POL00400795

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.

This version has been extensively restructured in line with previous discussions - focusing on policy and exceptions, so taking out descriptions, some details (particularly on networks) and roles by machine (though the complete role list has been left in). It has been reduced very significantly in size.

This is a first draft with the revised structure for comment - technical content has not yet always been revised, and will be before wider distribution.

Distribution:

Alan D'Alvarez
(John Dicks)
Peter Harrison
Dave Jones
Tom Parker
Barry Procter
Geoffrey Vane?
Peter Wiles
Frank Fallon?
Dave Tanner?

Document Status: First Draft with revised document structure

Document Predecessor: -

Associated Documents: See section 0.3

Author: Belinda Fairthorne

Approval Authority: John Dicks

Signatures/Dates:

Comments To: Author, copy to John Dicks, Dave Jones?

Comments By: -

0. CONTENT

0.1 Document History

Version	Date	Reason
0.1- 0.5	28/10/96 6/12/96	Initial drafts building up to first full version including responses to comments
0.6	4/3/97	Further clarifications in many areas
1.0	16/4/97	Terminology changes, major updates to the Post Office section and numerous minor changes
1.1/3		See separate note
2	23/2/98	Approved version of 1.3
2.1, 2.2	sep/oct 98	See separate note for technical changes; Approval responsibility passed to John Dicks
3.0	dec '98	Approved version of 2.3 which had minor updates
3.1	may '99	Re-organisation and change to focus on policy, taking out most descriptive text; See separate note for changes and issues.

0.2 Approval Authorities

Name	Position	Signature	Date
John Dicks	Customer Requirements Director		

0.3 Associated Documents

Ref:	Title	Identifier	Vers.	Date
SADD	Service Architecture Design Document	CR/FSP/004	5.1	23/7/98
TED	Technical Environment Description	TD/ARC/0001	4.2	13/10/98
SPOL	ICL Pathway Security Policy	RS/POL/0002	3.3	23/2/98
SFS	Security Functional Specification	RS/FSP/0001	3.2	5/8/98
NET	High Level Network Design, NR2 &2+	TD/DES/059	0.5	10/5/99

0.4 Abbreviations

ACP	Access Control Policy
BA	Benefits Agency
BES	Benefit Encashment Service
BPS	Benefit Payment Service
CAPS	Customer Accounting and Payments System
CAW	Certification Authority Workstation
CESG	Communications-Electronic Security Group
CFM	ICL Outsourcing (Client Services Ireland)
CLI	Calling Line Identification
CMS	Card Management Service
CS	Pathway Customer Services

DBA	Database Administrator
DSA	Digital Signature Algorithm
DSS	Department of Social Security
ECCO	Electronic Cash Registers at Counters
EPOSS	Electronic Point Of Sale Service
ESNS	Electronic Stop Notice System
FCMS	Fraud Case Management Service
FRM	Fraud and Risk Management
FTMS	File Transfer Management Service
HAPS	Host Automated Payment Service
HFSO	Horizon Field Support Officer
ISDN	Integrated Services Digital Network
IT	Information Technology
KEK	Key Encryption Key
KMA	Key Management Application
LAN	Local Area Network
MIS	Management Information Services
NAO	National Audit Office
NMS	Network Management Station
NSI	National Sensitive Indicator
NT	New Technology (Microsoft's operating system)
OBCS	Order Book Control Service
PAS	Payment Authorisation Service
POCL	Post Office Counters Ltd
PUN	Pick Up Notice
RDMC	Reference Data Management Centre
SMC	System Management Centre
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSC	System Support Centre
TACACS+	Terminal Access Controller Access Control System +
TIP	Transaction Information Processing
TME	Tivoli Management Environment
VME	Virtual Machine Environment
VPN	Virtual Private Network

0.5 Changes Forecast

Further changes may be needed as the design of Pathway develops for new services. Also, in the following areas, the current document needs further checking.

- Cryptography/key management
- Some details of support from remote sites e.g. EMC
- Telephone authentication procedures
- SMC 2nd application support (possible read only access to more systems)

- System admin/support at remote sites with FTMS links e.g. De La Rue

0.6 Table Of Contents

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

1. INTRODUCTION

1.1 Purpose

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

Effective control depends on:

- Understanding the information in the system and what access to it should be permitted, and where it is vulnerable, and
- Having a clear definition of the roles and responsibilities of all personnel who need some form of access to the system, and
- Setting access policies and controls to provide the required access while countering the threats and vulnerabilities.

1.2 Context

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

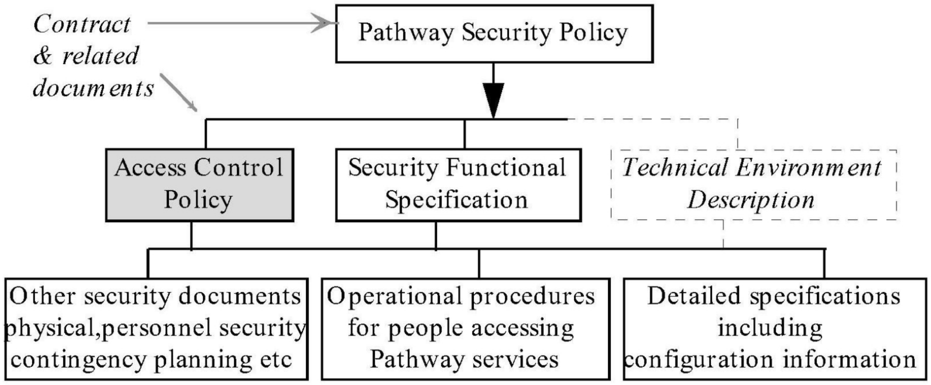

Contract & related documents
Pathway Security Policy
Access Control Policy
Security Functional Specification
Technical Environment Description
Other security documents physical,personnel security contingency planning etc
Operational procedures for people accessing Pathway services
Detailed specifications including configuration information

Figure 1 - 1 Pathway's Security Documents

The ACP defines the policies for controlling access to the Pathway IT system in compliance with the Pathway Security Policy.

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

The Technical Environment Description (TED) describes the architecture and technical environment for the Pathway solution.

Other documents define related policies, procedures and processes, for example, for the physical security of information, and the procedures for entering a site, using the system, safeguarding of manual records and handling security incidents. There are also specifications defining how the various Pathway components are configured. Many of these documents need to comply with the ACP as described in 1.5 below.

1.3 Scope and Document Structure

This Access Control Policy defines how access to information system resources is controlled in the Pathway solution. It covers the Pathway Data Centre systems, Pathway managed systems such as interface systems at POCL sites and closely related Pathway project systems. Access may be the result of direct user action, or automatically initiated activities..

The ACP contains:

- An outline of the services, the roles of the people and the sites used in the Pathway solution (Chapter 2)
- The access control policies for the whole of Pathway, covering policies for authentication, information access within systems, system set-up and network access etc (Chapter 3)
- Specific access controls for human users - where the policies in Chapter 3 are specialised for particular user roles or there are exceptions to the general policies (Chapter 4)
- Specific access controls for particular systems - specialisations and exceptions to the policies in Chapter 3 (Chapter 5)
- A complete list of Pathway human roles and an overview of the IT access permitted to each of these (Chapter 6)

This document specifies the access control policies, not detailed procedures for configuring and running these systems.

Separate internal Pathway documents also cover system development and test systems and other activities prior to the handing over of the software for operational use.

1.4 Access Control Policy Review

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

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

1.5 Effect on other Pathway Standards and Procedures

This Access Control Policy defines the policy for controlling access to resources in the operational Pathway system. As explained in section 1.2, other documents detail 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:

1.5.1.1 Configurations documents should define how systems are configured to conform to the ACP, for example, how the roles defined here are set up to restrict access as required.

1.5.1.2 The roles defined in the ACP should be used in other standards and procedures, not just information system controls. For example,

- 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 formally registered and 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.

1.5.1.3 In some cases, access controls require a combination of manual processes and IT controls, and so procedures need to conform to the ACP. For example:

- Pathway (and associated) staff visiting other sites must have a identity pass with photograph and signature. (see section 3.3.3)
- Post Office procedures for administering users, physically protecting tokens and passwords and authentication to Help Desks etc should conform with the ACP.
- Help Desk procedures should conform to the ACP policies for authentication of Help Desks to caller and vice versa (see 3.4.4)
- Support procedures should specify the authorisation processes for making any updates to the system (code and data) and the procedures, and related controls for calling in external support in line with the ACP. (See, for example, 4.6.2 and 4.6.3)

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

2. OUTLINE OF SERVICES, ROLES AND SITES

The Pathway system can be described from different views as follows:

- The operational systems and their business users.
- The business management users of the system, including security, auditing and fraud risk management.
- Implementation systems used during rollout of new Post Offices.
- System & operational management and support.

This chapter gives an outline of the people and systems involved as a context for the policies and roles described later. It is not intended as a complete description of the system - for that, see [TED].

2.1 Operational Services and their Main Users

The operational systems and their main business users and sites are shown in the following diagram.

