signing server. As this is part of the secure Feltham LAN, any authentication at that system is token based.

8.7 Application Support

8.7.1 Introduction

The main interactions of people involved in application support are illustrated in figure 8-8. Note: this does not cover support of network boxes such as routers (see 8.5) or the symmetrix discs (see 8.8) or support of Dynix (see 8.4)

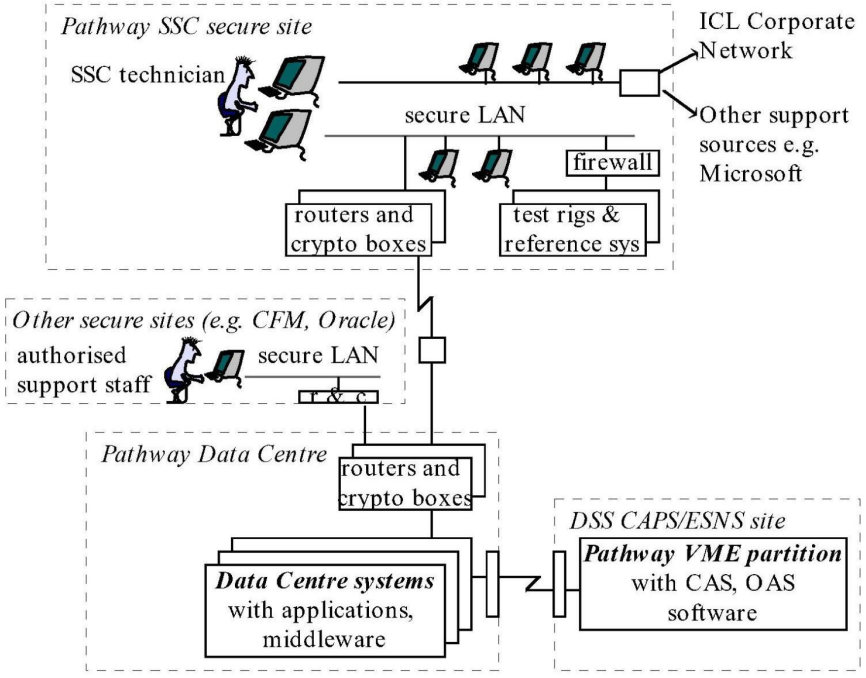


Figure 8-9 SSC and other support sites

POL00401199

SSC is the main application and package support unit supporting applications and packages on Sequent and NT systems at the Data Centre, and applications at the Post Offices. This support requires access to the relevant Data Centre systems to diagnose the problem. SSC also use test rigs to re-create problems and try out updates, before updates are included in the operational systems via the standard Configuration Management system (see 8.6).

CFM provide first line support for most systems and application support for some Sequent and all VME applications. Other units provide 3rd and/or 4th line support for particular applications and packages, though this is often off-line from the operational systems.

All application support staff with access to the Data Centre systems do so from secure sites using NT workstations on secure LANs separate from any other systems use (see also 8.2.1). All secure sites conform to Pathway requirements for physical, network and staff security.

Limited data may be downloaded from the Data Centres to the SSC test rigs for testing new software and to assist in diagnosing application problems.

SSC also assist Pathway Business Support when doing financial reconciliations - see 7.5. SSC, on request from Business Support. This also may sometimes require download to the reference system, with files of transaction adjustments sent back to the Data Centre for forwarding to CAPS.

A firewall restricts traffic between the test rigs/reference systems and the secure LAN. Permitted traffic is the file transfers described above and access from the SSC and Oracle secure LANs as required for supporting the applications.

The SSC site is connected via encrypted links to the Pathway Data Centres (indirectly via another secure site - see section [REF _Ref402000900 \n * MERGEFORMAT]).

8.7.2 Roles

Application support roles are included in the relevant sections of the ACP. There are two main application support roles (for SSC and CFM):

- Application support users diagnose problems and have read only access to the main Pathway systems
- Application support managers can also correct data under controlled conditions - see 8.7.3

POL00401199

3rd line application support roles (by other units) are always read only.

In addition, there are users of the test rigs. These do not have access to the Data Centre systems and so their system access is not covered further in the Access Control Policy. Note that as they have some access to DSS data, the test rigs, and access to them, are in a secure area on a secure LAN and staff are vetted to Pathway standards.

