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:	DSS POCL Pathway Pathway library
Document Status:	Issued subject to internal Pathway baselining
Document Predecessor:	-
Associated Documents:	See section 0.2
Author:	Belinda Fairthorne
Approval Authority:	Martyn Bennett Director Quality and Risk Management
Signatures/Dates:	
Comments To:	Author, copy to Martyn Bennett and Barry Procter
Comments By:	-

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 including Horizon System Help Desk instead of SIS Help Desk, SSC instead of EDSC, updated names for roles at Post Offices. Major items which have not yet been agreed have been moved to changes forecast and related incomplete text removed from the body of the document. This includes external auditors to access Data Centre Services. Major updates to the Post Office section have been made. An outline proposal for telephone authentication has been added. Numerous minor changes have been made.

0.2 Associated Documents

Ref:	Title	Identifier	Vers.	Date
SADD	Service Architecture Design Document	CR/FSP/004	2	27/9/96
TED	Technical Environment Description	TD/ARC/0001	2.0	14/12/96
SPOL	ICL Pathway Security Policy	PS/POL/0002	3.0	8/10/96
SFS	Security Functional Specification	RS/FSP/0001	2	11/11/96
HDM	Help Desk Call Enquiry Matrix	CS/FSP/0001	2.0	16/9/96
AUDT	Audit Trail	CR/FSP/006	1.1	8/10/96
FRMS	Fraud Risk Management Service Design	RS/SPE/0001	1.2	20/9/96
APOL	Pathway Audit Policy	RS/POL/004	0.4	4/3/97
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		
CONT	Pathway Contingency Invocation			26/11/96

FUJ00117497

0.3 Abbreviations

ACP	Access Control Policy
BA	Benefits Agency
BES	Benefit Encashment Service
BPS	Benefit Payment Service
CA	Certification Authority
CAPS	Customer Accounting and Payments System
CAS	CAPS Access Service
CESG	Communications-Electronic Security Group
CFM	Computer Facilities Management
CLI	Calling Line Identification
CMS	Card Management Service
DBA	Database Administrator
DSA	Digital Signature Algorithm
DSD	Distributed System Division (ex Sorbus, now CFM)
DSS	Department of Social Security
EPOSS	Electronic Point Of Sale Service
ESNS	Electronic Stop Notice System
FRM	Fraud and Risk Management
ISDN	Integrated Services Digital Network
IT	Information Technology
KEK	Key Encryption Key
KMS	Key Management System
LAN	Local Area Network
MIS	Management Information Services
NAO	National Audit Office
NSI	National Sensitive Indicator
NT	New Technology (Microsoft's operating system)
OBCS	Order Book Control Service
OAS	OBCS Access 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
TIP	Transaction Information Processing
TME	Tivoli Management Environment
TMS	Transaction Management Service
VME	Virtual Machine Environment

0.4 Changes Forecast

In some areas of Pathway, design is not yet finalised. While this document states the policy in these areas, details are subject to change as indicated in the relevant section. The main such areas are:

- Telephone authentication procedures (section 3.6.2 and elsewhere)
- Firewalls and associated network controls
- Use of a secure menu system on Sequent
- Use of security tokens for authentication of selected users
- Some aspects of Pathway system auditing
- Split of responsibility, particularly at DSS sites

Some additions are expected in future versions of this document. Several of these are dependent on requirements, and the way of satisfying them, being agreed. These are:

- Access to PAS/CMS and TMS archives.
- Access by POCL, DSS/BA and NAO auditors to central Pathway systems such as Correspondence Servers, PAS/CMS and System Management information.
- Other DSS access to Pathway systems for information associated with BPS. Several types of access are under discussion, but details have still to be agreed for some of these. DSS access to Pathway is expected to include:
    - Benefits agencies on-line access via CAPS to PAS/CMS. Transactions here include updates e.g. for urgent payments.
    - DSS Help Desk read only access to PAS/CMS.
    - Fraud Investigation Team access.
- NT failsafe startup may be added at Post Offices to allow regression to an earlier version on NT or Tivoli if the latest one downloaded to the Post Office fails to boot correctly. If so, this will affect the boot sequence described in 8.6.

0.5 Table Of Contents

1. INTRODUCTION

1.1 Purpose

This Access Control Policy (ACP) defines the policy for controlling access to resources in the operational ICL Pathway 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 how the security functionality described in the Security Functional Specification (SFS) will be used to enforce the required controls in the Pathway environment defined in the Technical Environment Description (TED).

1.2 Context

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

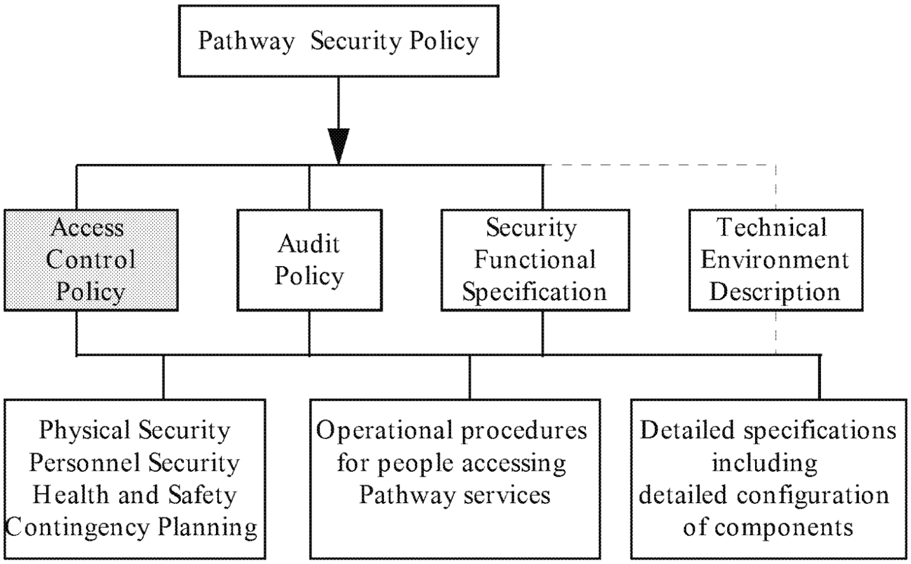
Pathway Security Policy
Access Control Policy
Audit Policy
Security Functional Specification
Technical Environment Description
Physical Security
Personnel Security
Health and Safety
Contingency Planning
Operational procedures for people accessing Pathway services
Detailed specifications including detailed configuration of components

Figure 1 - 1 Pathway's Security Documents

The Access Control Policy defines how access will be controlled throughout the Pathway system in compliance with the Pathway Security Policy. This uses security functionality in the Pathway environment.

The Audit Policy defines the policy for auditing activity on the operational Pathway system.

The Security Functional Specification describes how the security functionality will be implemented.

The Technical Environment Description describes the technical environment for the Pathway solution.

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, any 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 (such as files, databases, fields, objects) will be controlled in the operational Pathway system.

The document includes:

- 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] will be used to achieve that. For example, how people in different roles are authenticated, how access to the permitted functions will be 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.

- How the system will be set up on installation to protect the main applications which are triggered automatically.

Separate Pathway documents as described in 1.2 above define related standards and procedures.

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.

This policy is for the operational Pathway system and the associated management systems at the Pathway Data Centre. Separate internal Pathway documents cover the controls associated with system development, integration and other activities prior to the handing over of the software for use in the operational system.

1.4 Access Control Policy Review

Once approved, this document will be formally reviewed at least annually. It will also be reviewed where relevant after a significant attack or occurrence of fraud, 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

This document includes general policies and controls for controlling access in the Pathway IT systems and then the more specific controls for particular parts of the system. To assists this, the Pathway system is split into a number of security domains.

Section 2 identifies the Security Domains of the Pathway system and outlines the main functions in each domain. The domains include both the main operational processes and the management ones. This section also identifies the internal Pathway systems which have access to the Pathway Data Centres, for example, for feeding new software into the system. In addition, it identifies the sites which access the Data Centres both for management and support of the operational Pathway system and to support the feeds in and out of the system.

Section 3 specifies the Pathway wide access control policy. It outlines the main responsibilities of the Pathway organisations who have direct access to the IT system. It defines the generic roles which will be supported at most of the Pathway systems (though specific roles may have different details at different nodes). It also gives the general policies and controls which apply to all Pathway systems. Detailed configuration of any Pathway node should conform to this section and to the more specific controls in the appropriate later section.

Sections 4 to 11 specify the access control policy for each Domain in turn. For each domain (and sometimes for sub-domains) it gives a general description of the services in the domain to identify to what the access controls apply. It then identifies the roles and the access controls for that domain.

For each domain, the roles defined cover operational, management and support roles. Note that some roles are system wide (particularly system management and Pathway corporate ones) so will be referred to in each domain in which they occur (as the systems there must be configured to support them) but the full definition of these roles is in either the System Management or Pathway 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 domain.

So the access controls for a particular system are:

- The general controls in section 3 (those which apply to that type of system)
- The specific controls associated with the particular system (as defined in the appropriate later section)
- The controls referred to from that section as applicable to it.

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 services it provides,
- the components it uses to provide those services (such as VME, Dynix, NT, Oracle, Tivoli), and
- the organisation(s) responsible for providing the services (e.g. ICL Pathway, Girobank, ICL DSD).

Domains may be geographically distributed.

The services offered by several domains combine to provide the end-to-end services defined in the ICL Pathway Functional Specification, such as the Pathway Benefit Payment Service (BPS).

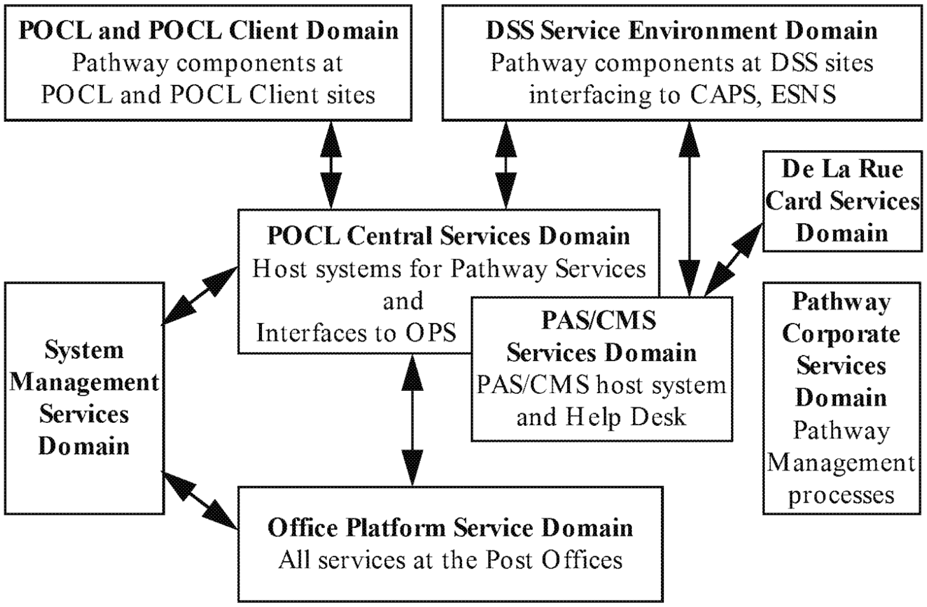
POCL and POCL Client Domain
Pathway components at
POCL and POCL Client sites
DSS Service Environment Domain
Pathway components at DSS sites
interfacing to CAPS, ESNS
De La Rue
Card Services
Domain
POCL Central Services Domain
Host systems for Pathway Services
and
Interfaces to OPS
PAS/CMS
Services Domain
PAS/CMS host system
and Help Desk
Pathway
Corporate
Services
Domain
Pathway
Management
processes
System
Management
Services
Domain
Office Platform Service Domain
All services at the Post Offices

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.

The particular machines and network connections used, and the aspects of the Access Control Policy associated with these, are covered in the more detailed domain information in later chapters of this document, particularly the Systems Management domain where the responsibility for Network Management lies.

2.2 Specifying Domain Access Control Policies

These domains represent major areas of responsibility for services within Pathway. Each has different characteristics which affect the type of access controls needed in that domain. The Access Control Policy, therefore, specifies the access controls needed in each of these domains in turn.

For each domain, the Access Control Policy includes:

- An introduction to the main services provided by the domain - including the information processed and the interfaces with other domains. This outlines the software and hardware components used to provide these services.
- An outline of the operational, management and support roles of all people with access to services in this domains and what services are provided without human involvement.
- For each role, a description of the main classes of functions and the organisation to which people with this role belong.
- The access controls in the information system for people in each role. This includes where these users are located (the workstation type as well as physical location), how they are authenticated and what resources they can access.
- 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.

Some aspects of the Access Control Policy apply to all domains and these are described in section 3, before the domain specific controls.

2.3 Domains Directly involved in Benefits Payments

The main operational flow of the Benefit Payments Service involves the domains illustrated in figure 2-2. These domains, and the others are described in the following sub-sections.

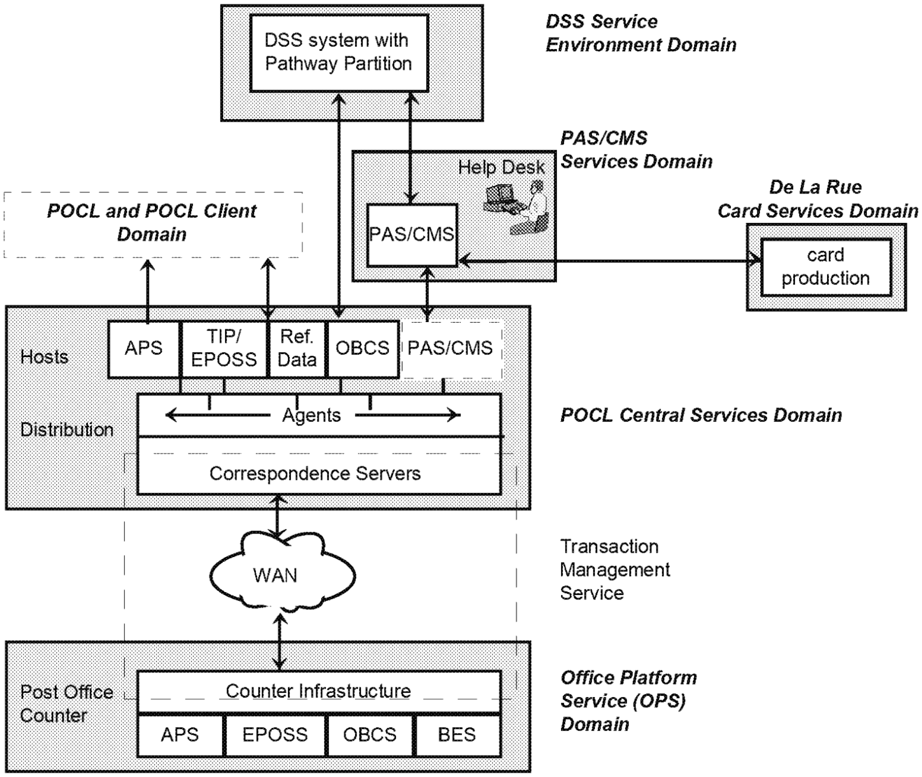
DSS system with Pathway Partition
DSS Service Environment Domain
PAS/CMS Services Domain
Help Desk
PAS/CMS
De La Rue Card Services Domain
card production
POCL and POCL Client Domain
Hosts
APS
TIP/ EPOSS
Ref. Data
OBCS
PAS/CMS
Distribution
Agents
Correspondence Servers
POCL Central Services Domain
WAN
Transaction Management Service
Post Office Counter
Counter Infrastructure
APS
EPOSS
OBCS
BES
Office Platform Service (OPS) Domain

Figure 2 - 2 Domains directly involved in Benefit Payments

2.3.1 The DSS Service Environment Domain

The DSS Service Environment Domain is illustrated in the first box of figure 2.2. It consists of the Pathway components at the DSS/BA sites.

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 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

Pathway also provides links to POCL and POCL Clients systems (other than the DSS ones above). The POCL TIP system receives records of all transactions at Post Offices and the associated POCL system provides reference data for the applications and shares the TIP link to Pathway. The POCL Automated Payments system processes Automated Payments on behalf of POCL Clients. This will be replaced in future by direct links to POCL Client systems.

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 POCL 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) except the PAS/CMS services, which merit a separate domain. All these run on Sequent machines and use Oracle databases.

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

Interfaces with other domains are shown in the third box in figure 2-2.

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

2.3.4 The PAS/CMS Services Domain

Files are transferred to/from the DSS Service Environment Domain to the Payment Authorisation Service (PAS) and Card Management Service (CMS). These process the payment authorisations and customer information for forward transmission to the Post Office or Card Producer as required. PAS and CMS share the same Oracle database running on Sequent hardware with the Dynix operating system.

The PAS and CMS Help Desks use Windows NT workstations with Oracle Forms applications to access the PAS/CMS database.

2.3.5 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).

2.3.6 De La Rue Card Services Domain

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

2.4 Other Domains

2.4.1 System Management Service Domain

The System Management Service Domain contains the central elements of the System and Network Management facilities for managing components in the other domains. It therefore covers:

- Software Distribution and associated software inventory management
- Event management
- Resource management
- Network management
- Hardware inventory management supporting software distribution 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.

The Horizon System Help Desk provides technical assistance on hardware, software and network problems, calling on others when needed.

2.4.2 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.

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

2.5 Post Office Roll-out

Rolling out new Post Office systems affects several domains. The Access Control Policy is concerned with those aspects where access is required to the operational Pathway System. The Roll-out and auto-configurer systems generate information for the Data Centres and Post Offices to configure the systems for new Post Offices. Rollout is described in the section on the System Management Domain.

2.6 Internal Pathway Services

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

- The Configuration Management system controlling information about software components for Pathway products prior to their distribution
- The Rollout database containing information about Post Offices to be rolled out
- The Powerhelp system used to record and maintain information about calls to the technical Help Desks and their progress
- The Dispatch-1 system which holds hardware inventory information

2.7 Sites linked to Pathway Data Centre Campuses

Figure 2-3 shows the sites which have electronic links with the Pathway Data Centre campuses.