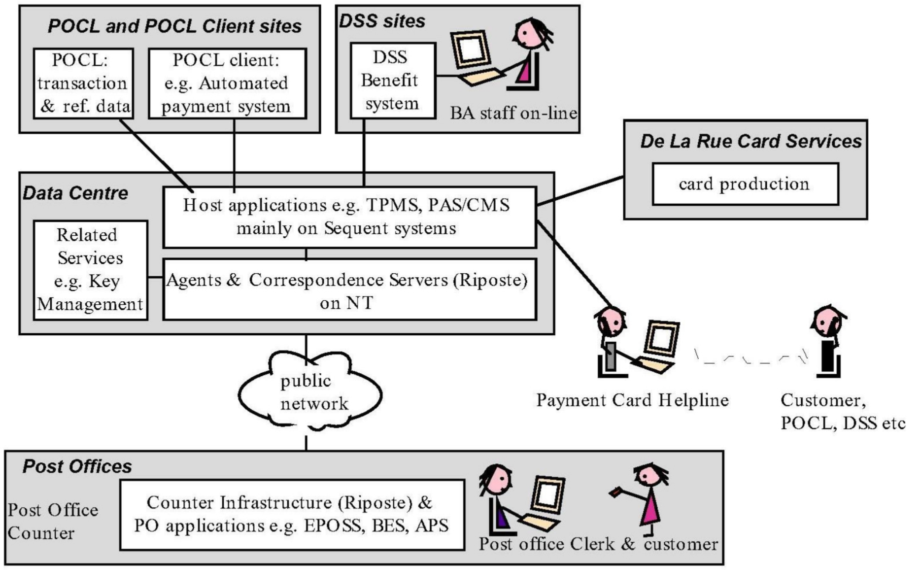

POCL and POCL Client sites
POCL: transaction & ref. data
POCL client: e.g. Automated payment system
DSS sites
DSS Benefit system
BA staff on-line
De La Rue Card Services
card production
Data Centre
Host applications e.g. TPMS, PAS/CMS mainly on Sequent systems
Related Services e.g. Key Management
Agents & Correspondence Servers (Riposte) on NT
public network
Payment Card Helpline
Customer, POCL, DSS etc
Post Offices
Post Office Counter
Counter Infrastructure (Riposte) & PO applications e.g. EPOSS, BES, APS
Post office Clerk & customer

Figure 2 - 1 Main Operational Systems

2.1.1 Services, Systems and Interactions

Information is sent from POCL (reference data), DSS (payment authorisations) and other POCL Clients to the Pathway Data Centres. DSS data may require new cards to be produced by the De La Rue card services. Most of this data is also forwarded to relevant Post Offices for use by applications there. Transactions at the Post Offices are recorded at the correspondence servers and forwarded to POCL and/or DSS and other POCL clients as relevant.

At the Data Centres, the main applications are on Sequent/UNIX systems, but the agents and correspondence servers which handle distribution of information to and from the Post Offices are on NT servers, as are most of the supporting systems such as the key management systems. Post Office Systems are also NT.

Apart from at the Post Offices, all activities are automated in normal circumstances, so there are no business users.

2.1.2 Roles

At the Post Office, operational roles are the **Post Office Manager**, **Supervisor** and **Counter Clerk**. These should be taken as also referring to the equivalent staff in franchises and Sub Post Offices including Sub Postmasters and their staff.

Payment Card Helpline Advisors respond to DSS, POCL and general public queries about benefit cards and payments. PCHL users are located at the Data Centre sites, so considered local, not external users.

Some DSS/BA staff access the Pathway system via DSS systems and then the on-line CAPS interface to PAS/CMS. To Pathway, they appear as system, rather than human, users.

2.2 Business/Corporate Management

Pathway corporate management users and the systems they use are shown in the following diagram:

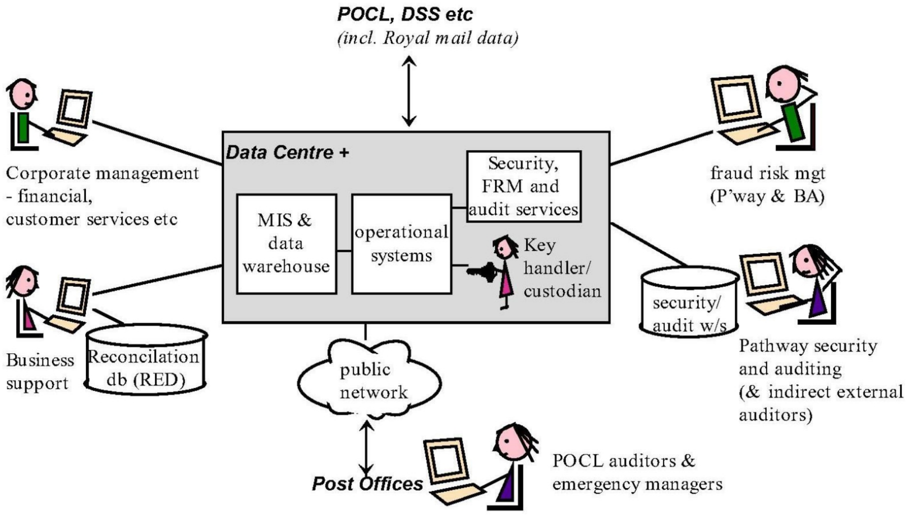

POCL, DSS etc
(incl. Royal mail data)
Data Centre +
Security, FRM and audit services
MIS & data warehouse
operational systems
Key handler/ custodian
Corporate management - financial, customer services etc
fraud risk mgt (P'way & BA)
Business support
Reconcilation db (RED)
security/ audit w/s
Pathway security and auditing (& indirect external auditors)
public network
Post Offices
POCL auditors & emergency managers

Figure 2.2 Corporate Management

2.2.1 Services and Systems

Corporate management services provide management information on Pathway's operation and analysis and reporting of this. Systems include:

- A Data warehouse (Sequent system) which takes input from many Pathway and related systems (including Royal Mail information about card distribution and BT & Mitel information about help desk calls).
- Related MIS systems, including a separate SLAM (Service Level Agreement) cache on NT and a financial system at a separate site.

The Data warehouse/MIS systems at the Data Centre support a number of services including Contract Management, Accounting and Asset Management and a Fraud Case Management System.

There are also Security Specific Services including an Authentication Service for security token users and key management services. Keys need to be installed at the Data Centre and also interface PCs at other sites.

2.2.2 Roles

The main roles are:

- A range of **Pathway corporate management** roles e.g. financial management, contract management and associated support roles.
- A number of Pathway customer service roles such as **Business Support** supporting business operations such as financial reconciliation of payments and **Reference Data** roles for maintaining reference data.

- **Fraud and Risk Management** (FRM) identifying, monitoring and managing fraud, particularly in benefit payments. This includes both Pathway FRM people and the BA Security unit at a DSS site.
- **Pathway Security Management** managing security tokens for Pathway users, and acting as the **Pathway Cryptographic Key Manager,** responsible for generating and distributing keys all cryptographic keys used in Pathway to protect communications links, digitally sign information and encrypt filestore.
  The Key Manager will delegate some responsibility for installing and updating keys to Pathway **Cryptographic Key Custodians** and **Cryptographic Key Handlers.**
- **Pathway Auditors:** both a **Business Function Auditor** responsible for general auditing of the Pathway system (focusing on business, rather than security, auditing) and a **Security Event Auditor** responsible for auditing all use of the Pathway systems. Both types of auditor access information at many Pathway systems
- **POCL Auditors, Investigators** and Emergency Managers who can access services at Post Offices.

POCL, DSS and NAO Auditors also have indirect access to audit information at the Data Centres, but via Pathway Auditors, rather than direct access to the Pathway systems.

2.3 Implementation

The main people and systems involved in implementation of new Post Offices are shown in the following diagram.

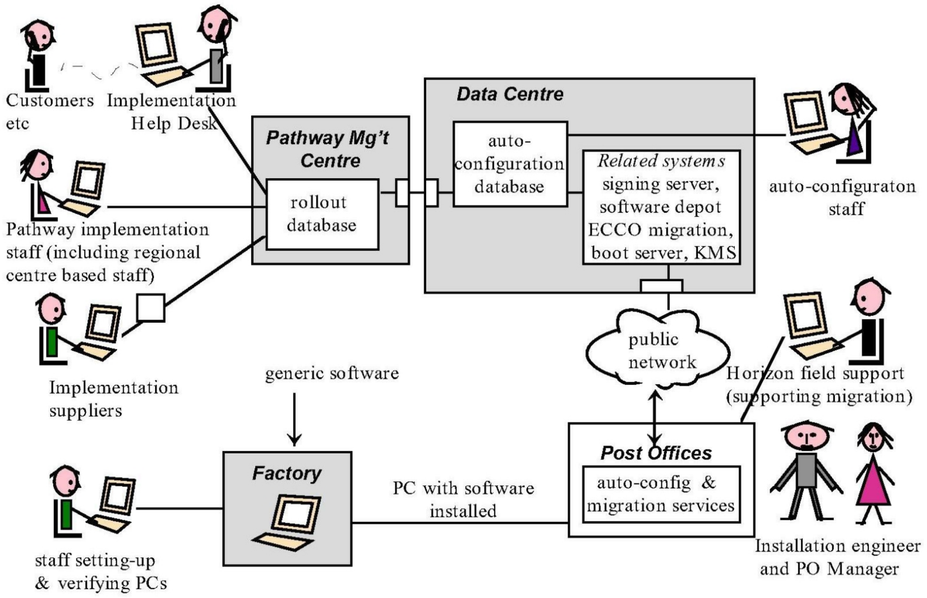

Customers etc
Implementation Help Desk
Pathway Mg't Centre
rollout database
Data Centre
auto-configuration database
Related systems
signing server, software depot ECCO migration, boot server, KMS
auto-configuraton staff
Pathway implementation staff (including regional centre based staff)
Implementation suppliers
generic software
public network
Horizon field support (supporting migration)
Factory
PC with software installed
Post Offices
auto-config & migration services
staff setting-up & verifying PCs
Installation engineer and PO Manager

Figure 2.3 Implementation services and people

2.3.1 Services and Systems

The rollout database contains information about Post offices where Pathway is to be implemented, for example, Post Office details, the state of the site and their staff training.

Configuration information comes mainly from the auto-configuration system and is used in the initial set-up of the Post Offices, updating the generic set-up of the counter systems as delivered. The autoconfiguration process is very largely automated.

Migration from current paper or electronic systems is also supported.

2.3.2 Roles

The main roles here are:

- The Implementation Help Desk
- Pathway implementation staff supporting the implementation process mainly from regional offices, but also Pathway project sites.
- The staff responsible for autoconfiguation, who may need to amend information in certain circumstances
- Horizon Field Support staff handling migration of existing PO systems to Pathway

  In addition, there are implementation suppliers responsible for training, site surveys, installation etc (who use bulk transfer, not interactive access to the rollout database) and the people who set-up and verify the PCs in the factory.