8.7.3 System Access Controls for these Roles

All application support users access Data Centre systems via secure NT workstations as described above. Some may need to see DSS data. Therefore all these support users should authenticate using tokens.

Much application support requires read only access to the relevant Data Centre and VME systems/package. (VME access is via Sonnet on the Sequent systems at the Data Centre). However, in some cases, update access is required.

Where update access is to code, and time permits, correction of errors is by re-issue of a new version of the software via the Configuration management system. When faster fixing is required, software updates may be made by CFM (operational management role) directly after a request by SSC, subject to agreed Pathway authorisation procedures.

In certain agreed circumstances, there is a need to correct data which has been corrupted by faulty code. Such corrections are made only by the application support manager, and are subject to agreed authorisation procedures. Where the data to be corrected is DSS data which is UK RESTRICTED, authorisation procedures include the Pathway Business Support Unit and DSS.

In all cases, updates to code or data by application support staff require two staff to be present when the change is made and all such changes to be audited, identifying what has been changed (before and after values) and the individual who made the change.

No application support users have access to Post Office counter systems - errors here are diagnosed using logs of events extracted via Tivoli.

POL00401199

8.8 Specific Hardware Support

Earlier sections of the ACP cover support of the main Pathway platforms - the NT and various UNIX systems and the routers. In addition to these, there are a number of other hardware boxes at the Data Centre. While most support will be on-site, remote support for some hardware is being considered.

Information about access controls for permitted support cases will be added in a later version of the ACP.

8.9 Horizon System Help Desks

There are two technical Help Desks:

- The Horizon system Help Desk described in this section. This is the main technical help desk. It is run by CFM and handles technical queries during normal running of the operational system. It forwards relevant queries to:
- The Roll-out Support Desk which deals with the specific issues of installing Post Offices. This is described in [REF _Ref401847521 \n * MERGEFORMAT].

8.9.1 Introduction

The Horizon System Help Desk handles technical queries from Post Offices, the Payment Card Helpline and from DSS and POCL as well as Pathway queries.

The main interactions of Help Desk staff using the IT systems is illustrated in figure 8-7

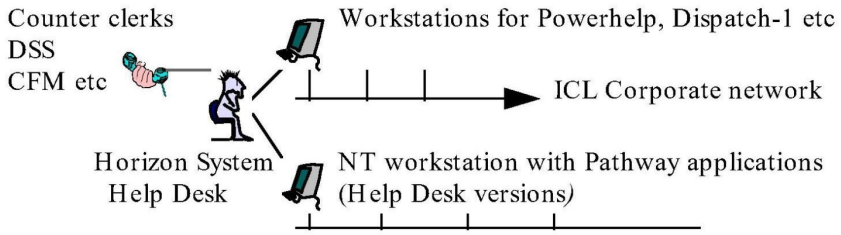


Figure 8-10 Horizon System help Desk

POL00401199

These Help Desk staff answer calls from a variety of sources and are responsible for registering calls, responding to them in some cases and passing other calls onto the appropriate unit. One workstation gives access to call handling systems such as Powerhelp, Dispatch-1 and Remote-1. Additionally, reference machines are available to Help Desk staff with a special version of Pathway applications (without live data) for use when responding to Counter Clerk queries. Note that calls from Post Office Managers about key recovery are forwarded to SMC to handle - see 8.3.

Horizon System Help Desk users do not have direct access to Pathway Operational or Management Information Systems, so details of Help Desk roles and associated access controls are not included in this ACP.

8.9.2 System Set-up

Horizon system Help Desk technicians are in a secure SMC area as for other SMC system management staff - see [REF _Ref401994263 \n * MERGEFORMAT] and [REF _Ref401994289 \n * MERGEFORMAT] above.

8.9.3 Other Access Controls

The Horizon System Help Desk receives calls on technical issues from:

- Post Office staff with a technical problem
- DSS via the ITSA Service Help Desk
- POCL offices
- Other Pathway sites

In many cases, some form of authentication is needed, as described in section 3.5.2 above.

Details of telephone authentication will be added in a future version of this document.