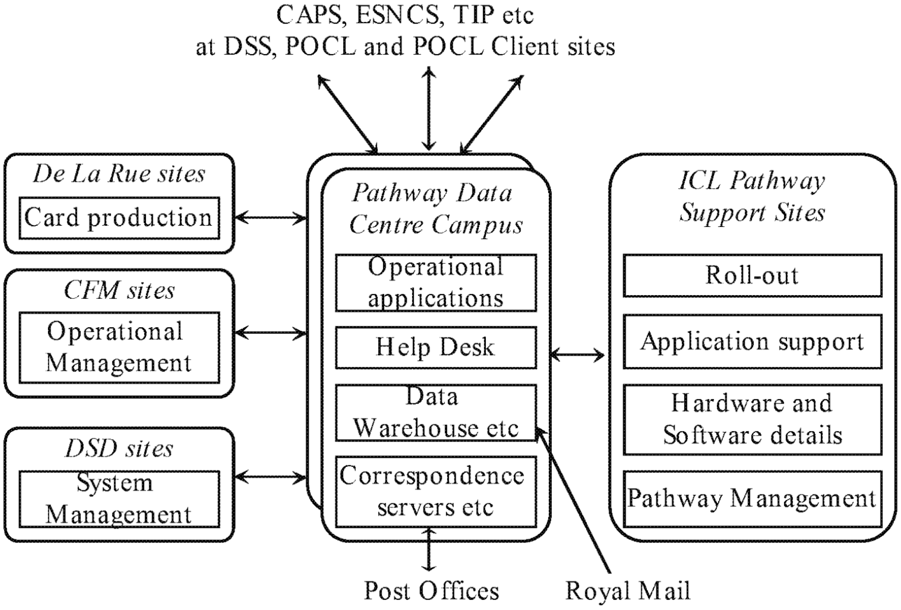

Figure 2-3 Sites with links to the Pathway Data Centres

The Pathway Data Centres are secure sites at Bootle and Wigan housing the main operational systems. The PAS/CMS Help Desks are in a separate area at each Pathway campus. The Pathway Management Information Systems are at Wigan.

All electronic interactions with DSS, POCL and POCL Client sites are via file transfers (at least initially - DSS interactive access is expected in future). Interactions with De La Rue sites are also by file transfers.

Interactions with the Post Office include the main data transferred via the Riposte TMS, System management interactions (software distribution, Tivoli scripts, events) and key management interactions.

CFM provide operational management of all the systems at the Pathway campus except the Girobank Help Desk Systems. This includes operational management of the Sequent systems and so requires privileged access to these systems. While some CFM staff will be at the campus, much of this management is done remotely (from Belfast).

DSD staff responsible for System Management and the Horizon System Help Desks are located at Stevenage, Footscray and Lytham St Annes. SMC are responsible for system management - software distribution, event handling, resources monitoring via Tivoli. DSD also provide the Powerhelp call handling system and Dispatch-1 hardware inventory.

ICL Pathway support and management sites also have access to the Pathway campus. These provide, for example, the link with the Pathway Configuration and Rollout systems from which software and Post office information is distributed. It is also used for some application support and Pathway management access. There are links from Feltham and the Oracle Bracknell site. Some application support is also done from other sites such as the CFM ones.

All links to De La Rue, CFM, DSD and other ICL Pathway sites are encrypted for integrity and confidentiality.

In addition to these electronic links, some contact with Pathway sites are made by telephone e.g. Counter Clerks phoning a Help Desk.

Later sections give define the permitted accesses between these sites.

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 11 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 Responsibilities for Services

ICL Pathway has overall responsibility for the design, implementation, roll-out and operation of the service throughout the contract period. This document is concerned with the responsibilities for accessing Pathway services during the (roll-out and) operation of the system.

Specific activities will be subcontracted to appropriate organisations both within the ICL group of companies and to other organisations. Figure 3-1 illustrates the responsibilities of these organisations in the operational use of the system.

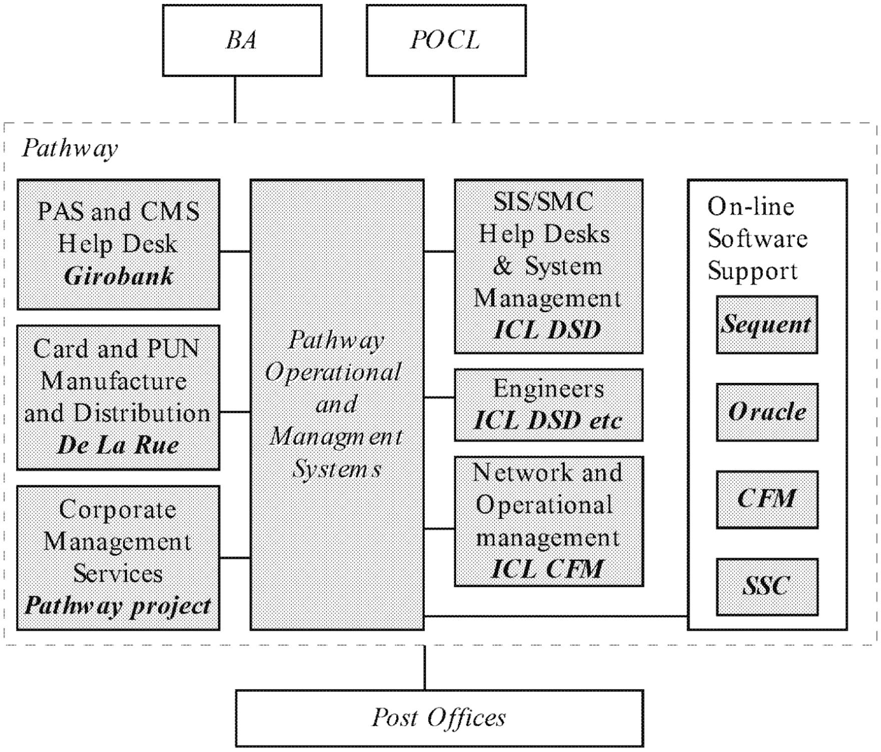
BA
POCL
Pathway
PAS and CMS Help Desk **Girobank**
Card and PUN Manufacture and Distribution **De La Rue**
Corporate Management Services **Pathway project**
Pathway Operational and Managm ent Systems
SIS/SMC Help Desks & System Management **ICL DSD**
Engineers **ICL DSD etc**
Network and Operational management **ICL CFM**
On-line Software Support
Sequent
Oracle
CFM
SSC
Post Offices

Figure 3-1 Pathway Responsibilities

The Pathway Access Control Policy covers control of access to resources in the Pathway operational systems by all these people.

The policy also covers access to Pathway services by other organisations - particularly Post Office staff accessing the Post Office systems. Other external access is also expected, for example, by POCL auditors.

The organisations involved in the operation of Pathway, and their responsibilities are described below.

- **Girobank** will run the PAS and CMS Help Desk.
- **De La Rue** will manufacture cards and distribute cards and Pick up Notices (PUNs).
- The ICL **Pathway project** will run the Corporate Management services, providing access to BA and/or POCL according to agreements. Pathway Management, including Auditing and Fraud and Risk Management, uses information from many Pathway systems.
- **ICL DSD (ex Sorbus, now CFM)** will run the Horizon System Help Desk and also be responsible for the overall System Management of the Pathway information systems. This includes software distribution, event and resource monitoring.
- **ICL DSD** provide engineers for maintenance of the central Pathway services and for maintenance of equipment at Post Offices. Engineers for other places such as the Girobank Help Desk are from other organisations.
- **ICL CFM** will be responsible for the operational management of the Sequent systems at the Pathway campuses. Their responsibility includes the Dynix operating system and Oracle databases. CFM is also responsible for Network Management.
- Under exceptional circumstances, DSD and CFM will need on-line support from other organisations for software in the Pathway system. This will be provided as follows:
    - **SSC**, the Pathway System Support Centre, will provide 2nd line support for most applications and packages including Riposte.
    - **Sequent** will support the Dynix operating system. Any on-line access will be at the Pathway Data Centre.
    - **Oracle** will support Oracle databases and provide 3rd line support for the PAS/CMS applications.
    - **CFM** will support applications in the Pathway partition on VME CAPS and ESNS machines and Business Objects applications at the Data Warehouse. (Enterprise systems also support applications on VME)

  No other organisations will have on-line access to the system. For example, there will be no on-line access by Microsoft for NT support or by Escher for Riposte support.
- **EDS** runs the DSS CAPS system and the firewall between it and the Pathway systems
- **Exel** will provide Engineers for Post Office rollout.
- **Girobank** also perform Fraud Risk management functions
- **EMC** provide the Symmetrix discs and may be called in to support these.

3.3 Pathway Roles

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

- **Operational roles** of the users of the system during normal running. These include, for example, the PAS/CMS Help Desk 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

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 will be 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.

3.3.1 Common Operational Functions

Much of the operation of Pathway applications is automated at DSS/BA, POCL and Pathway campuses, including the transfer of data to/from 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. The operational roles at the Post Office are 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.

The only operational function common to all domains is the computer operator. However, 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 the system management roles.

Control of access to resources for automated processes results from the way the system was installed and configured.

3.3.2 Common System Management Functions

System management functions are required in all domains. However some system management functions are done at the separate System Management Domain and are often 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**: setting up the base and application software on the system.

- **System Installation**: configuring the system for live running. This may be done as part of system set-up. Installation of some systems will include installing the cryptographic keys needed - see security management roles.

- **Software Update**: updating the software and reconfiguring it. Most updates to software are done automatically. 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).

- **Operational Management**: keeping the system running - responding to incidents, keeping it correctly configured. This is mainly concerned with operating system management, but may also involve some database administration

- **Package Resource Administration:** Pathway uses a number of packages to handle resources. The key packages and functions associated with them are:
  - **Oracle Database Administration.** This is separated into:
    - database structure set up and maintenance (with no access to application data)
    - full facilities (which include allowing access to all data)
    NB user management and defining which data is available to which roles in Pathway is a separate security management function - see later.
  - **Riposte Administration.** Management of Riposte message stores and groups is largely done automatically. Some residual administration may be required
  - **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 10 for more about Tivoli.

- **Application and Package Management and Support**: Managing the running of the applications themselves including handling application errors.

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

- **Network Management**: managing the network which connects machines and domains together.

- **Implementation management:** managing the roll out of the Pathway solution to Post Offices. (The Access Control Policy is concerned with that part of the roll out process which affects the operational system).

3.3.3 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, will be defined as part of the responsibilities for that role. Security management functions are:

- **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 when 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.

- **Security Auditing**: analysing and reporting on the audit logs in the system. There may be local auditing functions in some areas as well as the Pathway wide function.

- **Cryptographic Key Handling**: Keys are used to protect communications links, digitally sign information and encrypt filestore. There will be:
  - A **Pathway Cryptographic Keys Manager**: Responsible for all cryptographic keys used in Pathway, generating and distributing keys using the Key Management System.
    The Pathway Cryptographic Keys Manager will delegate some responsibility to:
  - A **Pathway Cryptographic Key Custodian**: Responsible for installation and later update of such keys at Pathway and linked systems, except where this is done automatically.

3.3.4 Common Support Functions

Support functions are primarily concerned with:

- Keeping all equipment operational, and
- Training staff to carry out their defined roles

On-line training is provided at Post Offices and PAS/CMS Help Desks.

Functions associated with keeping the equipment operational are:

- Running diagnostic applications to check for equipment faults (may be done by the Post Office Manager, as well as engineers, at the Post Office)
- Installing new Post Offices; done **Installation Engineers**
- Replacing and reconfiguring hardware; done by **Support Engineers**
- Technical Help Desks for reporting, and getting advice on, problems

3.3.5 Pathway Wide Functions

People in a small number of roles have access to several of the domains. These are:

- **Pathway Fraud and Risk Manager** (FRM). This is concerned with the identification, monitoring and management of fraud particularly in benefit payments.
  While much of this is done in the Pathway Corporate Services Domain, FRM staff also have access to operational Pathway systems such as the TMS journals and PAS/CMS data.

- **Pathway Security Manager.** This function includes the **Pathway Security Auditors** who are responsible for auditing all use of the Pathway systems. The Security Manager is also responsible for ensuring provision of personal data in accordance with the Data Protection Act.

  The Security Auditor will require access to most of the Pathway systems under some circumstances. However, the TMS will provide sufficient records at the Pathway central site for it to be unnecessary to provide Pathway access to the Post Offices.

These Pathway Management roles are described further in section 11 on the Pathway Corporate Services Domain.

3.3.6 External Roles

In addition to the Pathway roles defined above, some access to the system is required by people in POCL and DSS/BA. For example, a local Benefits Office may authorise use of a temporary token for a claimant to obtain benefits. Post Office customers receive benefits. These roles represent indirect users of the system, who contact direct users to perform actions on their behalf. They are operational roles and are therefore described with the other operational roles for particular domains.

Also, some external users are expected to have direct access to the Pathway system. The only external roles included by this version of the Access Control Policy are POCL Auditors. POCL Auditors can access services at Post Offices and are also expected to have limited access to information in other domains such as PAS/CMS archives and TMS journals. Details of this access have still to be agreed, so are subject to change.

The Audit Trail functional requirements specification [AUDT] identifies Auditors in DSS and possibly the National Audit Office (as well as POCL) who may require access to Pathway systems, but the type of access needed for these is not yet clear enough yet to include here.

There may be other external roles in future.

3.4 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. PAS/CMS Help Desk procedures, Post Office procedures
- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc.
- Security information about users, keys, security audit logs etc

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

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

3.4.1.1 All business data will be classified as RESTRICTED according to the UK government classifications. Access to data with a National Sensitivity Indicator will be further limited to authorised staff.

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

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

3.4.1.4 Digital signatures are used for integrity protection of business information between services where required. For example, information about authorised payments sent from Pathway to the Post Office is signed for integrity. Automated Payments details are signed at the Post Office prior to transmission via Pathway to POCL or POCL Clients.

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

3.4.1.6 Business information in filestore at the Post Office PCs is encrypted.

3.4.1.7 Information in Oracle databases is accessible only via authorised Oracle Forms except where there is a proven need for lower level access. Information accessed via Oracle facilities such as Oracle Forms will be subject to Oracle role based access controls.
Lower level access will only be granted for agreed operational management functions.

3.4.1.8 System Management actions by Tivoli will be activated using pre-defined Tivoli scripts which have been authorised for use by SMC and the Pathway configuration management and software distribution process.

3.4.1.9 Information on discs and other media (including printed output) will not be accessible for unauthorised use. For example, archives will be stored securely and information on discs removed for repair will not be accessible.

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

3.5 Information System Controls

3.5.1 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 will be automatically associated with a user when the user logs on. At other locations, the user will be given limited privileges on log-on and will have to ask for others, though will still be restricted to privileges for which he has been authorised. (This particularly applies to some management functions. For example, no users will be allowed to log onto UNIX with root access.)

- 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 will be 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:

3.5.1.1 Each user will be given the least privilege required for the job.

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

3.5.1.3 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.)

For system management users, a further separation of duties will be achieved using Tivoli regions to control which Tivoli region of Post Offices a particular individual manages for functions within his role.

3.5.2 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 Pathway systems will be 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 Pathway nodes will be 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 11 below. No other variants are permitted.

3.5.2.1 Workstations from which operational systems can be updated will have floppy drives disabled. Servers should should have floppy drives disabled unless there is a agreed need for them.

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

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

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

3.5.2.5 People accessing Pathway systems will be required to identify themselves using hand held tokens if:

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

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

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

3.5.2.8 Passwords will expire in one month unless otherwise stated (in the section on the appropriate domain).

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

3.5.2.10 The minimum password length will be 6 characters.

3.5.2.11 After 3 consecutive unsuccessful attempts to log-on, the user will be locked out unless otherwise stated.

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

- If accessing the system via a package such as Oracle or Tivoli, they will be 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.)

3.5.2.13 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. Any change to use another username will be controlled (as specified in that section) and audited in a way which will always be recorded.

3.5.2.14 The filestore will be structured to prevent interference between users and between applications.

3.5.2.15 Access to shared resources such as filestore will be 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
- 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).

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

3.5.2.17 Security audit logs will be protected from everyone except those permitted to take specified security 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.

3.5.2.18 Interference between applications will be prevented. For example, at any one system, different applications will 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).

3.5.2.19 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 PAS/CMS Help Desk users to Oracle Forms.

3.5.2.20 Audit records will be 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.

3.5.3 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. General policies are as follows.

3.5.3.1 All accesses in and out of the Pathway Data Centres will be restricted to the required traffic from/to specified sources. Once within the Pathway system, traffic will be routed only to specified ports at systems which require that traffic. Both these will be done using routers, and if necessary, other application gateways/firewalls.

3.5.3.2 Routing of traffic within the Pathway Data Centres will also be restricted to ensure traffic is only routed between systems which need to communicate. This will be done using access controls at the appropriate routers.

3.5.3.3 Each node at the Pathway Data Centre will be set up to restrict the traffic allowed at its ports to the permitted traffic there (except where routers, firewalls or other systems ensure that no other traffic is possible).

3.5.3.4 Workstations which have access to sensitive data will generally be on separate networks linked only into the Pathway secure network. Where such workstations are in any way connected to other networks, the sensitive data will be protected from the other network by an authorised combination of routers and firewalls configured to prevent any traffic between the network and these workstations. All such cases will be documented in this Access Control Policy and are confined to the Pathway management site (Feltham).

3.5.3.5 Where workstations and servers require access to both the Pathway Data Centres and other systems, an authorised combination of routers and firewalls will be configured to restrict the traffic to that permitted. All such cases will be documented in this Access Control Policy and are confined to the Pathway management site (Feltham).

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

3.5.3.7 No other accesses in and out of Pathway will be permitted.

3.6 Other Access Controls

In some cases, the information system cannot provide all the access controls required. This will be the case, for example, where a customer contacts Pathway by phone and asks for data which should only be available to authorised people. If this is the case, the caller will not be known to the IT system, so some other form of authentication of the caller is required.

3.6.1 Customer Authentication

No general policies are specified for how to identify customers who are not known to the system as these will be different for different cases - authenticating customers at a Post Office is different from authenticating them on calls to a Help Desk. The methods used for authentication of customers are included in the definition of the appropriate domain.

3.6.2 Other Telephone Authentication to Help Desks

Apart from customers, Help Desk 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 PAS/CMS Help Desk and the Horizon System Help Desk will maintain information on the Post Office and other relevant sites and offices. Where possible, CLI will be used to check the source of the call is from a permitted site. Where this is not possible, or the particular action requested requires further authentication of the user, the caller will be asked for further information which the Help Desk can verify. The information known about such offices and sites will include the office code, the name of the manager/contact, the telephone number and the address.

For certain cases, different (normally extended) authentication is required. For example, verification of a telephone number may include calling back on the known number. In some cases, more information will be available to support the extended verification. The methods used for authentication in these cases are included in the definition of the appropriate domain.