2.4 System & Operational Management and Support

The main people and systems are shown in the following diagram:

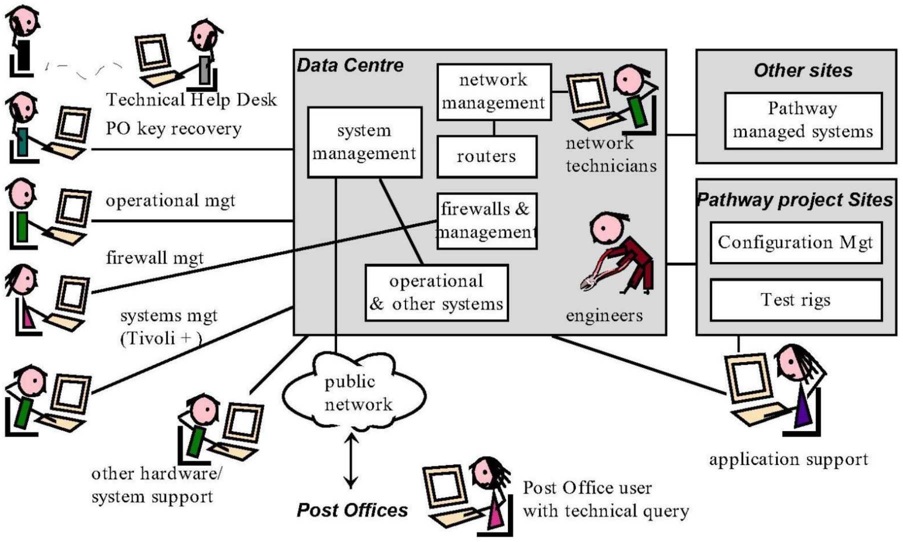


Figure 2.4 System management & support

2.4.1 Services and Interactions

System and operational management and support users manage and support the Post Offices, systems at the Data Centre (including routers and firewalls) and Pathway managed systems such as the interface PCs at POCL and De La Rue.

The help desk handles all technical calls from POCL, DSS and other Pathway users including those from the Post Office requiring key and password recovery services.

Pathway project sites include a Configuration Management system for software to be distributed to Pathway systems, including Post Offices. There are also test rigs used by application support staff for detecting and fixing bugs.

The technical help desk and system/operational management and support staff also use internal Pathway/ICL services such as the Powerhelp and PinICL systems for recording, progressing and monitoring calls to the help desk.

Note that many of the system and operational management and support staff are remote from the systems being managed.

2.4.2 Roles

The main roles are as follows:

- **Operational Management** (sometimes called **System Administration**): keeping the system running where this is not done by system management. Operational management is normally split into sub-roles, including:

  - **System set-up and installation**: setting up the base and application software on the system and configuring it for live running, including roles.
  - **Software update**, where this is not automated via system management
  - **Security/User administration**: administering user security information such as their authentication information, the roles they can perform and the groups they belong to.
  - **Database** (e.g. Oracle) or **Package** (e.g. Riposte) **administration**
  - **Computer operator**: on most systems, this is a minimal role - switching on machines, loading media and similar operations.
  - Other **system administration** functions

  Note that some package administration is done by people supporting the application users e.g. Discoverer and Business Objects are administered by corporate management support staff.

- **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), where this is automated, for example, at the Post Offices. As for operational management, sub-roles separate specific roles and also separate administration of users and the Tivoli system itself.
- **Network Management**: managing the network, including routers and firewalls, which connects machines and sites together.
- **Application support** - 2nd, 3rd, 4th line
- Other **hardware and system support**
- Horizon System and other **technical help desk**s and supporting staff
- **Engineers**

2.5 Pathway Sites and Interactions

The main Pathway services run at the secure Pathway Data Centres at Wigan and Bootle. This includes the main operational systems, most corporate management systems, some implementation systems and system & network management ones as outlined in the previous sections.

The main operational and management services can be run at either site, if needed, though there is a prime site for each. Figure 2-5 shows the sites with electronic links to the Pathway Data Centres.

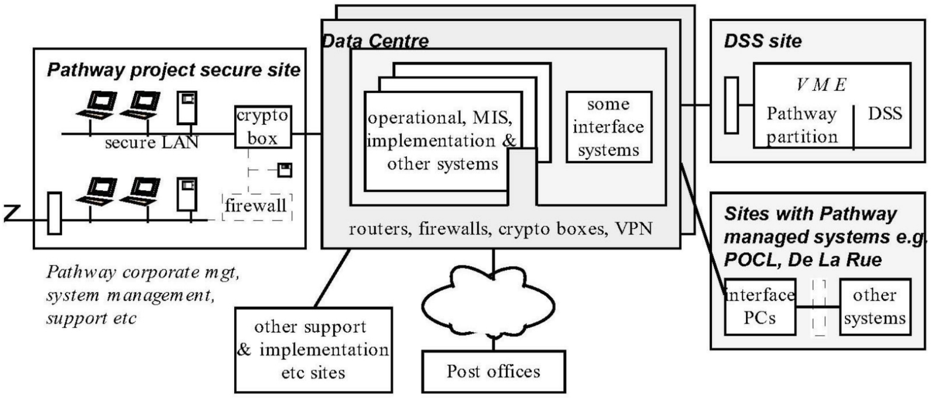

Pathway project secure site
secure LAN
crypto box
firewall
Z
Pathway corporate mgt, system management, support etc
Data Centre
operational, MIS, implementation & other systems
some interface systems
routers, firewalls, crypto boxes, VPN
other support & implementation etc sites
Post offices
DSS site
VME
Pathway partition
DSS
Sites with Pathway managed systems e.g. POCL, De La Rue
interface PCs
other systems

Figure 2.5 Pathway Data Centres and linked Sites

All links to the Data Centres are protected by routers, firewalls, cryptographic boxes or VPNs (or a combination of these) - depending on the requirements protecting each type of link and the data which travels over it. Routers and firewalls are also used to separate Data Centre systems in some cases.

Where Pathway communicates with other organisation's sites (such as POCL, De La Rue), Pathway manages an interface PC/router at that site to provide a gateway between Pathway and that organisation's systems. This is different at DSS sites, where Pathway have a partition on the relevant VME system.

The main Pathway project sites which have access to the Data Centre systems have secure LANs for that access with an encrypted link to the Data Centre. Where people at these sites access other systems, including other sites, there are separate networks. At some Pathway project sites (e.g. Feltham and Bracknell) there are more complex networks which permit limited traffic to/from other controlled systems (for example, for software distribution from the Configuration Management systems and downloading of data to test rigs for investigating faults). In these cases, firewalls are used at the project sites to control this traffic.

There are a number of other support and implementation sites with different types of access, so subject to different access control policies.

3. OVERALL ACCESS CONTROL POLICIES

This chapter identifies the overall access control policies and associated procedures and controls which apply across the Pathway solution. It gives the general policies which apply across systems and identifies where variants and exceptions are permitted. In these cases, the exceptions are defined in the appropriate sub-section of chapters 4 and 5 below. No other variants are permitted.

3.1 Introduction

The objectives in the Pathway Security Policy give the requirements for confidentiality and integrity of data, whether in storage or in transit, and integrity of the services and software components. The ACP defines the policies for controlling access in line with these objectives.

3.1.1 Pathway Human Roles

Human access to the Pathway information systems is specified in terms of roles. People in specified roles are permitted to carry out defined functions and access specified data. This is normally policed by controls within the information systems, though in some 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.

Where practical, the same or similar roles are defined for several systems to reduce complexity and make it easier to check compliance with the overall security policy.

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.

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

3.1.2 Types of Information and its Use

Information in the Pathway system to be protected from unauthorised access includes:

- The business data exchanged with POCL and DSS 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. DSS and related business data is classified as RESTRICTED according to UK government classifications. Some data also has a National Sensitivity Indicator.
  Business data is transferred between POCL, DSS etc and the Pathway Data Centres and between the Data centres and the Post Offices and card production systems. It is stored at the main operation systems and also in archives. Some data is also available for management services at the Data Warehouse - a particular instance is the fraud case data about suspected fraud.
- Pathway business management data - financials, service level agreements etc. There are confidentiality and integrity requirements for much of this data.
  This data is collected from the operational systems to the MIS ones, and information extracted to Pathway project sites and forwarded to POCL and DSS.
- Other data supporting the business processes such as training data (special, non-sensitive, business style data used in training sessions) and on-line documentation e.g. Payment Card Helpline procedures, Post Office procedures.
- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc.
  This data is mainly held at the Data Centre and other systems, and accessed remotely from system management and support sites
- Security information about users, keys, security audit logs etc

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

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

3.2 General Principles

The following general principles should be followed in controlling access to the Pathway systems.

3.2.1.1 The principle of “least privilege” should apply to restrict the access rights of users.

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

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

3.2.1.4 Where possible, the operation of Pathway should be automated to reduce the need for human intervention and the potential accidental and malicious security breaches resulting from human activity. For example, applications should be designed to reduce the human interaction needed and jobs should be scheduled automatically as the result of files being received or at a particular time.

3.2.1.5 Similarly, where practical, system management tasks should be automated, including taking remedial action where the results of monitoring the system show this is needed. Only where action cannot be taken automatically, or human verification of an action is needed, should human intervention be required.

Note that this Access Control Policy covers access by system entities as well as human users, but does not define roles for them.

3.3 Human Access

This section contains the policies for how human access to the Pathway systems is controlled. It is divided into sub-section for policies on:

- Authentication to prove the user's identity to the IT system, and hence his right to take on a particular role, and access particular resources
- User registration/ administration to establish and maintain the user's identity and security attributes (such as role, password)
- Authentication of visitors
- Authentication by telephone
- Control of human access to resources (see also 3.5)

3.3.1 Authentication to IT Systems

3.3.1.1 All users must be authenticated to the IT system. This must identify them as individuals. (The few permitted exceptions to this policy are in chapter 4)

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

- They are at sites remote from the Data Centre and can update operational or MIS systems (for example, to perform systems management actions)

- They can access BA and/or POCL business data (except at Post Offices).
- They are authorised to update system data which can affect the running of the Pathway systems. This includes people who have UNIX root privilege, NT users belonging to the administrators group and database administrators.

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

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

3.3.1.5 Where a user needs to authenticate to multiple systems/domains in one session, the first authentication (normally to the local workstation) should be with a token.

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

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

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

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

3.3.1.10 The minimum password length is 6 characters.

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

3.3.1.12 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 operational management roles in exceptional circumstances as specified in the appropriate later section (for example, for Sequent systems in 4.2.2). Any change to use another username must be controlled and audited in a way which will always be recorded.