8.10 Network Access Controls

8.10.1 Introduction

Pathway's main systems are at the Data Centres, but there are several other sites linking into these and providing supporting services as outlined in 2.5. This section looks at the network access control policies within and between these sites, depending on the security requirements for each type of link.

POL00401199

The following diagram shows the network in outline.

Later sections look at particular parts of the network, and the specific controls needed there.

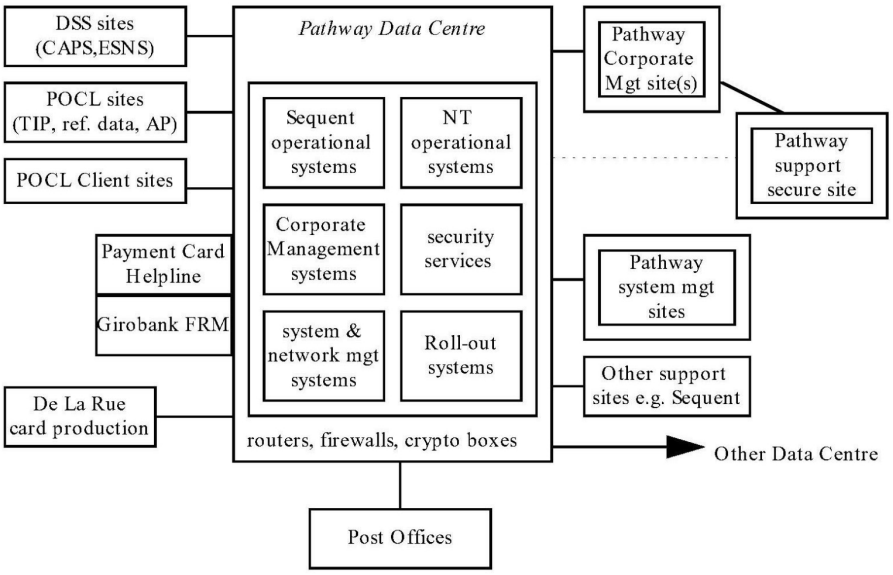


Figure 8-11 The Pathway network.

All links to the Data Centres are controlled by routers/firewalls.

8.10.2 Protecting Data in Transit

Business data is protected in transit in accordance with [SFS]. In summary:

- Business data in transit from CAPS has integrity protection and data origin authentication. On-line transactions are also encrypted. (Other traffic on this link is not protected)
- Data in transit on the POCL TIP/reference data link is integrity protected (using digital signatures).
- Data on the POCL HAPS link has confidentiality protection and also the data will be signed.
- The Payment Card Helplines and Girobank FRM systems are in Wigan and Bootle, so data in transit to them does not need encrypting.
- Details of customers for card production on route to the De La Rue card production system are integrity and confidentiality protected.

POL00401199

- Traffic to the Post Offices is protected using a VPN to provide authentication and encryption. Payment authorisations and also software and configuration updates distributed via Tivoli are digitally signed.

Other general policies for protection of links are:

8.10.2.1 All Pathway Corporate management, system management and support sites with access to the main operational systems have fixed links to the Data Centres

8.10.2.2 External sites with access to the main operational Pathway systems also have fixed links to the Pathway Data Centres.

8.10.2.3 All such fixed links are protected using Zergo encryption devices using Rambutan.

8.10.2.4 All ISDN links use VPN protection or CHAP authentication and CLI.

8.10.2.5 The Feltham site also acts as a gateway for some other sites accessing Pathway services. Where these are fixed links (as for the SSC site) the link between these sites will also be encrypted. (Note the SSC site also has a further encrypted link allowing an alternative connection to the Data Centres in the case of a failure at the Feltham site).

8.10.2.6 Where external support users, implementation suppliers etc access Pathway systems, Pathway firewalls control that access. Any exceptions to this must be agreed by the Pathway Security Manager and documented in the ACP.

8.10.3 The Data Centre Network Access Policy

The following diagram is a simplification of the network at a Pathway Data Centre showing the links into and out of it.