Note: this procedure is still under discussion and may change.

3.6.3 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 without prior notice to the Post Office Manager.

Pathway visitors to Post Offices will be subject to Pathway vetting procedures and approval by PDA. 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.

3.7 Key Management

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

- Confidentiality and integrity protection of some or all data on particular links e.g. CMS to De La Rue, CAPs to PAS/CMS, system management workstations to the Pathway Central sites.
- CHAP authentication between Post Offices and Pathway Data Centres
- Digitally signing information such as benefit authorisations in transit to Post offices, automated payment records from Post offices and software distributed via Tivoli.
- Filestore encryption at the Post Office.

Use of cryptography requires use of cryptographic keys. This Access Control Policy defines how the cryptographic keys are protected when in the information systems. As different keys are protected in different ways, this is generally defined with the other controls at the appropriate domain. The Key Management Service at the Pathway campus is included in the POCL Central Services domain.

Keys are protected in line with CESG requirements.

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

3.7.1.2 Keys are changed periodically according to CESG policy. Different periods are expected to apply to:

- Symmetric keys used for encrypting data
- Key Encryption Keys (KEKs) used to encrypt other keys
- Certification Authority keys.

3.7.1.3 New KEKs are not distributed using existing KEKs.

3.8 Effect on other Pathway Standards and Procedures

This Access Control Policy defines the policy for controlling access to resources in the operational Pathway system. It defines the controls required at a sufficient level to show how the system is protected. However, as explained in section 1.2, there are other documents covering, for example, 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:

3.8.1.1 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.

3.8.1.2 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.
- 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.

3.8.1.3 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 PAS/CMS Help Desk. 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 procedures (particularly CFM). These must detail, for example, how remote access is properly authorised and the lines configured to allow this when needed (see sections 6 and 10).
- System management procedures to authorise, for example, distribution of software.
- Technical Help Desk procedures to ensure all relevant calls are logged with the SMC Powerhelp 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. THE DSS SERVICE ENVIRONMENT DOMAIN

4.1 Introduction

The DSS Service Environment Domain is illustrated in figure 4-1.

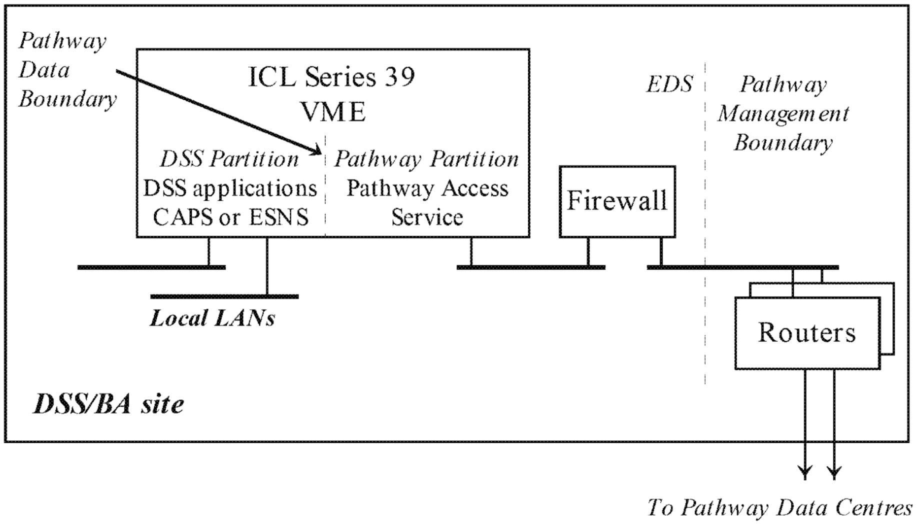

Figure 4 - 1 DSS Service Environment Domain

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

In both cases, applications in the Pathway partition of the VME machine handle transfer of information to/from the DSS partitions and to/from the Pathway Services at the Pathway Data Centres. The VME part of the CAPS Access Service (CAS) and the OBCS Access Service (OAS) transfer the information to/from the part of the Access Service at the Sequent system at the Pathway Data Centre, for transfer to the appropriate Pathway service (PAS/CMS or OBCS).

Transfer of this information is automated, and does not require human intervention.

This domain includes the following components:

- The software running in the Pathway partition of the VME platform, and
- The Pathway routers used to route traffic to the Pathway Data Centres.

4.2 Roles

The Pathway routers are managed as part of the Pathway Network Management as described in 10.4.

There are two types of roles with access to the Pathway partition on the VME CAPS/ESNS machines. These are:

- Roles for managing and supporting the Pathway partition and the applications in it.
- Roles for managing and supporting the VME system of which the Pathway partition is part. These include the EDS staff managing the VME system (including its split into partitions and resources allocated to these partitions) and the engineers analysing/repairing hardware or base software errors which involve the Pathway partition.

This Access Control Policy covers the roles for managing and supporting the Pathway partition. It does not define the roles of the EDS staff and Engineers who handle the VME platform as a whole.

Pathway System Management staff monitor the progress of the Pathway VME partitions using Patrol c.f. monitoring the Sequent systems at the Data Centre. All failures and warnings in CAS and OAS are raised as Patrol alerts. System Management via Patrol is described further in 10.3.

The following table lists the roles for the Pathway partition.

Note: *The split of responsibility for these roles has not yet been agreed, so the organisation responsible for the people in this role is not given. When responsibilities clarify, the definition of these roles will be reviewed.*

Role	Main Functions
System monitoring	Monitoring events in the Pathway partition.
Operational management	Operational management within the Pathway partition, including daily housekeeping.
Security Manager	Administering users of the Pathway VME partition.
Cryptographic Key Custodian (CAPS, but not ESNS sites)	Installation of the Red Pike cryptographic key which is 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).
Application support	Supporting applications in the Pathway partition, particularly CAS and OAS.
Pathway Security Auditor	Auditing security events relevant to Pathway.

4.3 System Access Controls for Human Users

The following table specifies for each Pathway partition role what access users of that role have to the system. In all cases, the user is individually identified. The user will be authenticated using the VME Enhanced Security Option. Where access to VME is from a remote site, these users will also have been authenticated individually to others systems - see sections 10 and 11.

Role	Access route	Resources Available
System monitoring	Interactive (MAC) access from remote site via Sonnet on Sequent. (Can also use Patrol)	Read only access to Pathway partition files except those holding cryptographic keys.
Operational Management	MAC access	Update access to partition files including software, but not cryptographic keys.
Security Manager	MAC access	User admin functions only.
Cryptographic Key Custodian	Local MAC access	Key installation software and files only.
Application Support	MAC access	Relevant applications and associated data (e.g. trailers in main data files).
Pathway Security Auditor	MAC access from remote site	Audit logs only (including user administration records).

4.4 System Access Controls

The Pathway VME partition has its own filestore separate from other partitions. This filestore will be set up to separate data with different access requirements and profiles will also be 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.

4.5 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 the Pathway Data Centres and the DSS site are:

- File transfer between the relevant VME service and PAS/CMS and OBCS on Sequent.
- Patrol management using ADI
- MAC interactive access for management, support and auditing
- Network management traffic to the routers.

5. POCL AND POCL CLIENTS DOMAIN

5.1 Introduction

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

- The POCL TIP system to which records of all transactions at Post Offices are sent.
- The associated POCL system which provides reference data about Post Offices and for EPOSS applications and shares the TIP link.
- The POCL Automated Payments system which processes Automated payments on behalf of POCL Clients. This will be replaced in future by direct links to POCL Client systems.

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

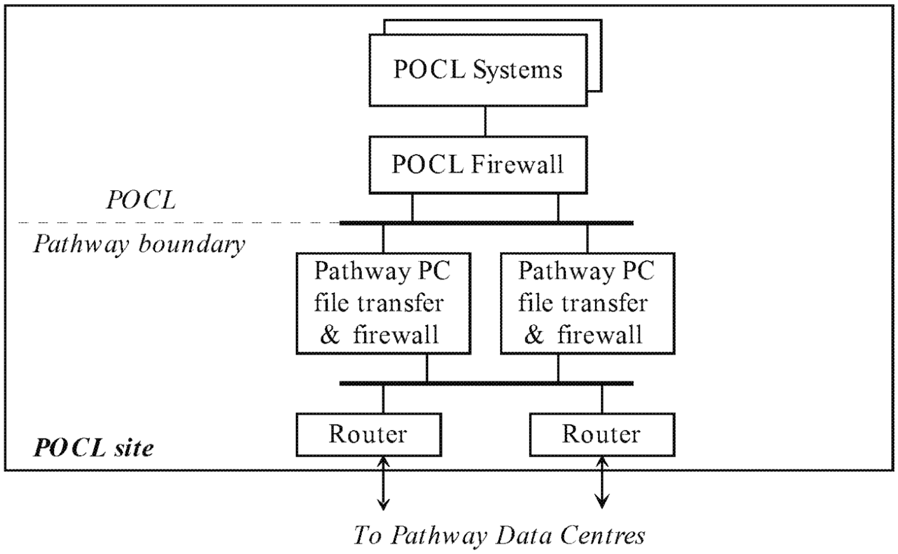

Figure 5-1 Pathway components at POCL Sites

The Pathway PCs at the POCL sites handle file transfer to and from the Pathway Data Centres. These PCs also contain firewall software to protect Pathway from the POCL systems.

Note: this has not yet been formally agreed.

The PCs are expected to be managed using Tivoli System Management from the Data Centres. The routers are managed using network Management from the Data Centres as described in 10.4.

There are some differences between these POCL sites as follows:

- Automated payments are signed and transferred over ISDN links;
- The TIP/Reference data link will be encrypted (post release 1)

5.2 Roles

The PCs and routers at the POCL sites will not normally have any human access - the only role supported is for engineering access. This will not be done while the PCs are configured into the operational system.

There may also be a Key Custodian role (post release 1).

POCL Auditors are not users of the Pathway components at POCL sites, so are not listed here.

5.3 Control of Connections to the Pathway Data Centres

Only the following traffic will be permitted between the Pathway Data Centres and POCL sites:

- The file transfers between Pathway hosts (TIP/EPOSS, Reference Data and AP) and the POCL systems
- System Management traffic to manage the PCs using Tivoli [to be confirmed.]
- Network management traffic for router management

The WAN (and in the case of the AP system, the ISDN) routers at the Data Centre will not permit other traffic to POCL sites. The Pathway router at the POCL sites accepts only this traffic.

5.4 Control of Connections to POCL Systems

Access from the POCL systems uses FTF. A firewall software product on the PCs at POCL systems is expected to restrict traffic as required (and provide address translation to Pathway IP addresses.)

Note: to be confirmed.

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.

6. POCL CENTRAL SERVICES DOMAIN

6.1 Introduction

The POCL Central Services Domain is illustrated in figure 6-1.

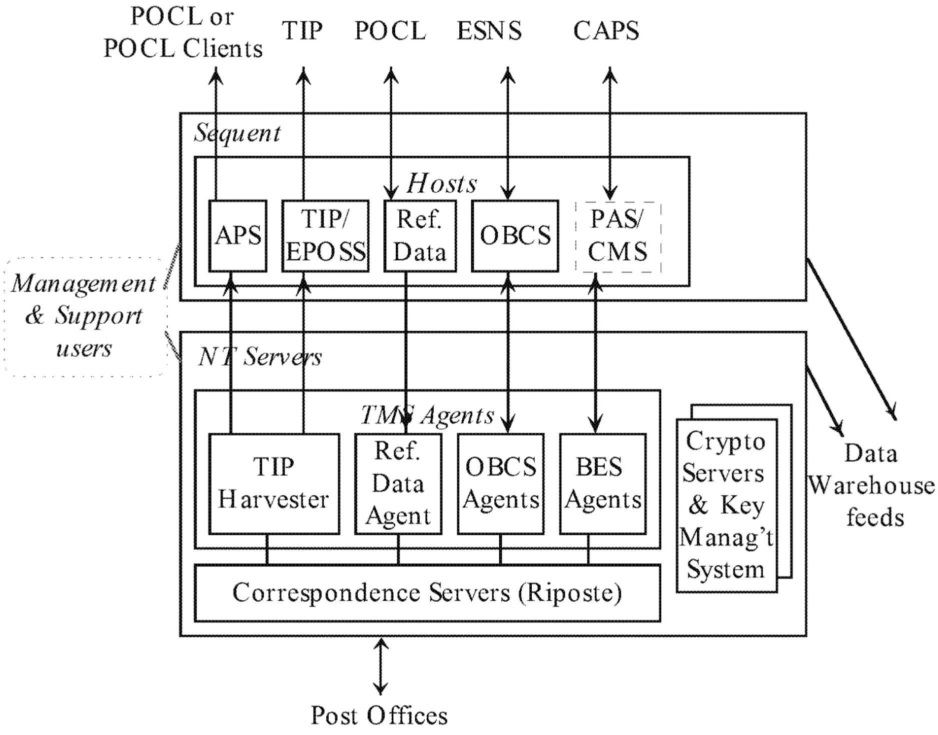

Figure 6-1 Interactions in the POCL Central Services Domain

The hosts at the POCL Central Services Domain are on Sequent machines running Oracle applications - APS, TIP/EPOSS, OBCS and the Reference Data Management Centre. (The PAS/CMS host and associated Help Desk is complex enough to be considered a separate domain).

The TMS agents act as the 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. (Currently, all host applications store data in Oracle databases).

One set of TMS agents (TIP Harvesters) extract all transactions from the correspondence service (via the Riposte API) for forward transmission to TIP. These also pass on transactions to application based agents for APS (and thence to POCL) and TIP/EPOS and to the Data Warehouse. The BES and OBCS Agents are separate.

The Correspondence servers are the part of the Transaction Management Service at Pathway campuses. They record all transactions at the Post Office Counters and archive these.

The main operational flows though the hosts, TMS Agents and TMS are automated, as is most System Management. (System Management is described in section 10).

6.2 Sequent Systems with Oracle Databases

All the host systems in this domain run on the Dynix operating system on Sequent and use Oracle databases. Interactions with Sequent systems are illustrated in figure 6-2.

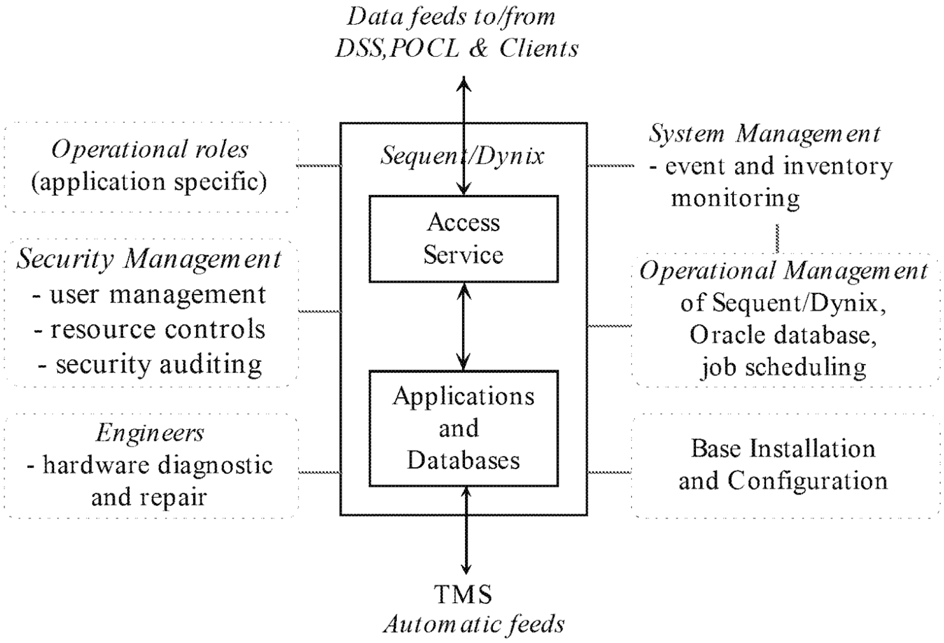
Data feeds to/from DSS,POCL & Clients
Operational roles (application specific)
Security Management
- user management
- resource controls
- security auditing
Engineers
- hardware diagnostic and repair
Sequent/Dynix
Access Service
Applications and Databases
System Management
- event and inventory monitoring
Operational Management of Sequent/Dynix, Oracle database, job scheduling
Base Installation and Configuration
TMS
Automatic feeds

Figure 6-2 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, most of the system management is done automatically (see section 10). As the results of monitoring the system, the need to take some remedial action will be recognised, and this action will generally be taken automatically. Only in exceptional circumstances is human intervention required. Active users on the operational system (apart from Tivoli system management) are defined in 6.2.1. The main users are:

- Security management who manage security information about users, access controls on resources such as files and database views etc.
- Operational Management people responsible for the management of the Dynix operating system and Oracle databases. The normal role here is monitoring the system. More active use of the system only occurs as the result of incidents.
- Application support people diagnosing software faults and engineers diagnosing and clearing hardware faults
- Security Auditors

6.2.1 Roles

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

Role (and organisation)	Main classes of functions
Computer Operator (CFM)	Physical operations e.g. media handling, but no on-line use of the system.
System Monitoring (CFM)	Monitoring the operational system using Patrol.
Operational management (CFM)	Management of Dynix including any action needed concerned with replication between campuses and local archiving. Oracle database administrator for database structure - setting up views, space allocation etc. Operational monitoring/management using Patrol workstations. Job scheduling (Sequent & NT) using Maestro workstation.
Security Management (CFM)	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.
Emergency operational management (CFM)	Operational management done by CFM staff on call. This is a subset of the full operational management functions above. It does not include security management or application support.
Dynix 3rd line support (Sequent)	Operational management of Dynix by Sequent staff when CFM cannot cure problem.

Role (and organisation)	Main classes of functions
Database 3rd line support (Oracle)	Operational management of Oracle when CFM cannot cure problem. This may sometimes require updating the database.
Application support (SSC)	Supporting Sequent/Oracle applications, including having access to the data in the database, not just its structure.
Application 3rd line support (Oracle)	Supporting Oracle applications
Engineer	Hardware diagnostics and repair including disc support
Base Installation and configuration (CFM)	Initial installation and configuration the base system - Sequent and Oracle databases. Later updates to these.
Security Auditor	Auditing security related actions

6.2.2 System Access Controls for Human Roles

As for all domains, system access controls conform to the policies in section 3.5.2. Specialisations of the policies for this domain are:

- Certain operational management roles on Sequent allow a change of username (see 3.5.2.12). This is restricted to use within the secure menu system described below.