3.3.1.13 An operational management role may need full system administrator access to the system in limited circumstances. In this case, where possible, the user should be given limited privileges on log-on and have to ask for other authorised, but potentially wide ranging, privileges when required. In particular, no user is allowed to log onto UNIX with root access (though some may be permitted a controlled change to root access later).

3.3.2 User Registration and Administration

3.3.2.1 People must be identified to Pathway information system as individuals. Users with direct access to the system should be registered as follows.

- If accessing the system via a package such as Oracle or Tivoli, they are registered with that package.
- Users who require direct access to the operating system are registered with that operating system (at the local system or NT domain)
- 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.)

3.3.3 Authentication of Visitors to Post Offices and Pathway Sites

3.3.3.1 All visitors to both Pathway and Post Office sites who need access to the IT system must have a company identity card which includes their photograph, signature and pass number.

3.3.3.2 Unless otherwise stated, for all such visits, the pass number of the visitor must be notified in advance to the relevant manager; access will not be permitted if this has not been done. However, Auditors will visit Post Offices and other sites without prior notice to the Post Office Manager.

3.3.3.3 Pathway visitors to Post Offices must be subject to Pathway vetting procedures and approval by Horizon.

3.3.3.4 Visitors to Pathway sites are subject to agreed vetting procedures.

3.3.4 Telephone Authentication at Help Desks

Authentication by telephone is needed at all three main Help Desks:

- The Payment Card Helpline (PCHL)
- The Horizon System Help Desk (HSHD), and
- The Rollout Help Desk

All these Help Desks receive calls from Customers, POCL staff at Post Offices and other sites and other people such as DSS and Pathway staff. The following categories of call have different authentication requirements:

- Category 1: Calls where the source of call would not affect the action taken. For example, the call is just a query of generally available information.
- Categeory 2: Where the result of the call is to cause an action which has only limited consequences e.g. to report a problem in the Post Office (which could result in an engineer call) or report a lost card (which could cause a card to be stopped).
- Category 3: Where the consequences of misidentifying of the caller could be serious (and the telephone authentication is the only authentication of the caller). For example, the wrong person may be allowed access to sensitive information, and/or be able to disrupt the service.
- Category 4: Where the consequences of the call could potentially be serious, but authentication of the user on the phone is only part of the process needed to complete an action. For example, a Post Office Manager has lost the PIN associated with the card used to boot the system, but will still also require a password to use the system.

3.3.4.1 For category 1 calls, no authentication is needed.

3.3.4.2 For category 2 calls made by customers, some level of authentication of the caller is required, depending on the type of call. For example customers making queries and reports about cards and PUNs (e.g. card lost or damaged) authenticate by responding to a number of verification questions asked by the PCHL advisor as specified in [SADD].

3.3.4.3 For category 2 calls made, for example, by POCL or BA staff, at least the location of the caller should be verified, for example, the particular Post Offices, or POCL regional centre. This location must be one already known to the Help Desk for which suitable verification information is available. Where the call is on behalf of a customer, authentication of the customer (see above) as well as the caller is needed.

3.3.4.4 For category 3 calls, the caller must be identified individually. (If the person concerned is not known individually to the Help Desk, the call must be routed via a known centre for verification. For example, calls from Post Office staff at the Outlet could be routed via a POCL regional centre whose staff authenticate to the Pathway Help Desk.)

3.3.4.5 For category 4 calls, the authentication process should at least verify the location of the call to one known and acceptable for this type of call.

3.3.4.6 Help Desks must maintain the information required to authenticate the callers and their sites/offices as required for the type of call.

3.3.4.7 If the call needs to be passed onto another internal Pathway help desk, the call should be forwarded only after the initial authentication has been carried out.

3.3.4.8 There are several different types of calls in each category. The authentication process for each call type must conform to these policies.

Details of the information used for different types of call must conform to these policies and be given in the appropriate Help Desk procedures.

Note: just location (fields from address, phone number and FAD code/pseudo FAD code) does not seem strong enough authentication for category 3.

3.3.5 Control of Human Access to Resources

Controls of access to resources is achieved partly by workstation set-up and partly by administration of the resource, for example, in the form of an access control list. Details of the way the access controls are implemented in the information systems depends on the product used and is not defined in this policy document.

3.3.5.1 All human users with access to Pathway Data Centre or Pathway managed systems on other sites must do so using controlled workstations as defined in 3.6.1.

3.3.5.2 Access controls associated with resources should define the “role” of the user, not the individual user’s identity (unless there is an agreed need for individual access). The role may be represented by a group identity, for example, in products such as Riposte, UNIX and Windows NT which support groups, not roles directly.

3.3.5.3 Access controls associated with resources should provide access to the resources as in the role definitions in chapter 6.

3.4 Non Human Users

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

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

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

3.5 Information and Resource Access

The Pathway Access Control Policy is concerned with protecting information in all Pathway systems at the Data Centres, at Pathway managed systems (such as interface systems at POCL and other sites), at the systems used to access Data Centre and managed systems and in transit between these. This includes protection of information during fault investigations and correction and information retained for auditing and fraud investigation.

3.5.*1.1* DSS and related business data is classified as RESTRICTED according to the UK government classifications and must be protected accordingly. Access to data with a National Sensitivity Indicator is further limited to authorised staff.

3.5.1.2 Where human access to this information is needed, it should only be accessible to those with a need to see it according to their role.

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

3.5.1.4 Digital signatures should be used for integrity of business information between the Post Offices and other services where required. For example, for signing payment authorisations sent from Pathway to the Post Offices and signing automated payments at the Post Office prior to transmission via Pathway to POCL or POCL Clients.

3.5.1.5 System data should also be integrity protected when required. For example, digital signatures protect software distributed to the Post Offices and elsewhere.

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

3.5.1.7 Passwords should be stored in encrypted form separately from application data and executable code, except for the specific cases listed in *Non Human Access* above.

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

3.5.1.9 Pathway systems should prevent human users interfering with each other or with the automated applications and should prevent applications interfering with each other.

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

3.5.1.11 Different applications should 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).

3.5.1.12 Access to shared resources such as filestore should be controlled by:

- Access to that filestore being restricted to a specific product which is available only to authorised users, 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).

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

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

3.5.1.15 Packages (such as Oracle and Tivoli) and applications above the operating system must also conform to the Access Control Policy. For example, Oracle should restrict Payment Card Helpline users to the authorised tables and views. Also, access to the package's resources should use role based access controls.

3.5.1.16 For client-server applications (such as Oracle Forms applications using PAS/CMS), audit records should be generated at the server so audit logs do not rely on input from workstations.

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

3.5.1.18 All systems, except Post Office counter systems, must provide read access to audit trails by authorised security auditors.

3.5.2 Key Management

Cryptography is used widely in Pathway as described in the Security Functional Specification [SFS] for:

- Protecting information on links for confidentiality, integrity and origin authentication in line with the requirements for that link.
- End-to-end integrity and data origin authentication, potentially over multiple links using digital signatures.
- Filestore encryption at the Post Office.

The following policies apply for protection of keys.

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

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

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

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

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

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

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

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

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

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

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

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

3.6 System Set-up Policies

3.6.1 Workstation Set-up Policies

3.6.1.1 Users with interactive access to Pathway systems should use "controlled, NT workstations" as defined in the following policies in this section. All such exceptions to the "controlled NT" workstation policy must be authorised and documented in the ACP.

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

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

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

3.6.1.5 Operating system set-up and services available at that workstation should be controlled by Pathway or shown to conform to Pathway standards.

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

3.6.1.7 The selection of tasks available on the desktop (or via secure menu system, where used) should be constrained to those available to users with that role.

3.6.2 Server Set-up

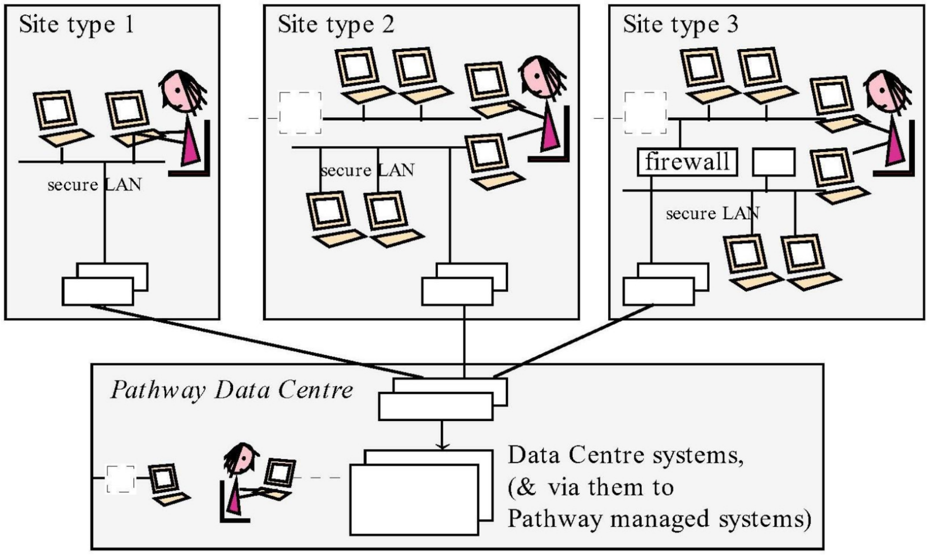
3.6.2.1 Servers should have floppy drives disabled at boot time. Booting from CDROM should also be disabled once a system has been configured. In all cases, exceptions to this rule must be agreed with Pathway Security Management and Horizon and be documented

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

3.6.3 Workstation Environment Related Access Controls

3.6.3.1 Users with interactive access to Pathway systems should access these systems via controlled, NT workstations in secure environments as defined in the following policies. All exceptions to these policies must be authorised and documented in the ACP.

The following diagram shows the main types of workstation environment supported for access to the Pathway Data Centres and other Pathway managed systems.



3.6.3.2 Workstations which have access to sensitive data or can be used to access Pathway systems (code or data) should be on separate secure LANS linked only into the Pathway secure network. (Site types 1 and 2 and the Data Centres)

3.6.3.3 The only permitted exceptions are:

- For authorised transfers of software and RODB data from the controlled Pathway LAN at the management site at Feltham to the appropriate Data Centre system.
- For application support users linking to test rigs. In agreed circumstances, authorised application support users may access to DSS data to investigate a problem and may download that data to the workstation or test rigs.