POL00401199

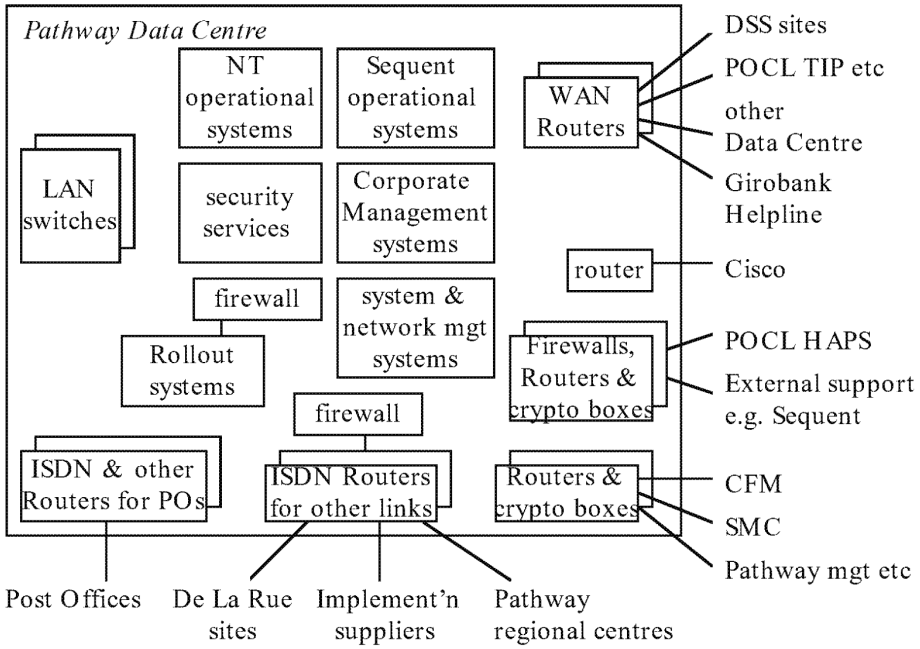


Figure 8-12 The Pathway Data Centre Network

Note that the above diagram does not show:

- The actual network within the Data Centres or the firewalls which protect specific links and systems. Rather this document gives the access policies which the network should achieve.
- The actual network outside the Data Centres such as the Energis backbone, or the ISDN network as these do not affect the access control policy.
- Some users where more information is needed e.g. DSS FIT

Traffic into and out of the Pathway Data Centres is mainly controlled by the routers and firewalls. These are also used within the network, and there are also controls on the use of ports at particular systems.

The links into the Pathway Data Centre should be configured to achieve the following.

8.10.3.1 Routers and firewalls on the links should be configured to restrict traffic as required by this policy - see 3.4.3. They should restrict traffic to the agreed external sources.

8.10.3.2 DSS and the POCL TIP/Reference Data link use a secure environment provided by the Energis ATM network. The closed user group restricts access to Pathway only.

POL00401199

8.10.3.3 Firewalls should protect the Data Centre systems from links to other services such as POCL HAPS, De La Rue and Implementation Suppliers.

8.10.3.4 Access to the Data Centre by external organisations for support or other access should also be firewalled. Any exception to this must be agreed with the Pathway Security Manager and documented in the ACP.

8.10.3.5 Roll-out systems which can be accessed from outside sites not conforming to the Pathway standards for a secure site should be firewalled from other Data Centre systems.

8.10.3.6 Traffic to/from DSS systems should be restricted to the authorised business traffic to/from the Sequent operational system (apart from network management traffic between the routers and the NMS).

8.10.3.7 Traffic to/from the POCL, POCL Client and De La Rue systems should be restricted to the authorised business traffic to the PCs handling that link (apart from network management traffic between the routers and NMS and system management traffic between the PCs and Tivoli Management Centre.

8.10.3.8 The Girobank Help Desk users should be restricted to only Oracle Forms access to Sequent (see 4.3.1 above). The Help Desk workstations should be set up to use only this access to the Data Centres and the Sequent systems to accept only this.

8.10.3.9 A set of routers should handle all traffic to/from operational Post Offices and accept traffic from outside the Data Centres only from Post Offices. No operational Post Office traffic should be accepted via other routes. These routers should also restrict where traffic can be routed to/from within the Data Centre. Permitted addresses are just for those services listed in 5.3 i.e. the Correspondence Servers, Tivoli management servers and KMS.