Access controls are the Sequent system are enforced using Dynix facilities with some additions. In particular, all operational management users will access the system using a secure menu system. This constrains the functions called depending on the user's role. It also audits all functions performed by that user. Most management activities will be done using specific functions on the menu. Where the function requires a change of username, that will be done automatically by 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.

Note: Some of the operational and system management users have access to a number of systems and are described more fully in section 10. Information in this section is limited to their use of the Sequent system.

The following table specifies for each role how users access the system (workstation type and location), how they are authenticated, where the users taking this role are defined and what resources are available to people with this role.

Role	Workstation type	Location	Authentication method	Where user defined	Resources available
Computer Operator	None	Pathway campus	none, as no access	-	none in system
System Monitoring	X terminal (or emulator)	Pathway campus and Belfast	UNIX with individual user name & password	UNIX	Resources as available via Patrol
Operational Management	NT Workstation (X terminals or emulators for Patrol & Maestro)	CFM secure site	UNIX with password and token authentication (see note 3) & Oracle password	UNIX with associated group; Oracle user with associated role for dba functions	Functions as on menu. This can allow use of root and UNIX commands and Oracle dba functions.
Security Management	NT workstation on secure LAN	CFM secure site	UNIX and token (see note 3)	as above	User information in UNIX and Oracle
Emergency Operational Management	NT Workstation on secure LAN	CFM site (see note 4)	UNIX and token authentication (see notes 3, 4)	as Operational Management above	as Operational Management above
Dynix 3rd line support	NT workstation	Secure site (see note 6)	UNIX plus token (see notes 5 and 6)	as above	UNIX, which can include root access
Oracle 3rd line support	NTworkstation	Secure site (see note 6)	UNIX plus token (see notes 5 and 6)	as above	Oracle dba functions, and limited UNIX as needed for db support
Application Support	NT workstation	Pathway secure site	UNIX	Associated UNIX and Oracle usernames	Relevant application and associated data only
Application 3rd line support	NT workstation	Secure site (see note 6)	UNIX plus token	as above	as above
Engineer	computer console	Pathway campus;	UNIX with engineer password (see notes 5 & 7)	UNIX	Access to relevant diagnostics and, when needed, data on suspect hardware
Base Installation	computer console	Pathway campus	UNIX	UNIX user and group	most
Security auditor	NT workstation on secure LAN	Feltham	UNIX and token authentication	UNIX	Audit logs

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 root privilege. 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 by CFM staff on call. This is currently expected to be from the CFM secure site at Belfast.
5. All visiting staff will be subject to manual procedures on entering the secure Pathway site to authenticate who they are and authorise their access to the computer room - see 3.6.3.
6. Sequent and Oracle staff will provide 3rd line support. This may be from the Data Centre. Where visiting Sequent or Oracle support staff are not known to the Sequent system individually, but are authorised by the manual mechanisms, a special UNIX user and password will be set up to allow them to use the system for this session under supervision.
   Access from Sequent and Oracle sites is being considered. If so, this will always be done from a secure LAN in a secure area via an encrypted link to the campus.
7. Visiting engineers are subject to manual procedures as in 5 above.

6.2.3 Dynix and Oracle Access Controls

The Dynix operating system should be set-up according to the access control policy in 3.5.2 above. For example, Security Audit Logs (both Dynix and Oracle ones) will only be accessible to Security 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 will be done by automated processes. Interface tables used for this will generally be defined in separate database views to restrict the damage possible due to failures during automated processes.

Database administration will be split into roles as defined above, separating database administrative functions concerned with the structure of the data and the resources used from user management and from access to the data in the database.

6.2.4 Control of Connections to the System

All links to the Sequent systems are controlled by routers and by controls on the use of Sequent ports. These restrict access to the Sequent system from other services at the Pathway Data Centres and elsewhere. There will be a separate port for each application and type of link to that application. The following traffic will be permitted:

- Telnet and X-terminal access to Dynix for operational management, 3rd line support, job scheduling and security auditors
- OSI traffic to VME (FTF, ADI and MAC) to support file transfer 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 to PCs for transfer of business data to/from POCL and De La Rue

Note that the links from remote management sites, including the CFM sites, are encrypted.

6.3 Windows NT Systems

There are several NT systems in this domain. TMS Agents are generally on separate NT servers from those used for the Correspondence Servers. The Cryptographic Servers and Key Management System are also on separate NT servers. Further NT systems in this domain, for example are the PCs providing the interfaces to transfer files to De La Rue, POCL and the server supporting the Time Service.

Users of the NT servers are illustrated in figure 6-3.

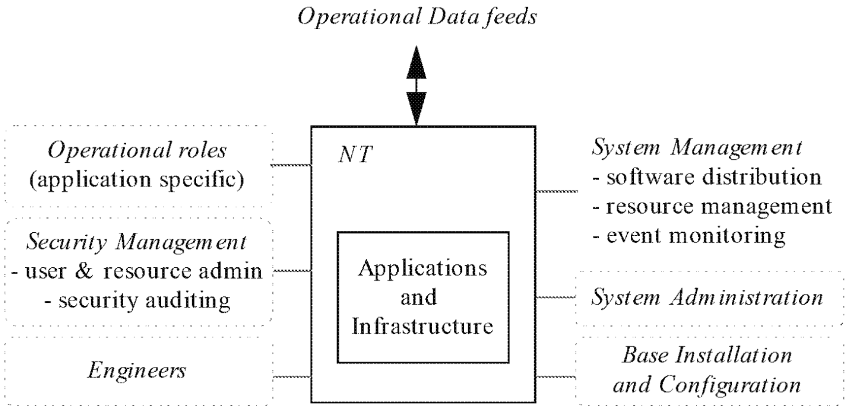

Figure 6-3 Users of NT systems

As for the Sequent systems, most of the use of the NT systems is automated so human intervention is an exception. Different NT servers are used to 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.

- The NT servers are managed using Tivoli and NT administration. Events and resources are monitored via Tivoli (see section 10) and appropriate remedial action is generally taken automatically. User administration is done using NT utilities.
- Software and configuration information is distributed to these systems via Tivoli (see section 10).
- NT servers also have local consoles which can be used 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 6.3.1. However, extra roles are used at some NT systems. For example, Riposte administration is required at the Correspondence servers and there will be a person responsible for keys at the Key Management System. Such specific roles are included in the particular sub-section about that system.

6.3.1 Roles

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

Role (and organisation)	Main functions
Computer Operator (CFM)	Physical operations e.g. media handling, but no on-line use of the system.
Operational on site management (CFM)	Any residual management of NT (not done by system management) which requires on site access.
Security Management (SMC*)*	Administering NT user information, including group membership.
Engineer (DSD)	Hardware diagnostics and repair
Base Installation and configuration (CFM)	Initial installation and configuration the base system - NT etc Later updates to this.
Security Auditor (Pathway)	Management of, and access to, Audit logs.

6.3.2 System Access Controls for Human Roles

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

Role	Where defined	Workstation type and location	Authentication method
Computer Operator	-	no w/s; on site at Pathway campus	none, as no access
Operational on-site Management	NT with associated group;	campus	NT with password
Security Management	as above	NT workstation at secure Pathway (SMC) site	NT with password plus token
Engineer	NT user	Pathway campus; no remote access	NT with password
Base Installation	NT user and group	Pathway campus	NT with password
Security Auditor	NT user	NT workstation at Feltham	NT with token

6.3.3 System Set Up

System access controls will conform to the policies in 3.5.2.

All NT servers are set up with a 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.

NT systems will 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 the domain. However, some roles (Engineer and Key Custodian) will always be defined as requiring the user to be local at the machine.

6.3.4 Control of Connections

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

- Telnet traffic for NT management, security auditor access etc
- NT domain traffic
- Maestro job scheduling
- Tivoli traffic for event management, software distribution etc

However, the KMS system 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.

6.4 Correspondence Servers

The Correspondence servers and their interactions with other services are illustrated in figure 6-4.

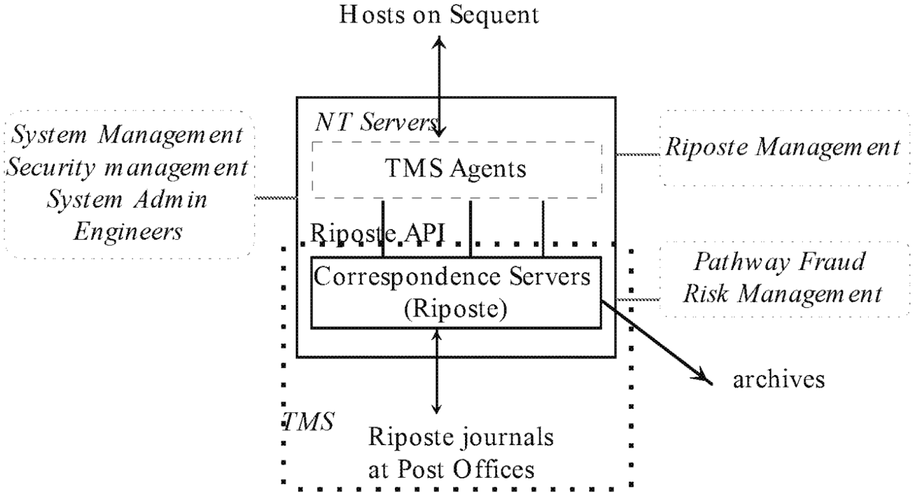

Figure 6-4 Correspondence Servers and their Interactions

The Correspondence servers, together with the Riposte infrastructure at the Post Office handling the Riposte journals there form the Transaction Management Service. TMS handles all application traffic between the Pathway campuses and the Post Offices. Note that there is other traffic between the Pathway campus and the Post Offices for System Management traffic and Key Distribution.

6.4.1 Roles

Operational use of Correspondence Servers is automated, so does not require human intervention. This includes transferring data to the Post Offices and transactions back from them and archiving these transactions.

People in the following roles have direct access to Correspondence Servers (in addition to System Management, Operational Management, Security Management and Engineer roles described in 6.3):

Role	Main Functions
Riposte Management (SMC)	Setting up and maintaining Riposte message stores and archives. Any configuring of correspondence servers which is not automated. (Setting up Correspondence servers as members of Riposte groups when new Post Offices are added will be done by the auto-configuration application.)

Role	Main Functions
Pathway Fraud Risk Management	Limited access to the TMS transaction log (see note)
Application support (SSC)	Supporting Riposte and other applications

Note: FRM access to the Correspondence servers may be allowed in exceptional circumstances for limited amounts of data (as otherwise, the performance of the system could be impaired).

6.4.2 System Access Controls for Human Roles

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 SMC secure site (see 10.2)	NT Correspondence server user with token	Appropriate Riposte utilities
Security auditor	NT at Feltham secure area	NT Correspondence server user with token	Audit logs and limited read only TMS access
Pathway FRM	NT at Feltham secure area	NT Correspondence server user with token	Limited read only TMS access (see note)
Riposte application support	NT at Feltham	NT Correspondence server user and password	Read only Riposte access

Note: Details of this access have still to be agreed. If no specialised query tool is available, relevant Riposte utilities will be used e.g. Message Query and Message Spy.

6.4.3 System Set Up

For the Correspondence servers, the initial system set up will include the initial configuration of Riposte. Different Riposte utilities are available to different types of user. For example, Auditors and Fraud Management staff will be restricted to utilities with read only access to TMS.

6.4.4 Control of Connections

Connections permitted in and out of the correspondence servers are the general NT ones listed in 6.3.4 plus:

- data transfers to/from agents using Riposte RPC
- data transfer to/from Post Office via TMS

6.5 BES Agents

The interactions with the BES agents are illustrated in figure 6-5.

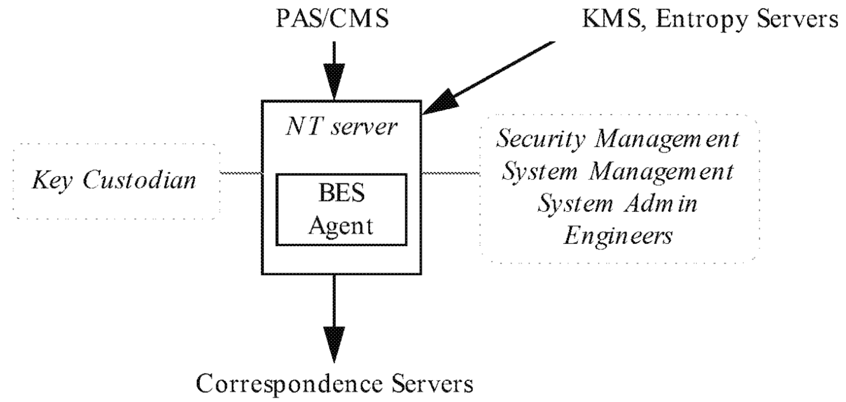

Figure 6-5 Interactions with BES Agents

BES Agent signs payment authorisations before they are transmitted to the Post Office. The BES Agent calls on an Entropy Server on a separate PC to obtain the entropy needed for signing using DSA.

The main difference for Access Control purposes between the BES and other NT servers in this domain is that it requires secure installation of keys (the Pathway DSA private key for protecting payment authorisations and associated public key certificate etc) and protection of these keys and the associated entropy within the NT system.

So roles at the BES Agents are the Cryptographic Key Custodian responsible for the required keys and certificates (as defined in 6.9.3) and the Management, Engineer and Security Auditor roles as for other Campus NT systems as defined in 6.2.

Connections permitted to other systems are:
- SQL*Net links to PAS/CMS for payment authorisation and card information etc
- Links via the Riposte API using RPC for distribution to/from TMS.
- Links to the Entropy Servers to obtains DSA entropy.
- Links to KMS for distribution of some key material using key distribution protocols which protect keys in transit.
- System Management links to Tivoli servers at the Campus.

Routers will be configured to allow only these links.

6.6 Specific OBCS Related Services

Figure 6-6 illustrates the flow through the OBCS applications. Note that this is very similar to the flow through the Benefits Payment Service as described in 2.3 except that there are no links to card production, no associated help desks and the agents are simpler.

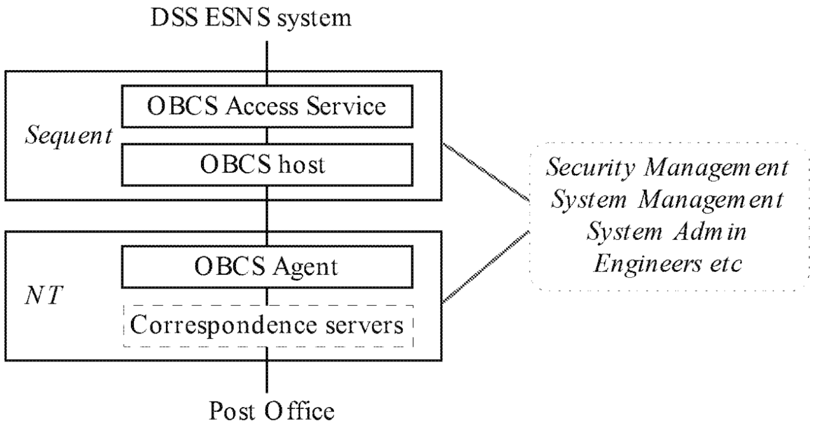

Figure 6-6

The OBCS Related Services are similar to the hosts and agents for other applications and have no special access control requirements. Access controls for the Sequent based applications as defined in 6.2 above and those on NT as defined in 6.3 above.

Connections to other systems are as illustrated in figure 6-6. (The Sequent connections are included in the table in 6.2.4.)

6.7 Reference Data Management Centre

Reference data is mainly the data associated with particular applications such as the price of stamps for EPOSS and the meaning of reason codes in BPS. However, it also includes other data such as the telephone number and the name of the Post Office Manager for a Post Office and the meaning of Help desk Codes used by the Horizon System Help Desk.

Interactions with the Reference Data Management Centre on Sequent are illustrated in figure 6-7.

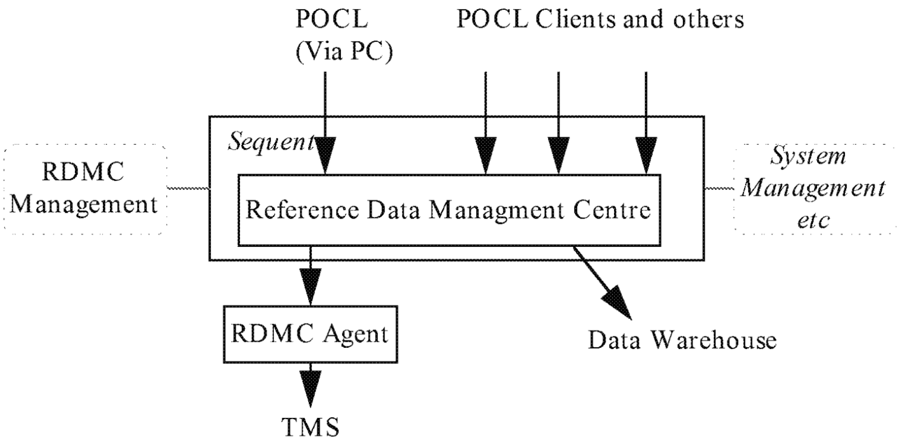

Figure 6-7 Interactions with Reference Data Management Centre

Data is fed into the Reference Data Management Centre (RDMC) from POCL and in future also other sources including POCL Clients. Data coming in is classified according to whether it should be used to update the RDMC 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.

Application reference data for EPOSS, OBCS etc is distributed via the TMS system to the Post Offices.

Reference data is also fed to the Data Warehouse, for example, to define transaction codes and the shape of the records to assist in the analysis of transactions.

For reference data of class 2 and above, the data is held at the RDMC until the dependencies for its use have been satisfied. For example, the software needed to process must be available and shown to work with it.

The RDMC is on the Sequent system, so subject to the controls in 6.2.

The RDMC manager kicks off the transfer of validated reference data of classes 2 to 5 to TMS when all required dependencies have been met. RDMC users have read access to the RDMC to assist in satisfying the dependencies. Oracles roles control this access. The RDMC Manager and Users are based at Feltham and access the RDMC from NT workstations there via the encrypted links.

Note that the security management role in 6.2 includes user management of the core users of the system, including the RDMC users.

6.8 Specific TIP Related Services

The Interactions with the TIP services are illustrated in figure 6-8.