In these site type 3 cases, firewalls between the LAN on the project site and the encrypted link to the Data Centres must constrain traffic to just that authorised from identified project systems to the identified Data Centre systems.

3.6.3.4 All such users (except PCHL ones) should authenticate using a token.

3.6.3.5 The secure LAN and workstations must be in a physically secure area restricted to permitted users as must any routers, encryption boxes and firewalls connecting them to the Pathway data Centres.

3.6.3.6 Where the workstation is remote from the system being accessed, encrypted links should be used. *[does FTMS contravene this*?]. (PCHL and Girobank FRM users are located at the Pathway Data Centre sites, so are considered local users not requiring encrypted links.).

3.6.3.7 Where a user also needs access to internal Pathway systems (such as the call recording and management systems and e-mail), the user must use a second workstation linked to the internal network and system required but not to the Pathway Data Centre. (site types 2 and 3)

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

3.6.3.9 External users, such as BA Security staff accessing the FRMS service from their own site, must conform to these policies for controlled NT workstations in a controlled environment via an encrypted link.

3.6.3.10 External support users of Pathway systems (such as Sequent and Cisco) should be permitted access to Pathway Data Centre systems only from approved sites/environments and subject to agreed network and other controls (see 4.6.3).

3.7 Network Access Policies

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 Data Centres and managed systems and also within parts of the Pathway management systems. In addition to the workstation environment controls above, network access policies can be enforced using a combination of access lists at routers, controls at firewalls, NT domain controls, platform controls on use of ports and other application controls where needed.

3.7.1 Information in Transit

3.7.1.1 Business and system data in transit to/from the Pathway Data Centres must be protected in accordance with [SFS]. This covers, for example:

- transfer of data to/from Pathway managed systems at other sites such as DSS, POCL, POCL Client and De La Rue systems.
- business and system management traffic to/from the Post Offices (which is protected using a VPN to provide authentication and encryption as well digital signatures in some cases - see above)

- business and system information between the Data Centres and Pathway management and implementation sites

Does the SFS cover protection of links to regional offices and implementation suppliers?

3.7.1.2 The Energis ATM network with its closed user group should be used to restrict access to DSS data and the main POCL data (TIP and Reference data) to Pathway only.

3.7.1.3 All ISDN links should use VPN protection (for authentication and encryption) or in cases where that cannot be justified, CHAP authentication and CLI.

3.7.2 Control of Traffic In and Out of Data Centres

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

3.7.2.2 All management and support users access the Data Centres (and other managed systems) from controlled workstation environments as defined in 3.6.3 above.

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

3.7.2.4 External support users with access to any of the Pathway systems containing sensitive or protectively marked information access the system via controlled workstations and environments as for Pathway support staff, but subject to extra controls - see appropriate section below. (Support of routers is an exception - see below).

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

3.7.2.6 Apart from links via the Energis closed user group to DSS and the main POCL systems (and via POCL, to Royal Mail), all access to the Data Centre by external organisations for support or other purposes should be firewalled from the main Data Centre systems. Any exception to this must be agreed with the Pathway Security Manager and documented in the ACP.

3.7.2.7 Traffic to/from Pathway managed interface PCs/routers at other sites (POCL, De La Rue etc) should be restricted (by routers and firewalls) to:

- authorised business traffic between the managed system and the particular Pathway Data Centre server handling that link (normally just file transfer between the systems).

Question: Should limited operational management and application support be allowed?ACP3 said these PCs were managed using via system management (c.f. the Post offices, though applications and set-up much simpler); any limited system admin needed would be done locally. I'm not keen to allow remote admin over unencrypted lines if this could access, for example, card data unencrypted after its encrypted transfer to De La Rue.

- network management traffic between the routers and the NMS.
- system management traffic between the PCs and Tivoli Management Centre

3.7.2.8 Traffic to/from the Pathway VME partitions at DSS sites should be restricted to:

- authorised OSI business traffic (file transfer, and SQL*Net for the CAPS on-line interface) between VME and Sonnet on Sequent.
- limited authorised operational management and application support
- network management traffic between the routers and the NMS

3.7.2.9 A set of routers should handle all traffic to/from operational Post Offices and accept traffic from outside the Data Centres only from Post Offices. No operational Post Office traffic should be accepted via other routes. These routers should also restrict where traffic can be routed to/from within the Data Centre i.e. to VPN servers? the Correspondence Servers, Tivoli management servers and KMS. *[don't know how this works - does it go to the VPN for onward routing?]*

3.7.2.10 When implementing a new, or significantly changed, Post Office, connection will initially be to a special boot server. Access to this from the Post Offices should be via a firewall, which also restricts traffic between the boot server and the main Pathway Data Centre LAN. *[check]*

3.7.2.11 Routers should be configured to deny access to external users (e.g. CISCO support) until this access has been agreed - see 4.6.3. When permitted, the appropriate router should be configured to restrict access to the Data Centre to the particular system(s) needing support.

3.7.3 Controlling Traffic Within Data Centres

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

- Systems concerned with roll-out of Post Offices should be separate from those used for operational running.

- Security services, such as the Key Management one, should be well protected from unauthorised access from other systems.

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

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

3.7.4 Controlling Traffic at and from Pathway Project Sites

Pathway project sites include:

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

3.7.4.1 For whole Pathway network at the main management sites (such as Feltham and Bracknell?) should be protected. The only permitted connections should be:

- to the Data Centres via encrypted links
- to other secure LANs via an encrypted link (i.e. between the Bracknell and Feltham secure LANs)
- to the ICL Corporate network via a controlled router, which restricts traffic to what permitted.
- to implementation users at regional offices and implementation suppliers at their sites via a controlled router and firewalls (for access to the RODB*)*

Note: the above still needs checking. Does the ICL corporate network link provide the links needed to services required by Pathway managers, developers etc (such as email, Powerhelp and the financial system, any electronic supply of software from other units)

Are Implementation users and suppliers to the roll-out database?

3.7.4.2 The Pathway management site network itself should be divided as follows:

- Most local users should only have access to specific LANs which provide access to local services and (via the router) to the ICL Corporate network. Access from these LANs to the (secure LANs and the) Data Centre must be controlled by a firewall which restricts data to that permitted (e.g. software from the Configuration management system at Feltham) as well as the encrypted links.

- All users with any interactive access to the Data Centres must do this via secure LANs (see also 3.6.3)
- Separate secure LANs should be used for separate user groups/activities where sensitive data is being handled at Pathway management sites. For example, Security Management, Auditing and FRM users should be on a separate high security LAN separate from other users.
- Servers at the Pathway management sites which require strong security because they handle sensitive/RESTRICTED data or are used to update the Data Centre should be on a secure LAN. This applies, for example, to the CM signing server which distributes software to the Data Centre, the RODB and reconciliation database.

4. SPECIFIC HUMAN ACCESS CONTROLS

4.1 Introduction

This chapter covers where the access control policies, and in particular, authentication policies, in chapter 3 for human users are specialised for particular roles and where exceptions to these policies are permitted.

Note that a full list of Pathway roles, outlining the IT access permitted to each of them, is given in chapter 6.

4.2 Post Offices - Operational and Implementation Roles

There are no system management and support roles at the Post Offices, as these tasks are run remotely, apart from some limited tasks available to Post Office managers.

4.2.1 Post Office Normal Running

For normal functions, Post Office Managers, clerks and supervisors authenticate using a Riposte username and password.

On normal counter start up (once installation is complete), the Post Office Manager (or authorised other user) uses the Post office Memory card and PIN (which is also used in protecting the filestore, as defined in the [SFS]).

The following specialisations of the policies in 3.xx apply in these cases.

4.2.1.1 A password cannot be re-used for 18 months.

4.2.1.2 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 password cannot be one of an agreed “excluded passwords” list.

4.2.1.3 After a period of inactivity at a Post Office counter, the session will time out, but can be resumed on entry of the password. After a longer period of inactivity, the user is forcibly logged out.

4.2.1.4 The PIN used for the Post Office Manager’s memory card is a 15 character alphanumeric value

4.2.1.5 The Post Office Manager should secure the Memory card and PIN for it in separate places

4.2.1.6 When a new Post office user is added to the system, a full name must be supplied, so that the user can be identified from the user name included in the transaction logged in the Riposte journals.

4.2.2 Customer Authentication at Post Offices

For most Post office operations, customers do not need to authenticate themselves. For DSS benefit related transactions, they are authenticated as defined in [SADD] for example:

4.2.2.1 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)

4.2.2.2 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.

4.2.3 Post Office Exceptional Cases except Implementation/Installation

This subsection includes exceptional cases involving the Post Office Manager and other Post Office staff and also support engineers, POCL auditors and emergency managers.

For some user groups, and some exceptional circumstances, the Post Office Manager (or other authorised person) authenticates using a one-time password with the assistance of the Horizon System Help Desk (HSHD). The Post office system generates a value, then phones the HSHD authenticating to the HSHD as defined for that user role/circumstances (see ??). The HSHD (after authenticating the user) provides a check value which the user can type in at the Post office counter to authenticate himself.

The following policies apply to these exceptions.

4.2.3.1 If there is a failure on booting the counter systems after installation of new software, the Post Office Manager the reverts to the failsafe version of NT supported by HSHD and using a one-time password.

4.2.3.2 If the Manager loses his password, he (or an authorised deputy in his absence) logs into a SUPPORT username using a one-time password provided via the HSHD.

4.2.3.3 If the Manager loses his card or PIN, he obtains an emergency recovery key via the HSHD (after authenticate to the HSHD).

4.2.3.4 Support engineers (installing new hardware and running tests to check it authenticate) and Auditors use generic Riposte usernames for the appropriate role and authenticate via one-time passwords. For both engineers and auditors, the pass number is also typed in, so individual users can be identified in the log.

4.2.3.5 If a POCL Emergency Manager takes over a Post office when the manager is unavailable or unco-operative, he may use the emergency recovery procedure to boot up the Post office - see 4.2.2.3.