8.10.3.10 When implementing a new, or significantly changed, Post Office, connection will initially be to the boot server which is separated by firewalls from both external access and the main Pathway Data Centre LAN.

8.10.3.11 The routers handling POCL and De La Rue ISDN links are separate from those used for the Post Offices. Traffic permitted to and from them are file transfer, network and Tivoli management (see section 6). The routers/firewalls should restrict file transfer traffic to the PCs allocated to handle this traffic from this site and restrict Tivoli traffic to the Tivoli server.

POL00401199

8.10.3.12 Routers should be configured to deny access to external users (e.g. CISCO support) until this access has been agreed - see 8.2.2. When permitted, the appropriate router should be configured to restrict access to the Data Centre to the particular system(s) needing support.

8.10.3.13 The routers used for internal Pathway site access only permit traffic from/to these locations.

8.10.3.14 The combination of routers and firewalls at Feltham should restrict traffic from there (and linked sites) to what is permitted. For example,

- SSC application support users are restricted to the systems they support
- Management users are restricted to the Data Warehouse and MIS systems at Wigan
- Configuration management traffic is only permitted to the appropriate software depot/Tivoli server.

8.10.3.15 Controls in the Data Centre should reduce the possibility of interference between systems by separating independent parts of the system, particularly where these which have different security requirements. (This may be by a combination of network set-up, router controls, controls at ports of specific systems and NT domain structure.) For example,

- Systems concerned with roll-out of Post Offices should be separate from those used for operational running.
- Security services, such as the Key Management one, should be well protected from unauthorised access from other systems.

8.10.4 Pathway Project Sites

System management sites remote from the Data Centres which are run by ICL Outsourcing are covered in sections 8.3, 8.4 and 8.8 above. The SSC application support site is covered in 8.7 above.

Other sites are used by Pathway management and the Pathway Implementation Unit. These include:

- The main Pathway management sites at Feltham and Bracknell
- The Implementation unit main site at Kidsgrove
- Regional offices used by the Pathway Implementation Unit.

The Pathway Corporate Management site at Feltham has a permanent direct link into the Data Centres. Users of Data Centre systems from this site are:

POL00401199

- Pathway management users accessing the Data Warehouse, MIS and SLAM systems - see section 7
- Pathway Business Support users - see 7.5
- Pathway Customer Services using the RDMC - see section 4.3.2
- Pathway Security, Audit and FRM users - see section 7
- Software distribution (see 8.6)
- Implementation/roll-out users - see 8.6

The Feltham site also provides links for other Pathway project sites such as SSC (see 8.7) which require Data Centre access as shown in the following diagram.

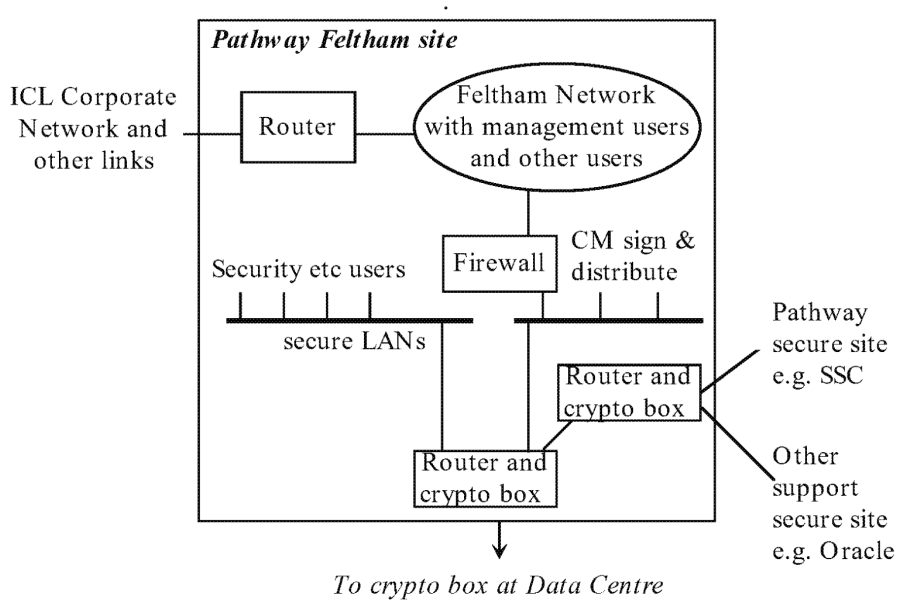


Figure 8-13 Feltham Pathway Network

The Kidsgrove site and Regional centres have simpler networks with routers and ISDN connections to the Data Centre. In the case of regional offices, access to the Data Centre is via a laptop dialling in (via local routers and then Data Centre routers and firewalls).