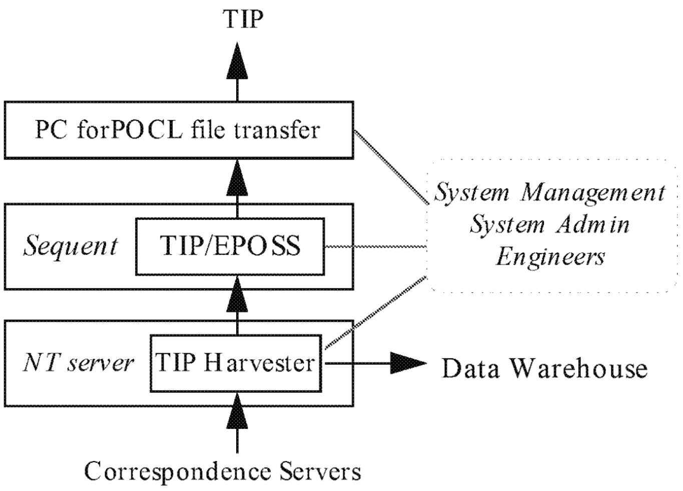

Figure 6-8 Interactions with the TIP services

The TIP Harvester handles all transactions from the Post Offices and forwards transactions via the TIP/EPOSS host to the POCL TIP system. It also supplies data automatically to the Data Warehouse.

The TIP/EPOSS host has access controls as for any other Sequent based host, so roles and system set up are as defined in 6.2 above.

The TMS Agent has access to all business transactions from Riposte, as all these need to be passed onto the TIP system and Data Warehouse (whereas other Agents should only have access to the transaction types they need to handle). Apart from this, the TIP Harvester Agent is controlled as for any other TMS Agent running on an NT system as defined in 6.3 above.

6.9 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 Service** (KMS) which (generates and) stores cryptographic keys for distribution to other Pathway services and the Post Offices.
  Associated with this is a **Certificate Authority** (CA) to generate public key certificates and **Entropy servers** which generate DSA entropy for digital signatures.

- An **Authentication Service** to support token authentication.

- The security services supporting encryption of links to other sites.

6.9.1 Key Management and Associated Services

Interactions with the Key Management Service and Certificate Authority are illustrated in figure 6-9.

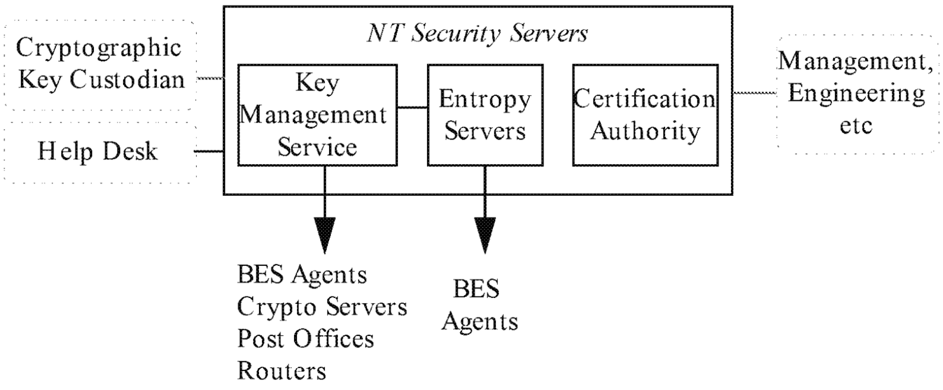

Figure 6-9 Interactions with the Key Management Service

The **Key Management System (KMS)** 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 KMS also uses the Entropy Servers to provides the entropy needed for DSA signatures.

A **Certification Authority (CA)** is used to generate public key certificates used when verifying digital signatures. This CA may be co-located with the KMS, though all CA functions are off-line.

(Private/public DSA key pairs are used to sign payment authorisations and also to sign software and Tivoli scripts before distributing them to the Post Office. Digital signatures are also used at the Post Office to sign automated payments.).

The Pathway Cryptographic Keys Manager will be responsible for generating keys at the KMS and providing the recovery key for a Post Office Manager who has lost his card or PIN, so needs one.

Apart from this, these NT systems will be set up with the roles and access controls as described in 6.3 above.

Note: control of connections for the KMS and CA have still to be defined.

6.9.2 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.

Note: details of this Authentication Services have still to be finalised.

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:

- Management of the underlying UNIX system
- Installation and configuration of the Authentication Server
- Administration of tokens and users for all Pathway users who require authentication via tokens.
- Security auditing, which may include real time monitoring as well as selective reporting from the Authentication Service audit logs.

6.9.3 Key Custodian Role

Several of the systems at the Data Centre require a cryptographic key to be installed and periodically changed. These keys are used to encrypt/decrypt data in transit between sites.

Such keys are installed manually on the following systems:

- The BES agents. These have the private key for signing payment authorisation for transmission to the Post Offices.
- The Sequent system (Red Pike key for protecting the link to CAPS)

- The PCs handling the De La Rue links. Keys are needed at PCs on both the Pathway and De La Rue sites.
- The Zergo boxes used to encrypt certain links e.g. Pathway Data Centres to Pathway sites such as Feltham and Stevenage.
- In future, the TIP link.

The private key for signing software will be installed at the Configuration Management system at Feltham.

Where keys are installed manually, the same Cryptographic Key Custodian is responsible for all systems. In all cases, this role is set up so that the user must be a local one. The Key Custodian authenticates using a token. The Sequent or NT box used for this must therefore support a SecurID client. Also, the filestore used to hold the key must be accessible only to the Key Custodian.

6.10 PCs Handling External Links

File transfers between the Pathway Data Centres and POCL, De La Rue, and in future, POCL Clients are handled by PCs at either side of the link. (File transfer to/from CAPS is directly to the Sequent machines.)

These PCs will be set up to limit the functions possible there to a minimum. The PCs at the POCL and De La Rue sites are controlled as described in sections 5 and 9. In general, these, and the PCs at the Data Centres will be managed as for other NT systems as described in 6.3.

Note that at least the De La Rue PC supports a Key Custodian role as defined in 6.9.3.

6.11 Other Data Centre Services

There are a number of other services at the Data Centres such as:

- The Automated Payments Service on Sequent which takes payments extracted from the TMS journal by the TIP Harvester and feeds data to the APS PC at the Data centre and from there to POCL (and in future, POCL Clients).
- The OBCS Service on Sequent
- The Time Service on NT

These services have no special access control requirements. On Sequent access control is as specified in 6.2 above and if on NT, as in 6.3 above.

System Management Servers are covered in section 10 below.

7. PAS/CMS SERVICE DOMAIN

7.1 Introduction

The Payment Authorisation Service (PAS) and Card Management Service (CMS) are the Pathway hosts supporting the Benefits Payment System. They run on Sequent machines at both Pathway campuses and share one Oracle database. Access controls for these are described in 7.2 below.

The PAS/CMS Help Desk supports customers, Post Offices and the Benefit Agency enquiring about payment authorisations, cards and PUNs. Help Desk Advisors have access to the PAS/CMS system via Oracle Forms from NT workstations. The Help Desk is managed by Girobank. Access controls for these are described in 7.3 below.

7.2 PAS, CMS and CAPS Access Services

The interactions with PAS, CMS and the associated access service to CAPS are illustrated in figure 7-1.

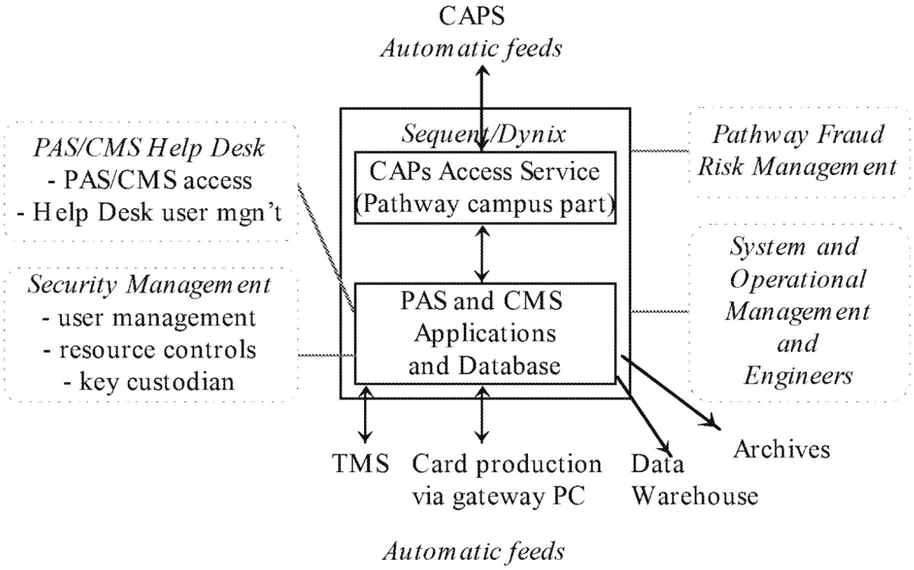

Figure 7-1 Interactions with the Sequent Systems

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 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.

7.2.1 Roles

General roles for the Sequent system are defined in section 6.2. Specific PAS/CMS roles are:

- PAS/CMS Help Desk Advisors using Oracle Forms applications to access PAS/CMS queries in response to calls and Help Desk Security Managers maintaining information about Help Desk Users at the PAS/CMS database. These users are further described in 7.3 below.
- Application Management generating payment authorisations when CAPS is down.
- Cryptographic Key Custodian installing/updating the encryption key needed for the CAPS to PAS/CMS link.
- Fraud Risk Management staff accessing PAS/CMS data when required information is not available via the Data Warehouse or archives.

7.2.2 System Access Controls for Human Roles

Access controls associated with these roles will conform to the policies in 3.5.2. The following table shows the system access controls associated with these roles. Apart form the Cryptographic Key Custodian, all these users access PAS/CMS information via Oracle tools.

Role	Workstation type and location	How authenticated to PAS/CMS (& where user defined)	Resources available
Help Desk Advisor	NT Help Desk workstation in Girobank area at campus	Oracle username, password (Oracle user associated with Oracle role)	Particular database views of PAS & CMS tables required for the authorised Oracle Forms (with sufficient write access to allow cards to be stopped, update call logging tables and change password.)
Help Desk Supervisor	as above	as above	As above, plus the ability to handle NSI calls (see note) and other more restricted dialogues.
Help Desk Security Manager	as above	Oracle username, password (Oracle user associated with Oracle role)	Oracle user and role tables via authorised Oracle Forms; access as Help Desk Advisors plus privilege to create users and assign/re-assign them to Help Desk roles.
Cryptographic key custodian	local machine console	UNIX with password and token	Special file containing key
Fraud Risk Manager	Girobank FRM area and Feltham	UNIX with password and token	Read only access main database in exceptional circumstances

Note: A separate role may be defined for Help Desk Advisors who can handle data with a National Sensitive Indicator.

7.2.3 Base System Access Controls and Control of Connections

In addition to the general Sequent controls in 6.2.3 above, for PAS/CMS, a separate username is required for the Cryptographic Key Custodian. Filestore accessible only to that user holds the cryptographic key.

All connections to the Sequent system are covered in section 6.2.4.

7.3 PAS/CMS Help Desks

The PAS/CMS Help Desks are run by Girobank at the central Pathway sites. They handle the following types of calls:

- Calls from Post Office counter clerks about payment authorisations and cards. Some of these can initiate changes to the 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

The Help Desks use NT workstations with shared NT servers. The workstations are linked via routers to the PAS/CMS system for queries on the PAS/CMS database.

Interactions with the Help Desk systems are illustrated in figure 7-2.

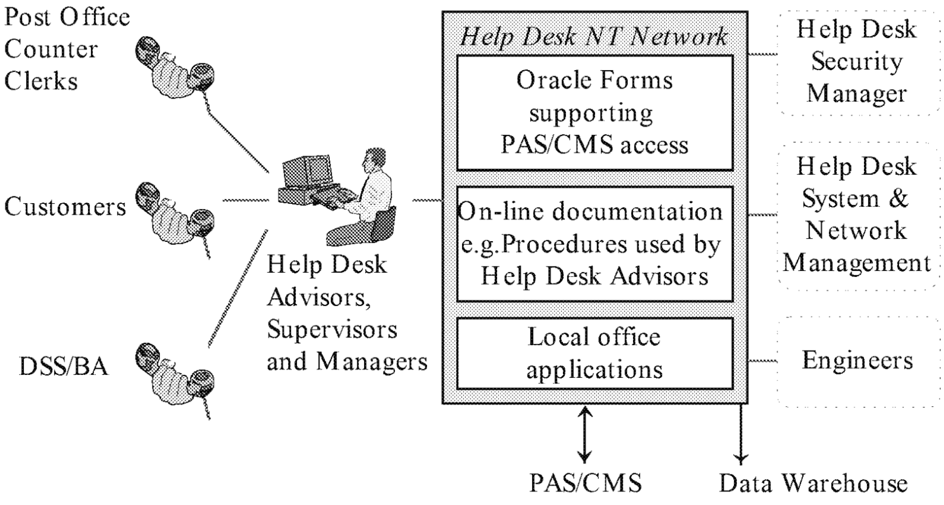
Post Office Counter Clerks
Customers
DSS/BA
Help Desk Advisors, Supervisors and Managers
Help Desk NT Network
Oracle Forms supporting PAS/CMS access
On-line documentation e.g.Procedures used by Help Desk Advisors
Local office applications
Help Desk Security Manager
Help Desk System & Network Management
Engineers
PAS/CMS
Data Warehouse

Figure 7-2 Interactions with the PAS/CMS Help Desks

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

Help Desk Supervisors also have access to some local office applications. Help Desk Managers rarely use the information systems, but if they do, have the same access to PAS/CMS as other Help Desk Users. They may use different local applications.

The Help Desk Security Manager is responsible for administering information about Help Desk users at both the local Girobank system and PAS/CMS.

Help Desks and their associated systems are run by Girobank, so are not managed by CFM and are maintained by different engineers.

7.3.1 Roles

People in the following roles have direct access to the Help Desk Network. All are in the Girobank Help Desk area of the campus and all use NT workstations. All are Girobank personnel except the engineers.

Role	Main functions
Help Desk Advisor	Use Oracle Forms to access PAS/CMS queries is response to calls - see 7.2.
Help Desk Manager	As Help Desk Advisor, plus use of local Girobank office applications
Help Desk Supervisor	As Help Desk advisors plus: - extra transactions at PAS/CMS - local applications - applications analysing Rockwell ACD data
Help Desk Advisor in training mode	Use standard Advisor Oracle Forms to access training version of PAS/CMS database
Help Desk Security Manager	Maintains information about Help Desk users locally and in PAS/CMS. Auditor for local systems
System & Network Administrator	Manages Help Desk NT Network - installation and operational management. Base software installation and configuration. Distribution of software (including Oracle Forms) from Help Desk Servers to workstations. Management of Girobank routers etc
Engineer	Hardware diagnostic and repair

In addition to these roles with direct access to the system, operational use of the system also requires some indirect users as shown in figure 6-3. i.e. Post Office counter clerks, Benefits Agency staff and Customers.

7.3.2 Local Network Configuration

The Girobank Help Desk network is illustrated in figure 7-3.

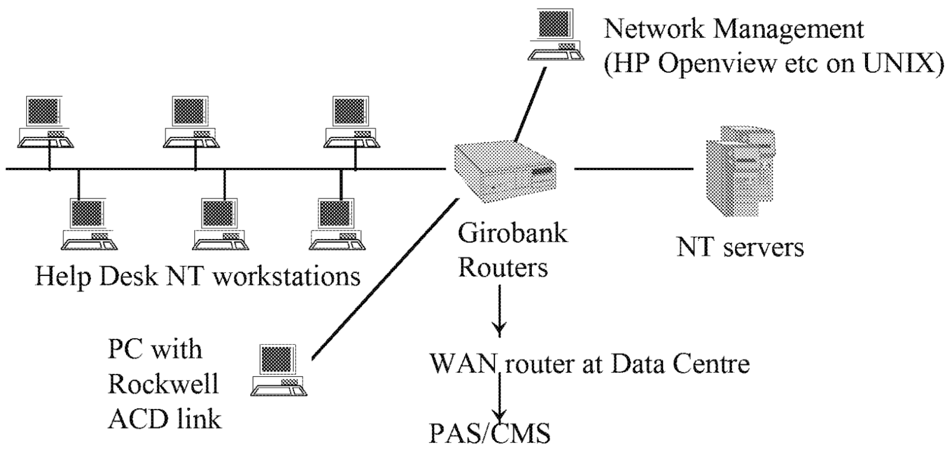
Network Management
(HP Openview etc on UNIX)
Girobank
Routers
NT servers
Help Desk NT workstations
PC with
Rockwell
ACD link
WAN router at Data Centre
PAS/CMS

Figure 7-3 Help Desk Configuration

The Pathway Access Control Policy is concerned with controlling the access from the Help Desk to the Pathway systems. Controls at the PAS/CMS Sequent system will restrict access to defined Oracle views. However, as write access is needed (to stop cards etc) control of the Oracle Forms applications is needed in the Help Desk environment to ensure Help Desk staff can only use authorised Oracle Forms menus and the associated authorised set of Oracle Forms for the permitted role.

All Help Desk staff use NT workstations. All these workstations can be used for:

- Running PAS/CMS transactions on PAS/CMS via Oracle Forms
- Viewing on-line documentation. Some documentation will be available to all Help Desk Advisors. Other documentation is restricted to Help Desk Managers and/or Supervisors.
- Running local office applications, including the application to monitor telephony traffic. (Any workstation can be used for training activities, even though special workstations may be allocated for formal training courses.)

All workstations used for access to PAS/CMS have their floppy drives disabled (to prevent floppies being used to update the Oracle Forms applications used to access the PAS/CMS system.) There will be at least one workstation on the Help Desk network with a floppy drive, but this will have controlled access and cannot be used to access PAS/CMS. (This is to allow supervisors to produce documents at Help Desk workstations and transfer them to laptops and other systems.)

Some applications and on-line documentation are held on the NT servers. Read only access is provided to all Help Desk Advisors, supervisors etc. For performance reasons, Oracle Forms applications are held at the workstation.

Girobank System and Network Administrators set up and administer the NT systems, including distribution of software within the network and administration of the Girobank routers.

7.3.3 Control of connections to the Help Desk

Most connections into the Help Desk are telephones. These are independent of the Help Desk network except that information is fed from the Rockwell ACD to a particular PC so that telephone traffic can be monitored. This PC will be configured as a separate domain so the telephony data can be routed automatically only to this PC. However, a Supervisor at a standard Help Desk can run an application to view this telephony information.