4.2.4 Implementation/Installation Roles at Post Offices

On implementation/installation of a Post office,

- The installation engineer sets up the connection to the data centre
- the Post Office Manager (POM) completes the Post office set-up for normal working including set up of the memory card and PIN
- The Horizon Field Support officer (HSFO) migrates existing stock records to Pathway - either manual ones or from ECCO equipment

4.2.4.1 The installation engineer must authenticate to the POM *(see Visitor Authentication)* prior to using the Auto-configuration application. Authentication to NT or Riposte must be impossible at this stage.

4.2.4.2 On first installation of the Post Office (after memory card set-up), the Manager logs in under the Set-up Manager username to create his individual username. After this, the Set-up Manager username *[should be deleted?;* on all future occasions, the POM must authenticate using his individual user name except in cases identified in 4.2.3 above.

4.2.4.3 For migrating manual records, the POM should check the HFSO's credentials and create a MiMAN user including the HFSO's name. The HSFO authenticates to that (using a shared HFSO password) under POM control and should only have access to the migration application. After migration, the POM and HSFO should check the name details are correct and the POM should then delete the migration account.

4.2.4.4 For Post Offices migrating from ECCO equipment, the HFSO uses a laptop, not counter (to read ECCO disks, and feed information to the Correspondence server records for the Post Office). As for manual migration, the POM should check the HFSO's credentials and control migration.

Question: how does the HFSO authenticate to the laptop? And how is his identity recorded at the migration server? Probably breaks the rule of individual authentication?

4.3 Operational Users of Data Centre Systems

This section covers business users, except for corporate management users. System management and support users are also in a later section.

DSS/BA and DSS Help Desk staff access PAS/CMS via the on-line CAPs interface, after authenticating to the appropriate DSS system. Pathway accepts their transactions via the agreed DSS interface without further authentication of these users. The DSS systems is also assumed to have performed any access controls needed to restrict these transactions beyond the normal ones, for example, restricting Help Desk users to read only transactions. At the interface, the DSS/BA member of staff is identified by a transition id which is used for Pathway auditing. At PAS/CMS, these users appear to be system, not human, users.

4.3.1.1 All Payment Card Helpline (PCHL) Advisors, Supervisors and Security Managers logon to their own NT domain (separate from other Pathway domains) using a password, and then logon to the PAS/CMS Oracle application (or the training version of this) using a password.

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

4.3.1.3 Their workstations and LAN must be secure and conform to the site type 1 policies for workstation set-up and environment in section 3.2.10.????

4.4 Corporate (including Security) Management Users

Unless stated otherwise, all corporate management users are authenticated to their local NT domain using a security token. They use controlled NT workstations on secure LANs at Pathway project sites linked by encrypted links to the Data Centres (see site type 1 in 3.2).

4.4.1 Business Management

These users may also need to authenticate to the relevant system and/or application for particular systems. This is required for Oracle applications, and for Business Object universes used to access data at Data Warehouse systems via Oracle/Business objects.

The only specialisations and exceptions to the policies in chapter 3 for these users are:

4.4.1.1 BA security staff doing FRM are treated as corporate management users. Their DSS workstations and environment must conform to Pathway policies for type 1 sites in 3.2 above.

4.4.1.2 People in the following roles have CDs at workstations with write access:

- Management support users, who write agreed warehouse data to be put on CD for transfer to DSS and/or POCL
- The FRM supervisor, who provides information to BA Security staff
- The Business Function Auditor, who provides information to external auditors?
  [In future, some transfers of data, e.g. to BA Security, may be via an encrypted link, not CD.]

Note: the ACP did have a policy to allow CS Managers to access the SLAM cache on NT from their normal workstations, rather the secure LAN. This depended on traffic being restricted to the right type of protocol and the NT SLAM cache machine at the Data Centre only. This policy has been removed.

4.4.2 Key Management

4.4.2.1 *[Needs to be a para re key manager/]*

4.4.2.2 The Key Custodian uses the local console at the platform where the key is to be installed/changed and authenticates using a token to the local system. (For NT, this is defined as a local role)

4.4.2.3 The Key Handler has the key on the appropriate media (e.g. floppy) for re-installation of the key during system reboot. He is not a known user of the system and does not authenticate to it.

4.4.2.4 The key handler role may be performed by identified, authorised (non-Pathway) staff at remote Pathway managed systems e.g. by EDS at VME partitions and by De La Rue, POCL etc at interface PCs at their sites.

4.4.2.5 The Cryptographic Key Manager and KMA Data Manager roles are SQL Server users, so log-on to Oracle (after NT workstation, token logon). This gives access to specific functions only.

4.5 Implementation Users

No specialisations to the policies in chapter 3 apply have yet been identified for implementation users, except at the Post Office - see above.

The NT logon to the migration server for ECCO migration is to establish the laptop access to this server. The HSFO uses applications at the laptop only, so is not a direct interactive user of the migration server.

RODB users do not have access to Pathway Data Centre systems, so are not covered by the policies.

4.6 System Management and Related Users

All system amangement, operational management and application support users have controlled NT workstations for management/support activities, and a separate workstation for access to call monitoring and other systems as in 3.3.7 site type 2 and 3.

4.6.1.1 SMC technicians, and other Tivoli users (e.g. Auditors, SSC application support) authenticate to Tivoli as well as the workstation logon to NT.

4.6.1.2 For Post Office key recovery, the SMC team leader may also need to log onto the KMA *[the process here is still to be agreed.]*

4.6.1.3 All network technicians access only the NMS and routers, so access for them is described in that section.

4.6.1.4 *The current agreed exceptions for disabled floppies/CDs need adding.*

4.6.2 Engineering Access

4.6.2.1 Where possible, engineering access to the machines, for example, for hardware diagnosis and repair, should be subject to the same controls as other users, as specified in chapter 3.

4.6.2.2 In agreed, limited circumstances, for example, when the operating system cannot be booted, special access is permitted, by-passing the normal controls. In all such cases, any visiting engineer must be subject to the policies for "authentication of visitors" procedures (see chapter 3) and two people must be present during such access.

4.6.3 Procedures for getting in Support Staff

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

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

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

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

4.6.4 Software Distribution and Exceptions for Fixes

4.6.4.1 All software (new software and fixes) must be registered in the configuration management system controlled by configuration librarians. It should be tested using test rigs and authorised by the CS Release Manager prior to distribution by Software Distributors.

4.6.4.2 In exceptional circumstances, where this is not fast enough, authorised code fixes may be done directly by ICL Outsourcing according to agreed procedures.

4.6.5 Application Support

Application Support calls come via HSHD, who forward them to the appropriate unit for support. Many application support calls are routed to SMC for filtering known errors, before being forwarded to System Support Centre (SSC) or CFM as appropriate for solving. Calls may sometimes be forwarded to 3rd/4th line support units, which may include application suppliers.

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

4.6.5.1 All support users with access to the Pathway Data Centre (or via them, to Pathway managed systems or VME partitions) must do so using NT controlled workstations in a secure workstation environment as defined in 3.2. (For SSC, the secure environment must include a firewall to restrict traffic between the test rigs and the secure LAN, though the workstation gives access to both Data Centres and test rigs.)

4.6.5.2 Limited data may be downloaded from the Data Centres to the SSC test rigs where this is required to assist in diagnosing application problems and testing new software to fix the problem.

4.6.5.3 Support users should have only read access to the supported systems, except for:

- SSC support managers (not normal SSC support users) "correcting" data under controlled conditions. (Data may need to be corrected where it has been corrupted by faulty code.)
  Correction of data must be subject to agreed authorisation procedures. For example, where the data to be corrected is DSS data which is UK RESTRICTED, authorisation procedures must include the Pathway Business Support Unit and DSS.
- CFM operational management staff fast fixing code, when authorised, under controlled conditions.
  Where time permits, correction of errors should be by re-issue of a new version of the software via the Configuration management system. When faster fixing is required, agreed Pathway authorisation procedures must be followed. For applications supported by SSC, this will start with a request by SSC.

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

5. SPECIFIC SYSTEM ACCESS CONTROLS

5.1 Introduction

This chapter covers where the access control policies in chapter 3 are specialised for particular systems. And where exceptions to these policies are permitted.

In addition to the policies in chapter 3, all systems should support the roles in chapter 6, with only the required functions and resources available as defined there with the human access controls defined in chapter 4.

Note: the ACP does not cover internal systems such as Powerhelp and PINICL.

5.2 Post Offices Platforms

A multi-counter Post Office has a local LAN with NT workstations, one of which is the gateway with a link to the pathway Data Centres.

The roles supported are Post Office staff (Post Office Manager, counter clerk and supervisor), Customer (indirectly), POCL Auditors and Emergency managers, Engineers (support and installation engineers) and Horizon Field support Officers (see 4.1, 4.2 and 4.4).

5.2.1.1 At no stage after leaving the factory should it be possible to logon directly to Windows NT or for a user to access NT functions or data.

5.2.1.2 No operational management roles should be supported at the Post Office systems, or any other roles than those listed in 5.2 above.

5.2.2 Factory Set-up Controls

Software is installed at the factory (though may be updated on installation) and initial configuration done.

5.2.2.1 Riposte user groups set-up should be Manager, Supervisor, Clerk, Engineer, Auditor, AuditorE (used by Emergency Managers, Support (used for emergency procedures such as the Manager forgetting his password) *[need to add MiMAN?]*. The Engineer, Auditor, AuditorE and Support groups should be set up to require one-time password authentication.

5.2.2.2 Usernames should 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) and a set-up manager *[and MiMAN?]* associated with the relevant Riposte groups. (The Post Office Manager will introduce further users later.)

5.2.2.3 When leaving the factory, it should only be possible to run the Auto-configuration application, not log-on to NT or Riposte.

5.2.3 Post Installation Controls

5.2.3.1 After ECCO migration, the ECCO disk used for migration must be invalidated, so it can no longer be used. Also, the Migration server should not accept another attempt at migration from this Post office.

5.2.3.2 After installation, special software used for installation only should not be accessible. Usernames used for installation only should be removed.

5.2.3.3 The encrypted filestore should not be accessible unless the workstation has been booted using the memory card and PIN (or agreed emergency procedures)

5.2.3.4 After a user has logged on using Riposte, all access to the system should be controlled by Riposte - the Riposte desk top should allow access to only those items available to people in the user's role. The user must not be able to call any other applications or NT functions or resources. No direct access to Windows NT should be possible at any time, even for engineers.