8.10.4.1 Workstations on a secure LAN, or individual secure workstations must be used for access to the following Data Centre services:

- Operational systems at the Data Centre, including related services such as the time server.
- Services with access to sensitive data (on MIS or other systems) or with update access to them
- Secure services on a Pathway project site such as the signing service

POL00401199

Note: this includes Security Management, Auditing and FRM users and some management users - see section 7.

8.10.4.2 Signing and distribution of software should also be from a secure LAN.

8.10.4.3 All traffic in and out of the Feltham Pathway Network should go through one of the routers/firewalls identified in diagram 8-12 i.e.

- be encrypted traffic to/from the Data Centres
- be encrypted traffic to/from another authorised secure site, or
- go through the routers/firewalls protecting the pathway network from the ICL Corporate network and external links

No access to the Feltham network by-passing these controls is permitted.

8.10.4.4 Traffic between the Pathway Feltham network and other networks (apart from the encrypted links) should be restricted to permitted traffic by the routers/firewalls at the boundary to the Pathway network. The main types of permitted traffic are:

- Links to services required by Pathway developers, managers and related staff. This includes email, Powerhelp and the financial system.
- Supply of software from other units, where this is done electronically.
- Access required by Implementation suppliers to the roll-out database.

8.10.4.5 All access to the Data Centres from the main Feltham network (rather than secure LANS), is restricted to the required application protocols to the permitted particular Data Centre services for this user. This applies to users with workstations on that network and external users such as implementation suppliers (see above). This is controlled by the configuration of the firewall between the network and the Data Centre link and associated routers.

8.11 NT Domains

Windows NT domains are used in Pathway to control which NT servers can share NT resources and which users have access to those resources. They are also used to simplify user authentication - a user need only logon once to a domain, or once to a set of domains which have an established trust relationship which includes trust in the users of the domains.

NT domains should conform to the following policies:

POL00401199

8.11.1.1 NT domains should generally have at least one Backup Domain Controller. This should be on a separate site from the Primary Domain Controller. Exceptions to this must be agreed and are expected to be small domains with few users.

8.11.1.2 Where a set of related NT systems is run by a different authority from other NT systems, this should be set up as a separate domain.

8.11.1.3 Where such a domain does not share users or resources with other domains, it should be a separate domain with no trust relationship with other domains. For example, the Payment Card Helpline systems are such a domain.

8.11.1.4 NT domains should be set up to conform to the policies in this ACP including the general ones in section 3, the NT specific ones in 4.4 (for Data Centre NT servers) and the need to reduce interference between systems in 8.10.

8.11.1.5 Domains may span sites where all NT workstations and servers in the domain are run by the same authority and are subject to the same physical and network security. (For example, the SMC system management domain spans the SMC workstations attached to a secure LAN on the secure SMC sites and the Tivoli NT servers at the Data Centre).

8.11.1.6 A domain must be confined within an area of the network which is subject to the same security policies and controls. For example, it must not include NT systems on different sides of a firewall.

8.11.1.7 Where sharing of resources, but not users, is required between domains, then the trust between domains should be restricted to sharing the agreed resources/files across the domain boundary. The resource sharing must be restricted to the minimum required for the agreed functions.

8.11.1.8 Where sharing of files is required between domains on different sides of a firewall, this should be subject to special authorisation procedures as well as the policy in 8.11.1.7.

8.11.1.9 A domain should not establish trust in users registered in a domain in a less trusted part of the network.

8.11.1.10 Users should only have access to the NT systems to which they are permitted access. The domain set up should prevent them accessing any other NT systems.

POL00401199

8.11.1.11 Users should not be registered as NT users at domains where their only access is at the application level, for example, via a remote client via an application protocol to a particular application which has its own logon.