The other link is the one to the rest of the Pathway network, particularly the PAS/CMS system. This will only be used for:

- Oracle Forms for using the PAS/CMS database - both in response to telephone calls and by the security manager for administering user information
- Feed of information about calls (from Rockwell ACD) to Data Warehouse system.

This Access Control Policy document does not cover functions internal to the Girobank network which do not affect the rest of the Pathway system e.g. configuration and management of Girobank routers.

7.3.4 System Access Controls for Girobank Roles

The following Help Desk roles are covered in this Access Control Policy.

Roles	Where defined	Authentication needed	Resource access controls
Help Desk Advisor	In local NT system (with user profile) and at PAS/CMS system as Oracle Forms user	NT password log-on initially: Oracle password log-on for access to PAS/CMS	NT logon gives access to on-line documentation Oracle role gives access to specified data view
Help Desk Supervisor and Manager	As Help Desk Advisor	As Help Desk Advisor	NT group gives access to further local facilities
Help Desk Security	In local NT system At PAS/CMS, Oracle	As Help Desk Advisor, but using	NT user information ; Oracle user information

Roles	Where defined	Authentication needed	Resource access controls
Manager	Forms user with privilege to add users	different Oracle username and password.	for Help Desk Roles only
NT System Administrator	NT system only	NT password log-on	Access to most NT information
Engineers	Not known in system	NT password logon under supervision	Access to most NT information

7.3.5 Other Access Controls

Contact is made with the Help Desk Advisors from Counter clerks, the Benefit Agency and customers by phone as detailed in the Help Desk Call Enquiry Matrix [HDM]. 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 being discussed and are not yet finalised.

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 Help Desk 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	See section 3.6.2.
PO staff on behalf of customer	Queries and reports about cards etc	See section 3.6.2 for verification of Post Office staff plus customer verification information.
DSS/BA	Enquiries on cards, payments. Request to stop cards, payments etc	See section 3.6.2. plus extra verification; details dependent on if Nationally Sensitive *[tbs]*
BA for customers	As customer queries and reports	See above for verification of BA staff, plus customer verification info

8. OFFICE PLATFORM SERVICE DOMAIN

8.1 Introduction

The Office Platform Service Domain is illustrated in figure 8-1.

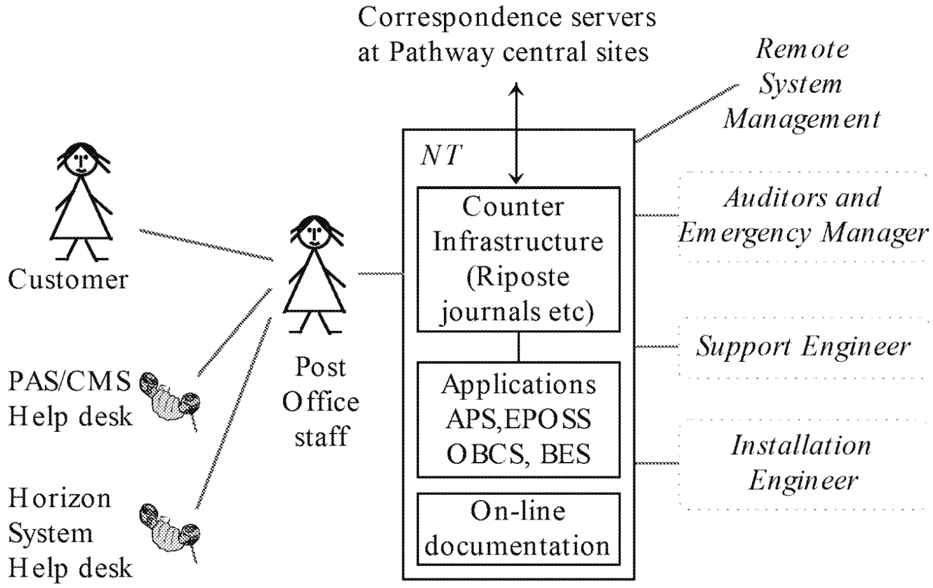
Correspondence servers at Pathway central sites
Remote System Management
NT
Counter Infrastructure (Riposte journals etc)
Applications APS,EPOSS OBCS, BES
On-line documentation
Auditors and Emergency Manager
Support Engineer
Installation Engineer
Customer
Post Office staff
PAS/CMS Help desk
Horizon System Help desk

Figure 8 - 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 PAS/CMS Help Desk, 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 and security managers 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.

Post Office Systems are monitored and managed via the Pathway System Management Services using Tivoli. This is used to distribute software and also Tivoli 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.

8.2 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 subpostmaster 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.

Pathway staff such as Security 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.

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 PAS/CMS Help Desk 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 (Exel)	Rollout of new Post Offices including setting up Post Office personality.
Support engineer (DSD)	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.

8.3 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 8-2.

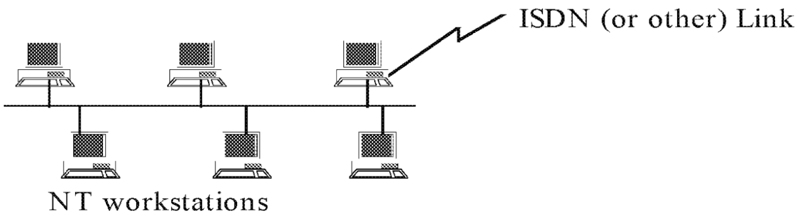

Figure 8-2 Post Office Configuration

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 will be made using the CHAP initial connection authentication protocol as defined in [SFS].

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

Service	Type of access
Auto-configuration on Post Office rollout	By installation engineer using auto-configurer application on rollout (using Tivoli and Riposte).
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 protocols. Scripts and software are signed for integrity protection.

8.4 System Delivery

As the result of Factory installation, Post Office workstations have NT, Riposte, applications and file encryption software installed. However, there is no specific information or code for a particular Post office. Personalisation information will be added during installation.

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 role 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 will be 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 8.6. These users will be 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-configurer one (see 10.6). It is not possible to log-on to NT or Riposte at this stage.

8.5 System Installation

The Auto-configurer application is run by the installation engineer on the gateway workstation. It 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.

8.6 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 normally printed) 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.

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.

8.7 System Access Controls associated with Human Roles

As for all domains, system access controls conform to the policies in section 3.5.2. The following specialisations of the general policies apply at this domain.

- Passwords will expire in 6 months, rather than 1 month (see 3.5.2.8).
- 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
  - the password cannot be the same as the username.
- 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 will be forcibly logged out.

The following table shows how access controls associated with human roles are enforced at the workstations.

In NT and Riposte, there is no direct support for roles, so these are represented by user groups - see 8.4. 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 Manager 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; member of 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	Workstation	Not in	Memory Card	Workstation start

Role	Function	Where users defined	Authentication needed	Resource access controls
permitted PO roles	start up	system	and PIN (see notes 2-4)	up only
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 with one time password (see note 6)	Relevant Riposte applications only
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. Use of Memory Cards on installation and workstation startup is further defined in [SFS]. More information about Roll-out in general is included in section 10.6.
3. The Post Office Manager is expected to lock away the Memory Card and PIN for it in separate places.
4. If the Manager looses his card or PIN, emergency recovery 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 using a Support username, using a one-time password (see note 6), to reset his password on his normal user name. In the absence of the Manager, this may also be used 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.

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.

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.]

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

8.8 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 also be contacted by the Horizon System Help Desk or Implementation Help Desk about technical or logistics issues. In this case, but no verification is needed in this case.

Post Office staff may contact Pathway Help Desks and will need to authenticate to them as defined in the section 7.3.5 (for the PAS/CMS Help Desk) and in 10.2.4 (for the Horizon System Help Desk).

9. DE LA RUE CARD SERVICES DOMAIN

9.1 Introduction

The De La Rue Card Services Domain is illustrated in figure 9-1.

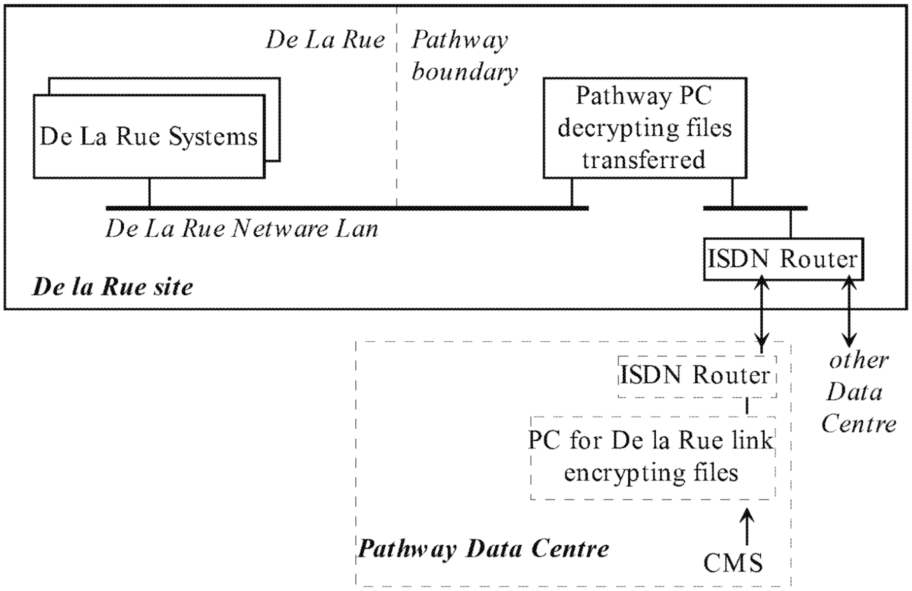

Figure 9-1 De La Rue Card Services Domain

Files of data for magnetic card 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 the Security Functional Specification. They are made available to the De La Rue system using NetWare file access. Information is returned to Pathway in the same way.

The PC is expected to be managed using Tivoli system management from the Data Centres. The router is managed using Network Management from the Data Centres as described in 10.4.

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

9.2 Roles

The only Pathway roles supported at the PC are:

- The Key Custodian installing and maintaining the Red Pike keys. For details of access controls associated with this role, see 6.9.3.
- An engineer installing or replacing the PC. This PC is not re-configured when linked to the Data Centres.

9.3 Control of Connections to the Pathway Data Centres

Only the following traffic will be permitted to/from the Pathway Data Centres:

Service	Type of Access	Controls at Data Centre
CMS	Automatic file transfer via the PC at Pathway Data Centre	At PC: file transfer from CMS only permitted At router: IP traffic for file transfer from DC PC
System Management (Tivoli)	Tivoli actions for the PC at the De La Rue site System management events reported from this PC to Tivoli	At router: Tivoli IP traffic from event management and software distribution servers permitted
Network Management (Open View)	actions for the router from Open View at the Data Centre	At router: IP traffic for network management from Open View server permitted

The ISDN router at the Data Centre allows no other traffic to the De La Rue sites from the Data Centre. The Pathway router at the De La Rue site only accepts the above traffic from the Data Centre ISDN routers. The PC at the De La Rue site will also restrict traffic to this.

9.4 Control of Connections to De La Rue Systems

All traffic from the De La Rue LAN is IPX - no IP traffic from this LAN will be permitted. Access will be permitted only from know IPX addresses on the De La Rue LAN.

Controls at the PC will ensure only read access from De La Rue via NetWare to incoming files from Pathway and ensure filestore separation from files for output back to Pathway.

10. SYSTEM MANAGEMENT SERVICE DOMAIN

10.1 Introduction

The System Management Service Domain is illustrated in figure 10-1.

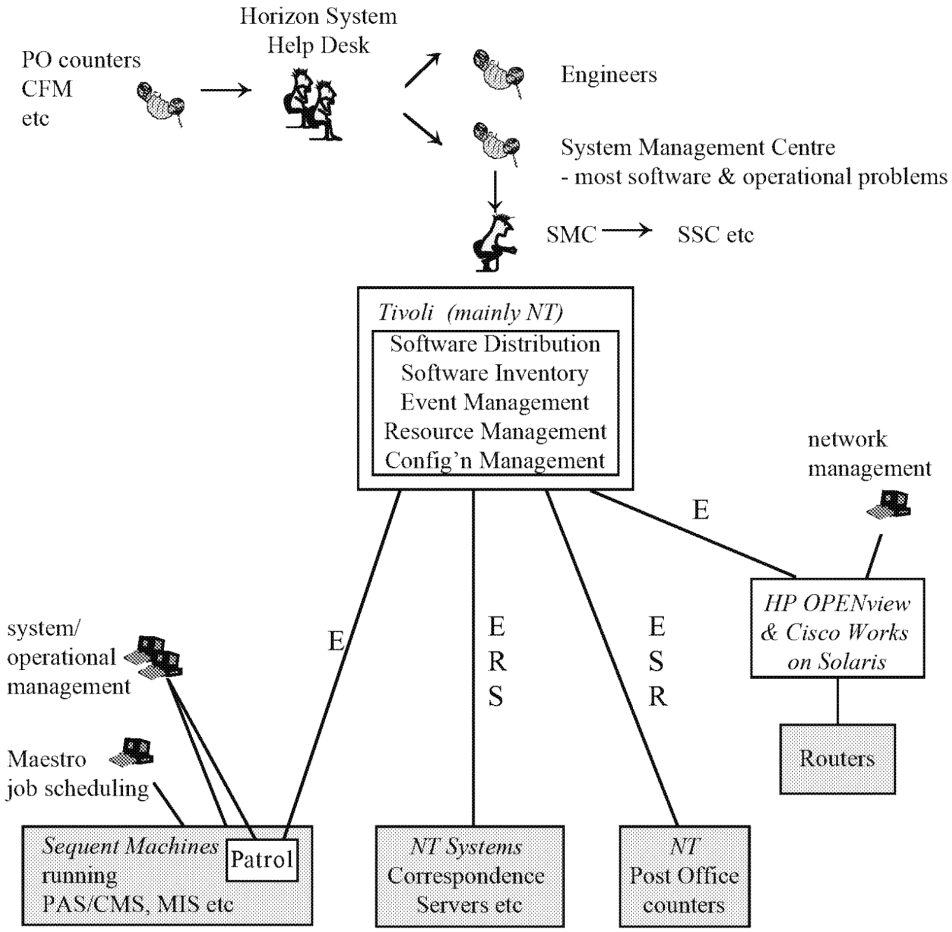

Figure 10 - 1 System Management Service Domain

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 UNIX systems)
- R - shows resource management such as performance and capacity monitoring (for Sequent, inventory management)
- S - shows software distribution

The Tivoli Management Environment (TME) is used to provide 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 all other NT boxes at the Pathway Campus, including Entropy Servers and Key management Service. 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.

Management actions may be initiated by:

- System management software detecting threshold conditions and automatically taking remedial actions.
- SMC System Management staff initiating software distribution or other action via Tivoli scripts.
- Technical Help Desks receiving all technical calls and fronting and managing the handling of these calls
- CFM Staff doing operational management via Patrol (for event/resource management), Maestro (for job scheduling), Oracle Database Administrator functions for Oracle database problems, UNIX or NT directly where needed.

The Technical Help Desks are supported by an existing Sorbus system (Powerhelp) for recording calls and later monitoring them.

This System Management section covers the following:

- Access control at the Horizon System Help Desk and in the Tivoli System Management system including at SMC management workstations.
- Access control for management associated with the Sequent machines using Patrol and Maestro consoles
- Access control in network management - both at the HP Open View workstation and routers.

Rollout of Post Offices affects several other domains so is also included in this section to the extent that it affects the operational Pathway systems.

10.2 Technical Help Desks and System Management

The main interactions of people involved in system management using Tivoli are shown in illustration 10-2.

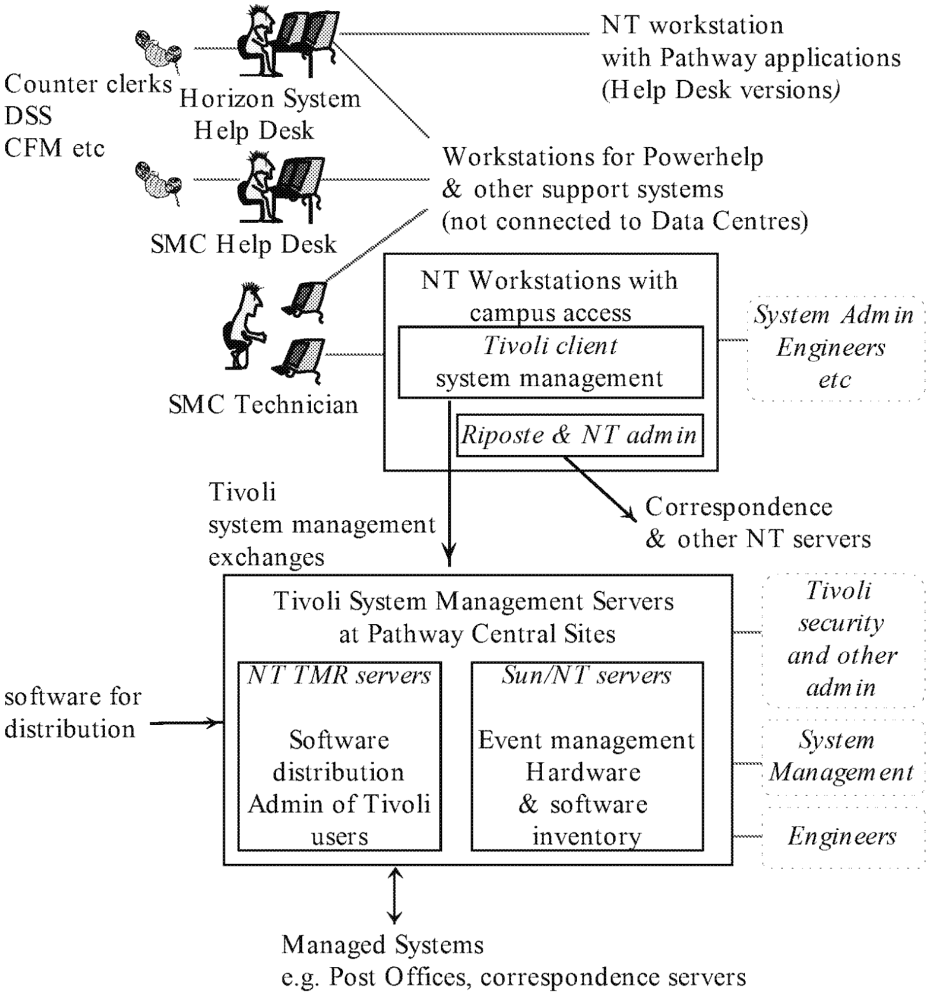

Figure 10-2 Interactions for Tivoli System Management

The Horizon System and SMC Help Desks are co-located and distributed between at least two sites, one of which is at Stevenage. There is also an SMC unit at Lytham St Annes for Tivoli software support.