5.2.3.5 The Riposte infrastructure should not need NT administrator privilege.

5.2.3.6 filestore encryption

5.3 Sequent Systems

5.3.1 Introduction

Sequent systems with Dynix operating system and Oracle databases are used for the main operational applications (see 2.1) and the Data Warehouse (see 2.2) at the Data Centres. The systems also have data in flat files (e.g. before/after transfer to/from other systems).

5.3.2 Human Access

All Sequent systems support the operational management and support roles listed in chapter 6. They also support application roles for the particular applications such as PAS/CMS, RDMC and Business Objects for access to Data Warehouse data.

5.3.2.1 All business users (such as the Payment Card Helpline) and business management users (such as the Business Support unit) should use Oracle applications - Oracle Forms, Business Objects or Discover 2000.

5.3.2.2 Where the SQL*Net access to the database could potentially give more access than that permitted for that business role, the application at the client must restrict access to that permitted. Also, a secure controlled workstation conforming to Pathway policies (see 3.2) must be used and the user identified there with the correct role so that the application controls cannot be by-passed.

5.3.2.3 PCHL, and similar users, just using Oracle via applications on their controlled workstations should be registered to the Oracle application, not the underlying operating system and authenticate using a password.

5.3.2.4 Where users need to be both UNIX and Oracle users, they should be registered in UNIX, and have Oracle use the result of the UNIX (and security token) authentication.

5.3.2.5 Oracle database administration functions should use:

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

5.3.2.6 Application support users of Oracle should use:

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

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

5.3.2.7 Users who require any access to operating system facilities must do so via a secure menu system which restricts the user to functions authorised for users of that role (and audits all functions performed by that user).

5.3.2.8 Where a function called from the secure menu system requires a change of username, that change should be done automatically by the menu system and audited. Changes to username must also cause a Patrol event.

5.3.2.9 The secure menu system should have specific functions for most system management activities. However, for emergency use, the menu will include an item which provides root access and use of UNIX commands.

5.3.2.10 Computer operators access Sequent systems from the console, using the secure menu system to access a limited number of predefined jobs such as back-ups.

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

5.3.2.12 Operational management staff always authenticate under their own names to UNIX and perform functions wherever possible without superuser/root privileges. 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.

5.3.2.13 Where non-Pathway, e.g. Sequent staff provide 3rd line support, this may be from the 3rd party site. In this case, access must be from a controlled NT workstation and controlled environment as for Pathway operational management - see 3.2. Call in procedures are as in 4.6.3.

5.3.2.14 As Sequent require root access, an independent monitoring system will be used where all key strokes on the Sequent workstation are captured and echoed on a CFM workstation.

5.3.2.15 Application support managers can correct application data subject to authorisation procedures - see 4.6.5. For Oracle applications, this should, where possible, be via specific functions available to the Oracle SSC role. In exceptional circumstances, use of SQL*Plus scripts will be authorised after checking. For other services, this may involve updates to flat files. In all cases, corrections to the data are audited.

5.3.3 Application/Oracle Roles at the Operational Sequent Systems

5.3.3.1 Database roles with appropriate database views/tables should be used to separate what data is available to whom

5.3.3.2 The following Oracle roles should be defined for all Oracle applications on the operational Sequent servers. Note that in some cases, people with different human roles in the list in chapter 6 may have the same access to the same Oracle role.

Oracle role	Functions, and roles
MONITOR	Read only access to application data in this database - used by Auditors, FRM, application support etc
AUDITOR	As MONITOR plus access to audit information - used by auditors
CFM_DBA	Full dba privileges
SSC	As for MONITOR, plus limited updates, implemented by pre-defined, authorised forms
BSU	specific business support functions on PAS/CMS and some other applications - see chapter 5.

5.3.3.3 Other application roles should be defined for particular applications to support the application roles listed in chapter 6, for example, PCHL roles at PAS/CMS, Reference Data roles at RDMC.

5.3.3.4 Information available to people doing ad-hoc queries should be further constrained e.g. using Business Object universes

Note that there are also roles for non-human users.

5.3.4 Dynix and Oracle Access Controls

5.3.4.1 The Dynix operating system should be set-up according to the access control policy in 3 above.

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

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

5.4 Windows NT Systems

This section covers NT workstations and servers at the Data Centres and other Pathway managed NT systems except the Post Offices. NT workstations at secure Pathway management and support sites should also conform to these policies, and the NT domain policies.

5.4.1 Generic NT Policies

NT systems support the operational management and support roles listed in chapter 6 unless other wise stated.

5.4.1.1 As on other systems, engineers should only have controlled access and must be accompanied by CFM staff when using the system.

5.4.1.2 Apart from event logs etc which are relevant to all NT systems, application support users should access application databases via relevant tools, rather than just operating system facilities.

5.4.1.3 All NT servers should be set up with a group and template user for the generic management and support roles (plus any others defined for the particular NT system). These templates should be 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.

5.4.1.4 While use of NT domains allows a user to log in once to multiple servers, some roles (such as Engineer and Key Custodian) should always be defined as requiring the user to be local at the machine.

5.4.2 NT Domain Policies

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

NT domains should conform to the following policies:

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

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

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

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

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

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

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

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

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

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

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

5.4.3 Correspondence Servers

5.4.3.1 Business Support, FRM and Auditor access to the operational Correspondence servers should be restricted to exceptional circumstances for limited amounts of data (as otherwise, the performance of the system could be impaired). In all cases, access should be controlled, and limited to use of a specific agreed query tool.

5.4.4 Security Servers on NT

Security services on NT are:

- A **Key Management Application** (KMA) which (generates and) distributes cryptographic keys to Pathway services and the Post Offices. An associated **Certification Authority** (CA) generates public key certificates and **Entropy servers** which generate DSA entropy for digital signatures.
- The **VPN servers** used for protection of the traffic to Post Offices
- The audit and key management workstations supporting the Pathway security manager and his staff
- Signing servers to sign software and auto-configuration information sent to the Post office

(This is in addition to the software security services to protect data in transit on particular links.)

5.4.4.1 The Certification Authority Workstation (CAW) which includes the CA should be off-line - not connected to any network.

5.4.4.2 The KMA should store all keys encrypted, and the key used to encrypt these keys should be subject to the normal KEK policies - see 3.5.

5.4.4.3 Application level access to the KMA should be restricted to the agreed functions for each of the specified roles, and each role should have the least privilege needed to do the job**.** All security significant actions should be audited.

5.4.4.4 On-line interactive access by human users to the NT server on which the KMA resides should not be generally be possible. It should require approval by the Pathway Security Manager to permit this access (except for key handling on reboot?). The access will only ever be permitted for:

- read only access by application support staff (updates should always be via the standard Tivoli software distribution)

- limited, authorised, system admin access by local users?? Dba auditor…
- engineers

5.4.4.5 VPN servers???????????????

5.5 Authentication Service for Authentication using Tokens

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

5.5.1.1 After installation and configuration of the Authentication Service , the only application access to the Authentication service should be by the Pathway Security Manager workstation at the Pathway management site.????????? These must be controlled NT workstations on the secure LAN (see chapter 3)

5.6 Cryptographic Boxes

Zergo boxes are used to provide link level encryption on a number of links. These are government approved point-to-point encryption devices using Rambutan.

5.6.1.1 Access controls at these devices should be as specified by the manufacturer.

5.7 Symmetrix discs

[should add]

5.8 Interface Systems at Business and Implementation Sites

The ICL Pathway project manages interface PCs at some related sites (POCL, POCL Clients, De La Rue, and implementation supplier? sites) and also a partition of the VME system at DSS benefit sites. It also has manages the interfaces to the Pathway network, for example, routers.

In all cases, routers are managed by Pathway Network Management and interface PCs are monitored?/managed using Pathway System Management.

5.8.1 DSS Benefit Interface Access Controls

At the Benefit Agency's CAPS and ESNS systems, the Pathway interface applications are in a Pathway partition of the VME machines.

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

5.8.1.1 No human intervention should be needed at the VME partition in operational use apart from exceptional circumstances.

5.8.1.2 All Pathway interactive use of the VME partition should be via Sonnet on Sequent. All users should be individually identified and authenticated using the VME Enhanced Security Option.

5.8.1.3 The Key Custodian (installing and updating the Red Pike cryptographic keys used to protect the transfers of information from CAPS to the Pathway Data Centres) should be done by authorised EDS staff at the local DSS site.

5.8.1.4 The Pathway VME partition filestore should be separate from other partitions' filestore. Transfer of data between the Pathway partition and CAPS/ESNS should be restricted to transferring files to/from the special transfer usernames using an agreed interface product.

5.8.2 Interface Systems with Interface PCs

Pathway has links to a number of Pathway managed interface PCs at sites remote from the Pathway Data Centres. These include POCL and POCL client systems and Pathway partners (such as De La Rue) for business transactions. (The POCL TIP link is also used for Royal Mail traffic.) There are also interface systems at Pathway Implementation Suppliers (with bulk transfer to the RODB at the Pathway management site).

5.8.2.1 Once configured, the PCs and routers at these sites should not normally have any human access - file transfers should be automated and the PCs managed remotely using Tivoli.

5.8.2.2 The operational management role at these sites is limited to local system administrative functions only.

The two points above were in ACP3, and have not been changed to allow remote access for system admin and support, despite the current machine set up, as its unclear that data would be adequate protected in this case - see also 3.7.2.7. FTMS encrypts data during file transfer, but it is held in clear in filestore after transfer, so could be read by system administrators over the unencrypted link. Will the VPN be extended to handle the whole dialogue here, rather than just having FTMS encryption?

5.8.2.3 The engineer role is restricted to installing or replacing the PC. The PC will not be repaired when configured into the operational system.

5.8.2.4 Business data in transit to the Data Centres is protected as defined in 3.7 above.

5.8.2.5 Where the PC is directly connected to other systems (such as the POCL ones), it should also be configured to restrict traffic with such systems.

5.8.2.6 Controls at the interface PCs at POCL (and similar) sites must ensure separation of incoming and out going files so that all files supplied by Pathway are read only for POCL access. In addition, files for different systems (e.g. TIP, Royal Mail and Reference Data) are separated.