8.11.1.12 Set up of NT domains should assist separation of systems to reduce interference between them.

0.1.1.1

POL00401199

APPENDIX A: SUMMARY OF ROLES

The following table is a summary of the roles in this document. Services accessed are listed under:

- Sequent (operational) for the main Sequent systems which support the application hosts
- NT (operational) for the main NT systems which support the main business applications on NT such as TMS and its agents and the PCs linking the Data Centres to other business sites (DSS, POCL, De la Rue etc)
- The Management systems including Data Warehouse and other MIS systems, including SLAM, FRMS. Note that this includes Sequent and NT systems
- Other systems - mainly those concerned with Post Office implementation, system and network management and security management. Note that this includes different system types including NT and Solaris ones

Role	***Services/Systems Accessed***					***ACP sections***
	Post office	***Sequent (operational)***	***NT (operational)***	***MIS***	***Others***	
POCL steady state Post Office Roles						
Post Office Manager	Post Office counters					5
Post Office Supervisor	PO counters					5
Post Office Clerk	PO counters					5
Emergency Manager	PO counters					5
POCL Auditor notes 1 & 2	PO counters					5 (7.5)
Benefit Payment Support Roles						
DSS/BA clerks		PAS/CMS via CAPS				6.1 (4.3.1)

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	*Sequent (operational)*	*NT (operational)*	*MIS*	*Others*	
DSS Help Desk		PAS/CMS via CAPS				6.1 (4.3.1)
Payment Card Helpline Advisor		PAS/CMS				7.4 (4.3.1)
Payment Card Helpline Advisor (NSI)		PAS/CMS				7.4 (4.3.1)
Payment Card Helpline Supervisor		PAS/CMS				7.4 (4.3.1)
Other Support roles used by customers						
Horizon System Help Desk Technician					local only	8.9
SMC Team Leader acting as SMC Help Desk Technician					local including one-shot password system; KMA	8.3
Roll-out Support Desk advisor					RODB (NT)	8.6
Business Operational Roles - Pathway staff						
Reference Data Change Manager		RDMC				4.3.2
RDMC Loader		RDMC				4.3.2
RDMC User		RDMC				4.3.2
RDMC access administrator		RDMC				4.3.2
Business Support Manager		PAS/CMS, TPS, APS, OBCS	TMS?		reconciliation db (NT)	7.5 (+7.9, 4.5, 4.3.1)
Business Support		as above	as above		as above	7.5 etc as

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	***Sequent (operational)***	***NT (operational)***	***MIS***	***Others***	
Analyst						above
Fraud Risk Management, Audit and Security Roles						
FRM Manager		PAS/CMS	TMS	FCMS, DW (Sequent)	For evidence gathering, others as Business Function Auditor	7.3 (+ 7.9, 4.3.1, 4.5)
FRM Analyst		as above	as above	as above	as above	as above
FRM User				FCMS, DW		7.3 (7.9)
DSS FIT				FCMS		7.3 (7.9)
Pathway Business Function Auditor		Main host systems	Main operational systems	DW and others	Auditor workstation	7.6 (+ lots)
Pathway Security Event Auditor		All systems	All systems	All systems	Most systems, including Tivoli events	7.6 (+ lots)
Pathway security management					Token Authentication Service (Solaris)	7.7 (4.6)
Cryptographic Key Manager			KMA, CAW			7.7 (4.6)
Cryptographic Key Custodian		key mgt application	key mgt on Agents, CMS link PCs		VME, Signing service (NT)	7.7 (+ several)
Cryptographic Key Handler		as above	as above		as above	7.7 (+ several)
PO key recovery (subset of SMC Team			KMA			8.3 (4.6, 7.7)

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	***Sequent (operational)***	***NT (operational)***	***MIS***	***Others***	
leader role)						
Other Pathway Management roles						
Pathway Management Support				DW (Sequent) - Business Objects and several apps, SLAM (NT)		7.8 (+7.9)
Pathway Financial mgt				CCS application		7.8 (+7.9)
Pathway Contract mgt				CON application		7.8 (+7.9)
P'way Ref. Data mgt				DW		7.8 (+7.9)
Pathway CS Managers				SLAM on NT		7.8 (+7.9)
Pathway Business Dev.				DW		7.8 (+7.9)
Implementation and Software/Configuration Distribution Roles (apart from help desks above)						
Auto-configuration user					ACDB	8.6
ACDB data adminstrator					ACDB	8.6
Roll-out/RODB user					RODB	8.6
RODB data administrator					RODB	8.6
HFSO - ECCO migration	laptop at PO				Migration server	5, 8.6
HFSO - manual migration	PO counter					5
Software Distributer					CM signing service	8.6
Pathway operational management/ administration						