These Help Desk staff respond to calls from a variety of sources. 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.

SMC technicians handle calls passed to them via Powerhelp but also have access to Pathway operational systems via a second workstation. They monitor and manage Pathway systems using Tivoli and also administer Riposte at the Correspondence servers.

The Tivoli System Management servers are at the Pathway Campus.

10.2.1 Horizon System Help Desk, SMC and Related Roles

This Access Control Policy is concerned with access to Pathway operational and management systems. So the following are **not** covered by this document as they require no access to operational systems:

- Use of the Windows 95 workstations by Horizon System Help Desk staff and SMC for access to Powerhelp, Dispatch-1 etc.
- Use by the Help Desk staff of the Pathway applications on the NT workstations (and associated servers) in support of customer queries.

The following table lists SMC and related roles which are covered by the Access Control Policy.

Role	Functions
Horizon Help Desk technician	Contact on all technical calls, registering them, responding in some cases, and passing the rest on.
SMC Technician - Pathway management (multiple roles) (SMC)	Monitoring & Management of Pathway resources under Tivoli control. Sub-roles separate management functions and regions to be managed (see 10.2.1.1).
SMC Technician - Riposte management	Administration of Riposte in any cases not covered by auto-configuration
SMC Technician - Tivoli Management - multiple roles (SMC)	Configuring Tivoli including controlling data import/export, maintaining inventory of managed systems etc. (see 10.2.1.2)
Tivoli support (SMC, Lytham)	3rd line support of the Tivoli software
SMC Security Management	Maintenance of user information - SMC technicians at SMC NT workstations - Tivoli users at the Pathway campus - NT users at NT systems supported by SMC at the Pathway campus
Pathway Security Auditor	Access to Tivoli notices
Operational management of Tivoli servers (CFM)	Installing and configuring base software when this cannot be done by Tivoli.

10.2.1.1 Pathway System Management using Tivoli is split between different people with responsibility for different functions, and in some cases, for these functions only in particular Tivoli regions. This division responsibility should be in line with the Access Control Policy to provide separation of duties etc as defined in section 3.

The number of roles which can activate unplanned changes to the system should be very limited. Such actions should very rarely be needed and require some separate authorisation. Expected roles include:

- System monitoring of events resources with no update rights.
- System monitoring and confirming action suggested by the system.
- Distributing authorised software, Tivoli scripts etc in line with the planned schedule for activation at a planned time.
- Taking unprompted and unplanned actions as the result of serious problems. In all cases, this should only use authorised Tivoli scripts. In most cases, there should be authorised scripts to handle expected emergencies. Where this is not the case, any new script produced must be authorised according to SMC procedures prior to distribution and use.
- Authorising a new Tivoli script or software patch for release. This will only be done by a senior SMC technician.

10.2.1.2 Management of Tivoli will control:

- The inventory of managed systems
- Configuration information about thresholds to activate alerts, what audit information to generate etc
- Configuration of bulletin boards of notices and who can access them
- Source of data to update Tivoli server information about hardware, software, auto-configuration of Post Offices etc

10.2.2 System Access Controls for these Roles

All these Help Desk and SMC staff are authenticated to the local NT system using a password. Those with access to the Data Centres also use a token. This results in display of a desktop which contains only those applications available to this user.

SMC technicians also authenticate to the appropriate Pathway Operational system.

The residual operational management of Tivoli servers is done by CFM as for other servers at the Data Centre, as specified in section 6, so is not included in the following table.

Role	Workstation type and location	Where user defined and Authentication needed	Resources available
Horizon Help Desk Technician	W95 and NT in DSD area	Local systems only	Call monitoring etc on W95; Pathway related services on NT
SMC technician - Pathway management (multiple roles see 10.2.1.1)	NT - SMC secure area (Stevenage or Footscray)	Local NT system, Tivoli user with appropriate role, regions, ACE server at Data Centre for token authentication.	resources required for that role and region
SMC technician - Riposte management	as above	Local NT user, NT Data Centre user and ACE server for token	Appropriate Riposte management utilities
Tivoli management	as above	as SMC technician for Pathway management above	Appropriate Tivoli functions
Tivoli support	NT workstation, Lytham St Annes	as SMC technician above	All Tivoli functions
SMC Security management	NT at SMC secure site	as SMC technician above	Tivoli user admin
Pathway Security Auditor	NT workstation, secure area, Feltham	Tivoli, NT user at other management system.	Access to audit logs

Note: Use of token authentication have still to be agreed - see 6.9.2..

Note: Procedures for Help Desk handling of one-time passwords in response to calls from the Post office are being defined, as are those for key recovery.

Tivoli roles, management regions and policy regions are used to split system management functions as described in 10.2.1.1 above.

Tivoli roles will also be used to control who can manage/configure which Tivoli functions and resources (see 10.2.1.2). A separate role should be used for the Auditor who can set the amount of auditing and analyse and manage the audit log/bulletin boards.

10.2.3 Controls on Connections

The NT workstations which are used by SMC technicians for managing the operational Pathway system will be on a separate LAN from other workstations at the SMC sites and only these will have access to the Pathway Data Centres.

The links between the SMC sites and the Pathway Campuses are encrypted, so all traffic is confidentiality and integrity protected. (Tivoli integrity features will also be used).

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

10.2.4 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 3.6.2 above.

In outline, authentication of these contacts is as follows:

Contact	Function	How authenticated
Post Office staff	Reporting technical problems	as section 3.6.2 to identify the outlet
Post Office Manager	Key recovery, resetting Manager's password	as above, plus identification of Manager
Engineer, Auditor, Emergency Manager at Post Offices	Use of one-time password as part of log-on; emergency key recovery	As 3.6.2 plus at least pass number checked (see note 2)
Other Pathway sites	Reporting technical problems	As 3.6.2
POCL other sites	Reporting incidents	As 3.6.2
DSS	Reporting software problems e.g. with CAPS, CAS	As 3.6.2

Notes:

1. CLI is used where possible
2. The Help Desk has a record of pass numbers of engineers and POCL auditors, including those who can be Emergency Managers

10.3 Sequent and Oracle Management

The components involved in the management of the Sequent systems at the Pathway Central sites are illustrated in figure 10-3.

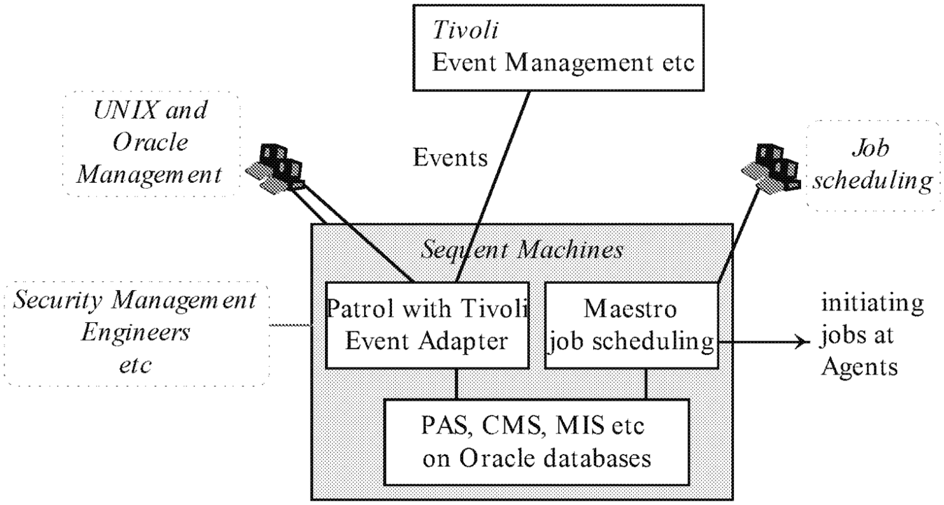

Figure 10-3

Patrol is used for system management of both Dynix and Oracle. (It is expected to be used for all Oracle database administrator functions.) A Patrol knowledge module in the Pathway partition on DSS VME machines adds VME system management events allowing them to be monitored via the same Patrol workstation. Patrol passes on relevant events to Tivoli. The associated workstation is used for monitoring the system and taking any action if needed. 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 6.2 above is used only when the automated management and Patrol cannot cope.

Maestro is used for job scheduling 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.

10.3.1 Roles

System management related functions are:

- Sequent system/operational management including use of Patrol
- Sequent system monitoring via Patrol

- Emergency operational management
- Job scheduling via Maestro
- Job monitoring via Maestro

These roles are all defined in 6.2 as they affect management of the Sequent systems e.g. what users need to be known there. (Further roles associated with the Sequent systems are also defined in 6.2 including Security Management of Dynix and Oracle and Engineers.)

10.3.2 System Access Controls for these Roles

Section 6.2 above defined the controls within the Sequent system.

People carrying out management functions which may update Pathway systems from the remote will need to be authenticated by token.

If CFM management staff working at home is permitted, the PC will be configured in a secure environment to ensure it contains only the required software and to link to ISDN routers which will cause token authentication. Floppy drives will be disabled.

The links between the and Pathway campus will be encrypted.

10.3.3 Control on Connections

The NT workstations used for this access are on a secure LAN at a secure CFM site. The links to the Data Centres are encrypted.

10.3.4 Other Access Controls

Call out of CFM staff is done according to CFM procedures which ensure that the call comes from the required source, so should be acted on. Associated procedures ensure the ISDN port is enabled to allow the authorised access to the system. This utilises Powerhelp.

10.4 Network Management

10.4.1 Introduction

The Pathway network routers are managed using HP Open View with Cisco Works as illustrated in figure 10-4 below.

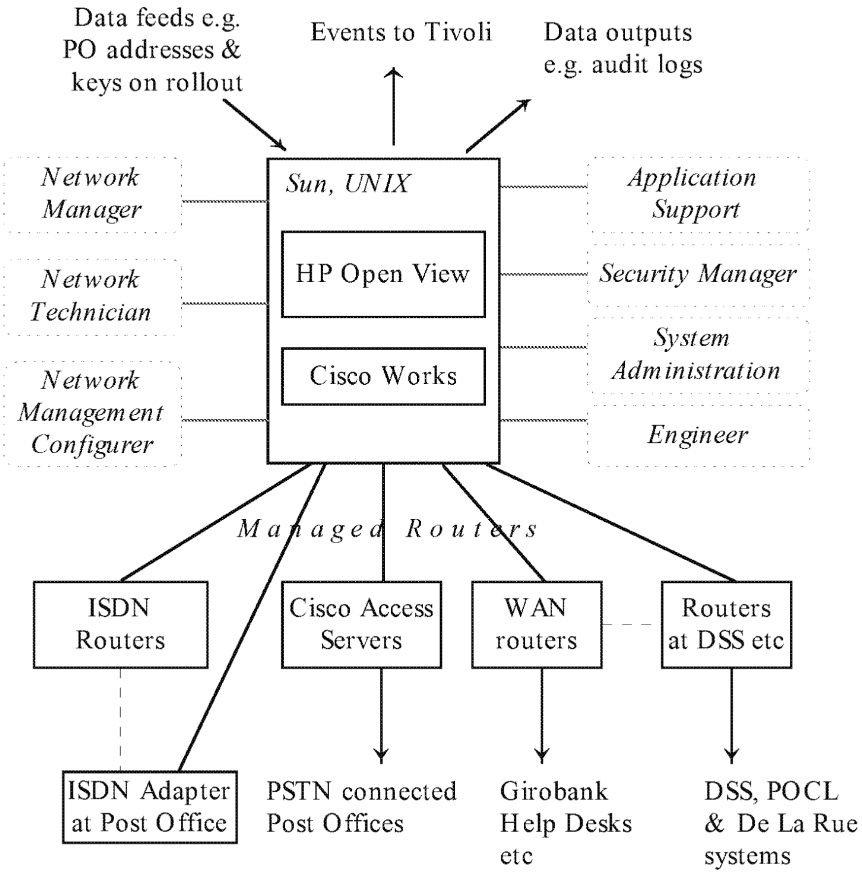

Figure 10-4 Network Management

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 rollout, the (ISDN) addresses of the Post Office to be rolled out soon are fed to the routers, as are the CHAP keys required.

The main roles are:

- 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 System itself, for example, Open View configuration. This role is carried out by the Network Management team before live running.
  The configuration of the network management will be validated by more than one CFM technician and signed off by a senior CFM person before use.

There is a single Network Management station at each Pathway Data Centre. At any one time, the Network Manager role is available at only one of these, with the other being used by a Network Technician for monitoring.

10.4.2 Roles at the Open View System

The following table lists the roles of people with direct access to the system.

Role (Organisation)	Functions
Network Manager (CFM)	Monitoring the network. Updating router configuration information when required e.g. - Post Office information e.g. ISDN addresses - Access Lists of permitted addresses, protocols, ports. Updating information about routers available when needed (including confirming bringing a mended one back on line - see 10.4.4 below)
Network Technician (CFM)	Monitoring the network
Network Management Configurer (CFM)	Configuring Open View - what to display to whom - actions to be taken on certain events etc. 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 (DSD)	Diagnosing, repairing hardware faults

10.4.3 Access Controls associated with Human roles

People in all these roles use the console at the machine for all access to the Network Management System. There are no remote users allowed on this system. The following table shows how the users defined above access the system and what is available to them.

Role	Authentication method & where user defined	Resources available
Network Manager	UNIX & Open View as individual user	Open View and Cisco Works network management functions (no direct UNIX access)
Network Technician	as above	Specified Open View and Cisco Works functions only
Network Management Configurer	as above	Open View configurer functions
Security Manager	as above	User information and audit trails
System Administration	UNIX after system taken out of network	All UNIX facilities
Engineer	UNIX via special password c.f. Sequent systems	UNIX facilities and data required to diagnose fault

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.

10.4.4 Access to Routers

Pathway routers are controlled from the Network Management Service described above. No other remote management of the routers will be done.

The routers will not normally have consoles, though console access will be enabled for cases where a router fault is detected. Any attempt to use console access will be flagged via Open View.

If a router has a fault, it will be configured out of the network and then a console will be 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 Open View 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.

10.4.5 Access controls configured in Routers

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.

10.5 Network Access Controls

10.5.1 Introduction

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

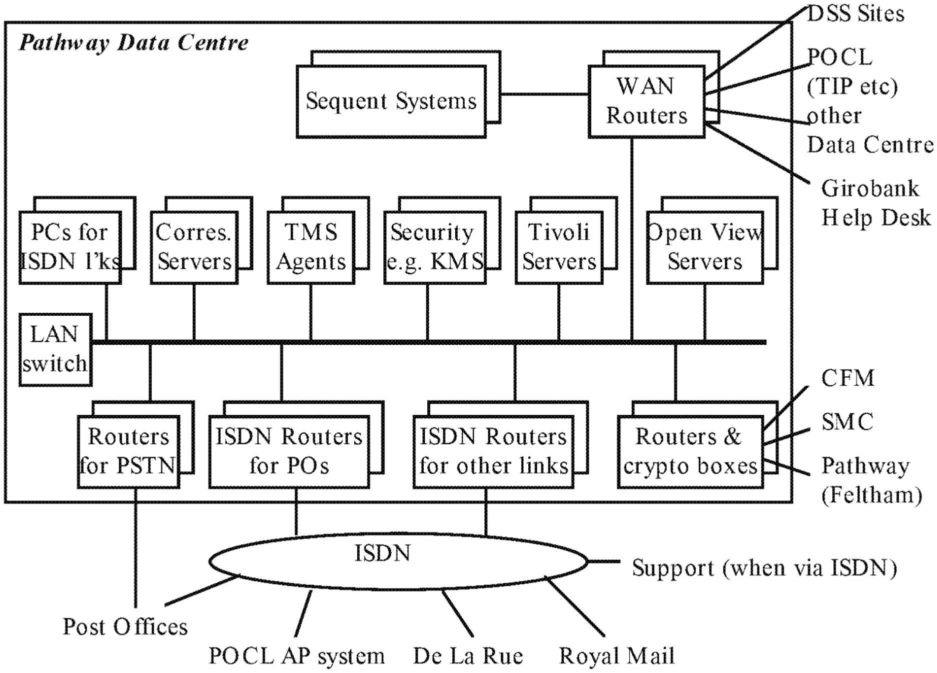

Figure 8-5 The Pathway Data Centre Network

Note that the above diagram does not show the Energis backbone, or the duplication of connections within the Data Centre for resilience as these do not affect the access control policy.

There are the following connections into a Data Centre:

- High speed WAN links, e.g. from CAPS, coming into the router which is linked to the Sequent machine (Bootle) or machines (Wigan)
- Post Offices connected via ISDN to ISDN Routers or via PSTN to other routers
- Other ISDN connections such as to the POCL system at Farnborough which handles Automated Payments coming into other ISDN routers
- The links from Pathway sites used to manage and support the operational and management systems.

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

Note: Configuration of the routers and positioning and configuration of the firewalls is still being discussed and is subject to change.

10.5.2 High Speed WAN links

The following systems connect into the Pathway Data Centres by high speed WAN links:

- The DSS CAPS and ESNS sites
- The POCL TIP and Reference Data systems
- The Girobank Help Desks at the campus
- The other Data Centre

All these links come into a pair of routers which do not accept traffic from any other source outside the Data Centre.

At the Bootle site, where there is no Data Warehouse or MIS machine, all traffic to and from these connections goes to the one operational Sequent system.

The type of traffic permitted to/from the DSS and POCL systems are controlled by firewalls at the DSS and POCL sites (see sections 4 and 5).

The Girobank Help Desk uses only Oracle Forms access to Sequent (see 7 above). The Help Desk workstations are set up to use only this access to the Data Centres and the Sequent systems to accept only this.

10.5.3 Post Office Connections

Post Office are normally connected via ISDN, though some are connected via PSTN or GSM.

A set of routers handle all ISDN traffic from Post Offices and accept traffic from outside the Data Centres only from those. Further routers are configured to handle traffic from PSTN connected Post Offices.

The routers handling Post Office traffic also restrict where traffic can be routed to/from within the Data Centre. Permitted addresses are for those services listed in 8.3 i.e. the Correspondence Servers, Tivoli management servers and KMS.

10.5.4 Other ISDN Connections

All ISDN access to the Data Centres is protected by routers which only permit traffic to/from agreed sources. Apart from the Post Offices, ISDN connections are permitted with the following systems:

- The POCL site at Farnborough handling automated payments (and in future other POCL clients)
- De La Rue sites
- The Royal Mail (Wigan only, post release 1)

- In some circumstances, certain support organisations such as Sequent and Oracle

The POCL, De La Rue and Royal Mail ISDN links go to a different set of ISDN routers than those used for the Post Offices. These only permit traffic from outside the Data Centres from these addresses. Each of these links have associated PCs at the Data Centre to handle traffic on that link. The routers restrict traffic from these links to the appropriate PCs. Traffic is restricted to file transfer and Tivoli management - see sections 5 and 9.

As for the DSS and other POCL sites, the type of traffic permitted to/from the POCL, De La Rue and Royal Mail systems are controlled by firewalls at the remote site (see sections 4 and 5).

In exceptional circumstances, support of Dynix and Oracle on Sequent machines may be required from Sequent and Oracle. Remote access will only be permitted after a call from the Operational Management of that machine confirms the need for access and tells the Network Management staff to configure the appropriate router to permit that access. In this case, the router will be configured to restrict access to the Data Centre to the particular Sequent system needing supporting.

All traffic over these ISDN links is protected at the application level as defined in the Security Functional Specification.

10.5.5 Links from ICL Pathway related Sites

A number of ICL sites need access to the Data Centres as follows:

- The CFM sites at Belfast and Stevenage
- SMC sites at Stevenage, Footscray and Lytham.
- The Pathway management site at Feltham which is also used for Configuration Management, rollout, some support and FRM.

All these links are low speed ones and encrypted (using cryptographic boxes) and linked into a particular set of routers.

These routers only permit traffic from/to these locations. At CFM and SMC sites, the workstations used are not connected to any external network so do not need firewalls. Traffic to/from these sites is as described in 6.2, 10.2 and 10.3 above.

The Feltham site has links to a number of sites as it accepts some software and rollout information from other parts of ICL and other organisations. The network is shown in the following diagram.

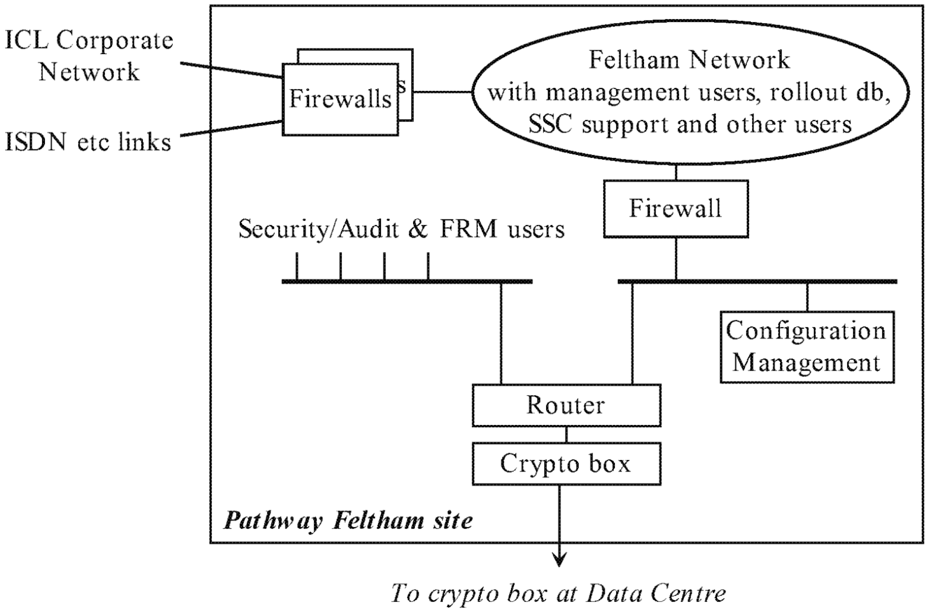
ICL Corporate Network
ISDN etc links
Firewalls
Feltham Network with management users, rollout db, SSC support and other users
Firewall
Security/Audit & FRM users
Configuration Management
Router
Crypto box
Pathway Feltham site
To crypto box at Data Centre

Figure 10-6 Feltham Network

The connections between Feltham and the Data Centres are:

- Pathway Fraud Risk Management staff and Security Auditors from a secure LAN in a physically secure area
- Distribution of signed software and Tivoli scripts from the Configuration Management system
- Supporting rollout including transfer of Post Office information between the rollout database and Data Centre
- Management users accessing management data
- SSC application support

The Feltham router will permit traffic from the FRM users and CM system and also the firewall to the Data Centre.

The main Feltham network is protected from the ICL Corporate network and ISDN lines from which rollout information is received by firewalls.

A further firewall protects the Data Centre from the Feltham network (and translates the IP addresses to Pathway addresses). This firewall restricts traffic to the Data Centre to only those workstations and servers with a need to access it and restricts the type of traffic to that permitted.

However, this does not control where at the Data Centres this traffic can go this is done by routers at the Data Centres.

10.5.6 Network Access Controls within the Data Centres

Other sections of this document identify what connections are allowed at the various systems in the Pathway Network to allow both the automated processing of the business applications and also management and other access. Some of these controls are enforced by the routers, some by controls at the particular systems.

The routers controlling the links from CFM, SMC and Pathway project staff at Feltham will be configured to have the following controls

- CFM from Belfast can only access the systems they manage
- SMC can access Tivoli servers and NT boxes managed by them (see 6.3)
- SSC application support users at Feltham 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 Tivoli server

Controls of use of ports at particular systems are generally specified as part of the particular system. In outline:

- Correspondence server access is limited to the TMS agents, and routers handling traffic from the Post Offices (apart from management and support access).
- TMS Agents only allow traffic to/from Correspondence servers and the appropriate Sequent system(s), except the BES agents which also have links with the Entropy servers (apart from management and support access).
- Security servers control connections to restrict access to the minimum required, though note that this will include routers linking to the Post Offices.
- PCs handling links with outside systems will restrict traffic to only those types of applications permitted on the specific ports from the specified addresses.
- Tivoli servers allow different connections depending on the function
- Open View servers allow no outside access and permit links only to the routers.
- The Sequent operational system permits only those connections listed in sections 6 and 7 e.g. CAPS, ESNS, TMS agents, PAS/CMS Help Desk, operational management.
- The Sequent Data Warehouse and MIS systems permit access to management users, but only FRM staff (and in exceptional circumstances application support staff) are permitted to access the Fraud Management Service.

10.6 Roll-out

This Access Policy is concerned only with those parts of the Rollout mechanisms which affect the operational system. This is illustrated in figure 10-7.

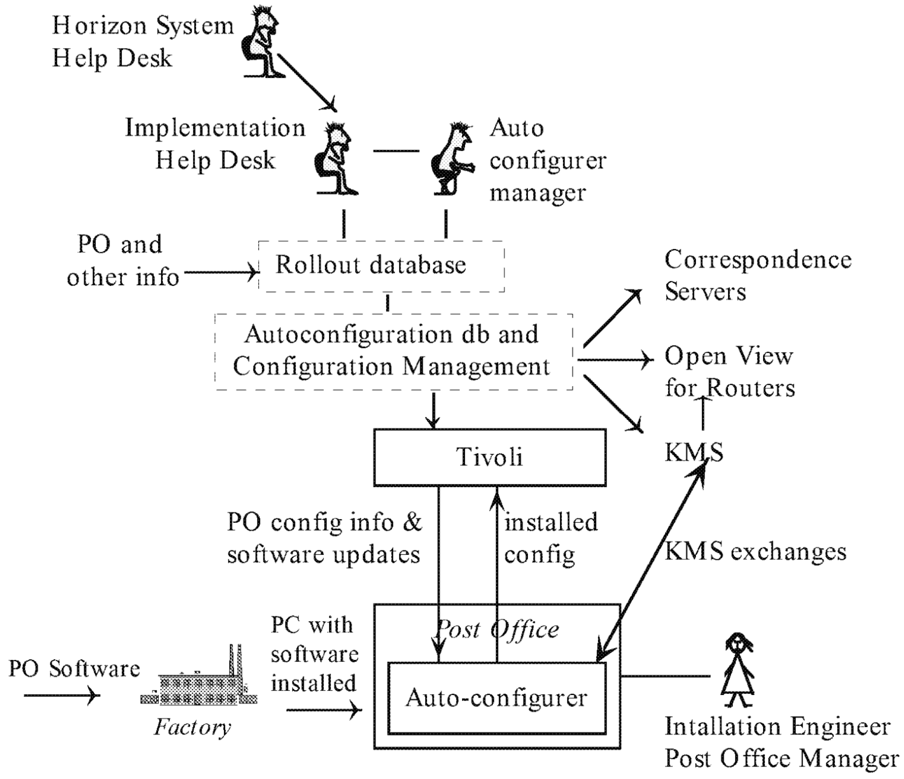

Figure 10-7 Interactions on Roll-out

The information needed to implement roll-out of Post Offices is managed in the Roll-out database which takes input from POCL and other sources.

Information about Post Offices to be installed soon is transferred to the Pathway Auto-configuration database. A member of the Implementation Operations Unit in Pathway initiates the Auto configurer 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 signed by the Configuration Management system and sent to Tivoli to distribute as for all Tivoli script and software updates to the Post offices.

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, any changes needed to the software are sent to the Post Office and the details of the installed configuration returned to Tivoli. When the Post Office Manager takes over and first boots up the Post office, the keys for standard running are delivered from the KMS.

10.6.1 Roles

There are two Implementation Operations Unit roles to support Rollout:

- Implementation Help Desk technician
- Auto-configuration Manager

The Horizon System Help Desk forwards relevant calls to the Implementation Help Desk. The technicians there will handle the call, communicating with Pathway suppliers. The Rollout database may be used both to respond to queries for information and to update it, for example, if an installation date must be changed

The Auto-configuration Manager controls the auto-configuration process. This may be split, so updates to Correspondence servers and routers etc are done at different times from generating the Post Office configuration file.

As the Rollout database and Configuration Management system are internal Pathway Services at Feltham, this Access Control Policy does not define the access controls for these roles.

11. PATHWAY CORPORATE SERVICE DOMAIN

11.1 Introduction

The Pathway Corporate Services Domain supports:

- Management processes using Management Information Systems.
- Security processes including Fraud and Risk Management and Security Auditing.

11.2 The Management Information Systems (MIS)

There are two Sequent platforms at the Data Centre at Wigan supporting Management Information Services. The Data Warehouse is the main information repository for all Pathway corporate systems. A second MIS platform supports an EIS and Financials service utilising information from the Data Warehouse. Both systems are managed in the same way, so have similar access controls.

These MIS and Fraud Risk Management services are illustrated in figure 11-1.

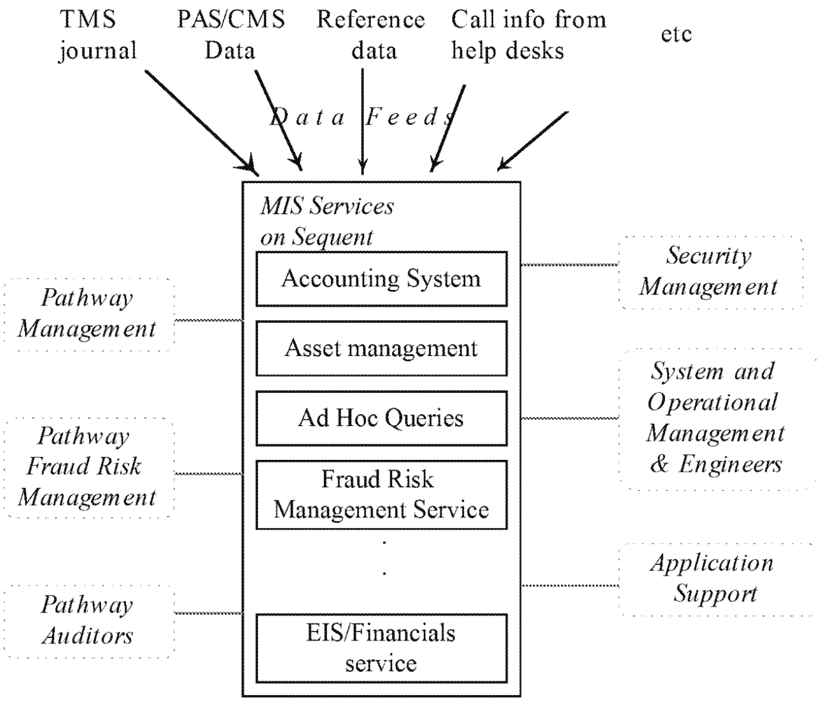

Figure 11-1 MIS Systems at Wigan

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
- 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 6.8).
- Data from the Reference Data Management System (see 6.7)
- PAS/CMS data (see 7.2)
- Information on calls to the PAS/CMS Help Desk. This consists of Rockwell ACD data (see 7.3) 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 from 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.

All business access to the EIS/Financials service it is by Pathway Management users in Feltham using SQL*Net.

11.2.1 Roles

The roles specific to these MIS systems are:

- Pathway Management staff at Feltham running the various management services.
  Some of the data these people handle is commercially sensitive for Pathway (e.g. financial information). Other data may be sensitive for DSS and/or POCL.
- Pathway Security Auditors
- Pathway Fraud Risk Management staff responsible for identifying and managing fraud (Data Warehouse only)

Both systems are managed in a similar way to the other Sequent systems at the Pathway Data Centres. Therefore people in the following roles defined in 6.2 are also supported here.

- Computer operator (CFM)

- Operational Management (CFM)
- Security Management (CFM)
- Oracle 3rd line support (Oracle)
- Dynix 3rd line support (Sequent)
- Engineers (Sorbus)

For a definition of these roles and how they access the system, see 6.2.

Application support is similar to the applications on the operational Sequent systems i.e. SSC provide 2nd line support for all applications and the application supplier provides 3rd line support. In this cases, this is:

- Oracle for all Oracle applications
- CFM for Business Object applications used to support queries on the data

11.2.2 System Access Controls

System access controls will conform to the policies in 3.5.2. For example, all users are individually authenticated and their access to the system is limited on a need-to-know basis.

Database roles with appropriate database views will be used to separate what data is available for what use. Information available to people doing ad-hoc queries will be further constrained using the Business Object "universes" to provide restricted views of the Data Warehouse.

These controls will be used to separate data available to different Pathway management roles.

Fraud Risk Management will have access to individual customer information relating to fraud as well as benefit related transactions and data. Because of this, Fraud Risk Management staff will be located in physically secure areas.

Data Warehouse or MIS specific Role	Workstation & location	Where users defined & authentication	Resources available
Pathway management (ICL Pathway)	NT or Windows '95 in Feltham (see note 1)	Oracle	Data relevant for specific service only.
FRM (Girobank)	NT at secure area in Bootle	Oracle plus token	FRM database
FRM (ICL Pathway)	NT at secure area in Feltham	Oracle plus token	FRM Database
Security Auditing	NT at secure	Dynix + token	Audit logs

(ICL Pathway)	area in Feltham		

The Data Centre is protected from these terminals as described in section 10.5 above.

11.2.3 Control of Connections

All access to the Data Warehouse from outside the campuses is by encrypted links.

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

11.3 Pathway Fraud Risk Management

Fraud Risk Management is concerned with identification, monitoring and management of fraud associated with/relevant to the ICL Pathway system. This is generally done using the Fraud Risk Management Service described in [FRMS].

There are two groups of Pathway people involved in Fraud Risk Management:

- Girobank Fraud Risk Management (FRM) staff at Bootle
- ICL Pathway FRM staff at Feltham

Both are small groups and have access to the same information.

Most FRM access to Pathway is to the Fraud Risk Management Service as described in 11.2 above. In exceptional circumstances, FRM staff may require access to other Pathway systems in order to investigate a potential fraud. Access is currently expected to be needed to:

- The PAS and CMS data
- The TMS journal of Post Office activity
- Data transfer logs

Access to PAS, CMS and TMS data is expected to be mainly to the archives, not the operational system except in exceptional circumstances. More detail of this access is given in the sections about the systems being accessed.

FRM staff at Feltham access systems at the Pathway Data Centres from a secure area via an encrypted link. They authenticate themselves using tokens.

11.4 Security Management and Auditing

The POCL and DSS 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.

Pathway Security Management are responsible for:

- Security Auditing of Pathway
- Cryptographic keys used in Pathway
- Responding to requests under the Data Protection Act.

Security Auditing is concerned with auditing all access to the Pathway systems, including that by Pathway operations and management staff. Because of this, Pathway Security Auditors will be separate from other Pathway management roles. The main activity will be a monitoring one, though on occasions, more active investigations are expected.

Pathway Security Auditors will access audit logs generated at many Pathway machines. This includes:

- Operational application logs such as the Riposte journal which records events at Post Offices and the PAS and CMS logs (including records of PAS/CMS Help Desk transactions)
- Management logs, normally at the Data Warehouse
- System Management audit logs
- Logs recording system level activity such as user logon and administration (when done by at system level) and other security relevant events
- Logs at some of Pathway's internal systems such as Configuration Management.

However, the Security Auditor will not have access to:

- Post Office systems as all Post Office transactions (including user administration and authentication as well as business transactions) are recorded in the TMS journal, or
- The PAS/CMS Help Desk systems as all interactions of the Help Desk users with the Pathway systems will be recorded in the Oracle logs at the Sequent machines.

Note: More detail of audit access will be provided when the Audit design is available.

11.4.1 Security Management Roles

People in the following roles are all part of the Pathway Security Management organisation.

Role	Main Functions
Pathway Security Auditor	Using the audit logs in most Pathway systems to monitor and analyse use of the system.
Pathway Security Manager	Responsible for cryptographic keys (though installing keys is done by the Post Office Manager at Post offices and by the cryptographic key Custodian at other platforms.)
	Obtaining the required information in response to requests for subject information under the Data Protection Act.

11.4.2 System Access Controls

The Security Manager and Auditors (and FRM staff) at Feltham access systems at the Pathway Data Centres from NT workstation in a secure area on a secure LAN via an encrypted link. They authenticate themselves using tokens.

Security Auditors can access logs at most Pathway systems as described in 11.4 above and are registered at each system accessed. More information on their access is given in the appropriate section about the systems being accessed.

At each system, the Auditor has access only to the audit logs there. Logs are separated from other information using the facilities of the software generating/accessing them. For example, operating system logs are in separate files/directories, Oracle logs are available via separate views.