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	***Sequent (operational)***	***NT (operational)***	***MIS***	***Others***	
Computer operator (on Sequent systems)		UNIX/secure menu	NT	All systems	All systems	4.2, 4.4, 4.7 (+ others)
Senior operator		UNIX/secure menu		UNIX/secure menu		4.2
System Monitoring		Patrol		Patrol on Sequent; NT		4.2
Database monitoring		UNIX/secure menu		UNIX/secure menu		4.2
Operational mgt/ system administration		UNIX/secure menu	NT	UNIX/secure menu	All systems (NT, Solaris etc)	4.2, 4.4, 4.7 (+ others)
Operational mgt/ database administration		UNIX/secure menu; Oracle applications		UNIX/secure menu	RODB, ACDB (SQL server)	4.2, 8.6
Secure menu administrator		UNIX/secure menu		UNIX/secure menu		4.2
Security Management		UNIX/secure menu	NT	UNIX/secure menu	All systems	4.2, 4.4, 4.7 (+ others)
Legato Administration			Archive server			4.5.1
Payment Card Helpline Security Manager		PAS/CMS				7.4
Base Installation and configuration		UNIX	NT	UNIX	All systems	4.2
Riposte Management			Correspondence servers			4.5

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	*Sequent (operational)*	*NT (operational)*	*MIS*	*Others*	
KMA Data Manager					KMA	4.6
Pathway systems management, administration for CFM (DS) systems						
SMC technician					Tivoli/Oracle system management services	8.3
SMC technical Team Leader					Tivoli/Oracle system management services	8.3
SMC MSS technical support					Tivoli/Oracle SMS plus SMS OS etc	8.3
SMC security manager					Tivoli/Oracle SMS plus SMS OS etc	8.3
Pathway Network and Firewall Management and management of Network systems						
Network technician					OpenView on NMS	8.5
Network manager					OpenView and NMS (+ telnet to routers)	8.5
Network management configurer					NMS	8.5
NMS security manager					NMS	8.5
NMS system administrator					NMS	8.5
Firewall Manager					Enterprise Centre	8.5.6
Firewall Monitor					Enterpise Centre	8.5.6
Support roles						
Engineers		UNIX	NT	UNIX, NT	NT, Solaris	4.2, 4,4, 4,7
PO Installation Engineer	PO counters					5

POL00401199

Role	*Services/Systems Accessed*					*ACP sections*
	Post office	***Sequent (operational)***	***NT (operational)***	***MIS***	***Others***	
PO support engineer	PO counters					5
Dynix 3rd line support		UNIX/secure menu		UNIX/secure menu		4.2
Oracle db 3rd line support		UNIX/secure menu		UNIX/secure menu		4.2
Oracle application 3rd line support		UNIX/secure menu; Oracle application				4.2
Application support manger		UNIX/secure menu; applications	NT	UNIX, NT	many	8.7 (+4.2, 4.4...
Application support user		UNIX/secure menu; applications	NT	UNIX, NT	many	8.7 (+4.2, 4.4....
VME application support		UNIX/secure menu + VME				4.2, 6.1
Support Roles - non Pathway staff						
Oracle application and db support		UNIX/secure menu + Oracle		UNIX/secure menu + Oracle		4.2, 8.7
Sequent support		UNIX/secure menu		UNIX/secure menu		4.2
Cisco router support					routers	8.5.4

Notes:

- External Auditors only have direct on-line access to the Post offices. They have indirect access to other Audit information via Pathway Auditors - see 7.6. The table above only covers direct users of the system, so indirect access from DSS, POCL and NAO auditors is not shown.

POL00401199

- POCL Investigators have the same rights as POCL Auditors, so are not distinguished from Auditors for access controls.