5.8.2.7 For De La Rue systems, separation of the Pathway managed PC and the De La Rue system is via an airgap between these systems. Information is transferred between systems using media - floppy/zip. The computer operator at De La Rue sites does not log to the system and perform any NT functions????????

5.9 System Management Servers

A set of Tivoli system management servers are used to manage the Post Office systems and related Data Centre NT systems (mainly using Tivoli products). They also monitor other Pathway management systems and collect event data from other systems also.

5.9.1.1 All users of Tivoli must be registered at the Tivoli server and associated with the appropriate roles, groups (and regions) to restrict their access to facilities which they are permitted to access. (All such users have security tokens, so are also registered with an Authentication Service)

5.9.1.2 In addition to SMC roles, Tivoli servers should also support:

- Pathway Security Auditors with read access to audit information via the web interface - platform audit logs, Tivoli notices, Tivoli events collected for auditing.
- Application support users with access to Pre-authorised Tivoli tasks to extract diagnostic information from the Post Office.

5.9.1.3 Tivoli integrity features should also be used to protect Tivoli traffic on the link.

5.10 Network and Firewall Management

5.10.1 Network Management and Routers

The Pathway network routers are managed using HP Open View with Cisco Works as illustrated below.

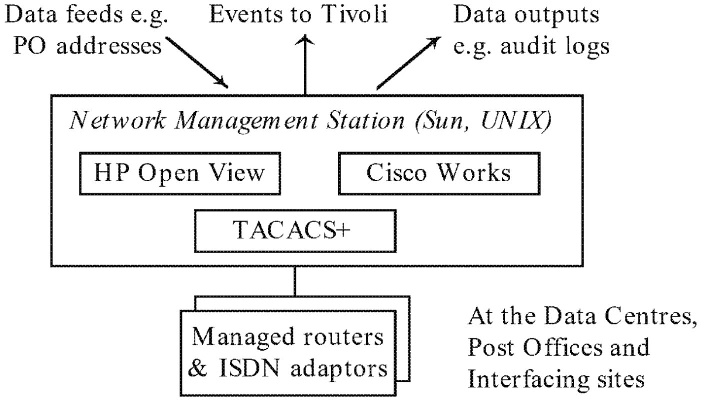


Figure 5-1 Network Management

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

The network management roles are:

- Network Manager, Network Technician, Network Management Configurer, Cisco router support.

Engineers may also require direct access to routers.

There are no on-line application support roles. Support of Open View, Cisco Works etc is done off-line. Pathway auditors access audit information from the NMS via audit records sent through to Tivoli and extracted audit logs.

5.10.1.1 The Network Management Configurer is responsible for the configuration of the Network Management Station itself, such as Open View configuration. This role must be carried out by the Network Management team before live running. The configuration must be validated by more than one network technician and signed off by a senior ICL Outsourcing person before use.

5.10.1.2 The Network Management workstations run 24 hours a day. However, at the end of the shift, the existing user must log out and the new user log on to give individual accountability. Other users of the system must also authenticate themselves e.g. prior to doing configurer or security management functions.

5.10.1.3 NMS users use controlled NT workstations with tokens (see section 3) but also need to log onto UNIX for access to authorised OpenView and Cisco Works/View functions.

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

5.10.1.5 Telnet access to routers is permitted only to ICL Outsourcing senior network management staff and Cisco staff supporting the routers from a remote CISCO site

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

5.10.1.7 All users of Telnet access to routers must authenticate using TACACS+ and their access audited at the NMS.

5.10.1.8 ICL Outsourcing senior network management staff access the routers in agreed exceptional circumstances (for example, for fault resolution requiring use of the debug facility, in times of excessive network workload or during fault conditions). Authorised ICL Outsourcing Network Managers use Telnet access to routers from a specific dedicated NT system on the Operational Bridge area of the Network Centres.

5.10.1.9 Cisco staff must access the router needing support via a separate gateway router dedicated for Cisco use. This gateway router must be configured to permit Cisco access only when Cisco support is needed. A different TACACS username and password must be used on each occasion, valid for the particular session only. The standard Cisco engineers must only have read access to the routers. Named and authorised senior CISCO staff (NSA Engineers) may have the "enable" mode, as that needed for reviewing configuration files and debugging. CISCO should not be permitted to make changes to the routers (though the router controls cannot enforce this?); they should advice the Network Manager of any changes required.

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

5.10.1.11 In normal running, the routers must not have consoles attached, though console access may be enabled. Any attempt to log-on at a console should be via TACACS+, so flagged at the NMS.

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

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

5.10.2 Firewall Management

Firewalls are managed using Enterprise Centres on Solaris systems (shared with Security token management), one at each Data Centre.

Enterprise Centre roles supported are Firewall Manager and Firewall Monitor. There are no on-line support roles for the Enterprise Centre application or the firewall application.

5.10.2.1 All access to the firewalls must be via the Enterprise Centre, except for hardware maintenance. As for routers, in normal running, firewalls must not have consoles attached - they should only be attached for hardware maintenance after the firewalls has been configured out of the system.

5.10.2.2 All configuration changes must be made via the Enterprise Centre and logged via Tivoli.

5.10.2.3 Firewall audit logs are sent to the Enterprise Centre.

5.10.2.4 Firewalls should restrict traffic as in the network access policies in 3.7. (This is different for different firewalls).

5.11 Software Distribution Servers

Software distribution servers include the Configuration Management and associated signing servers on Pathway project sites and the depot/Tivoli servers at the Data Centres to which software is sent for onward transmission to other Pathway systems at the Data Centres, Post Offices and elsewhere.

5.11.1.1 The Configuration management system should have access controls which conform to this policy, even though it is not at the data centre, or on a separate secure LAN.

5.11.1.2 The associated signing server should be on the secure LAN, and controls should be fully conformant with this policy.

5.12 Implementation Servers at the Data Centres

Implementation of new Post Offices, including migration of in-office data involves several servers at the Data Centres. The Post Office counters are delivered with a standard configuration which needs to be personalised and updated when installed.

The servers involved in this process are shown in the following diagram.

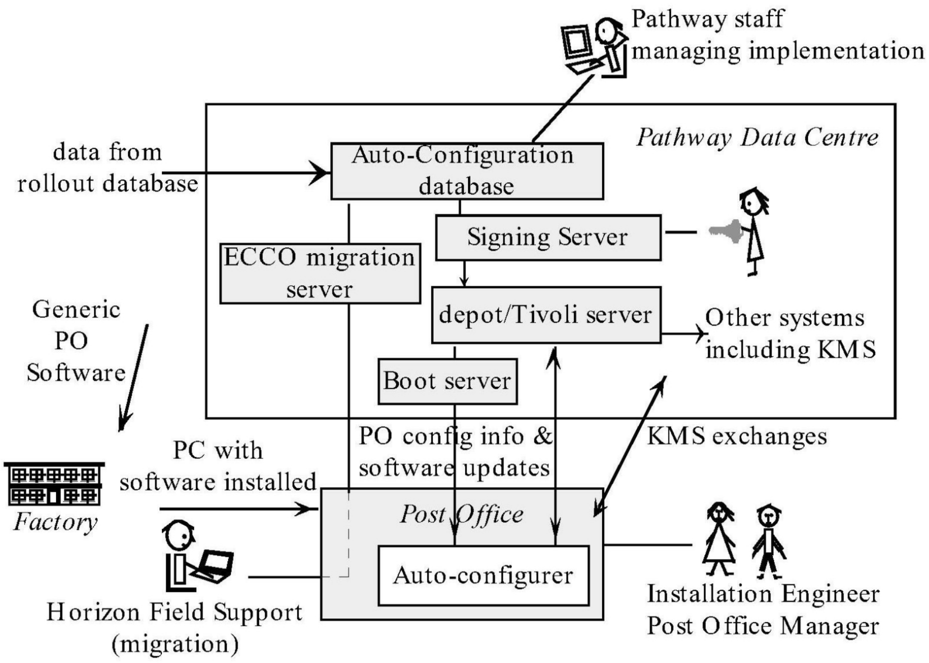


Figure 5-2 Interactions on Post Office Implementation

5.12.1.1 The PCs should be delivered from the factory conforming to an agreed build with software, including an Auto-configurer application, installed.

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

- Implementation staff in regional centres connecting to the RODB via modems will be restricted to read only SQL access to the RODB.
- Implementation suppliers will be restricted to (FTMS controlled) file transfers between a Pathway PC at the suppliers site at the RODB.

5.12.1.3 ECCO migration laptops can only connect to the migration server at the Data Centre

6. ROLES AND PERMITTED ACCESS

This chapter specifies all human roles with access to the Pathway Data Centres and the other Pathway managed systems such as the interface PCs at POCL and De la Rue sites.

For each role, the following table outlines the job functions performed and also the IT functions and resources accessed to carry out these roles, including which systems are accessed. The table is ordered into:

- Main operational roles (Post office staff, payment card helpline staff and BA staff on-line via CAPS)
- Corporate management roles (Pathway business management, customer services including business support, FRM related roles including BA security, Pathway security roles including cryptographic key ones and auditor roles including POCL, DSS and NAO auditors)
- Implementation roles (implementation help desk, ACDB roles, Horizon field support officers)
- System and operational management and support roles (operational management on Sequent, NT etc, SMC system management, software distribution, network and firewall management, application support and other support roles)

In the following table:

- The site type is:
  - DC for Data Centre
  - PPS for a Pathway project site
  - SL/PPS for secure LAN at a Pathway project site
  - PO for Post Office
- The system is:
  - Seq for all Sequent systems
  - DW for Data Warehouse
  - HS for the Host Application Sequent system

Unless otherwise stated, users access the system via controlled NT workstations, logging into the appropriate NT domain.

Role (Organisation)	***Main job functions***	***IT functions & data access***	***Systems accessed***
Main Operational Roles			
Post Office Staff and Customers at Post Offices			
Post Office Manager (The person in charge of the Post Office, who may be a sub-postmaster or agent.) (POCL)	All the management of the Post Office system including setting up workstations, introducing users, doing accounts. Post Office Managers may allow other staff to deputise for them, and so take this role. Workstation set-up, emergency procedures, installation functions.	Key (and memory card) custodian - installing, changing and recovering keys. User management (of local post office staff). Specific management applications, for example, balancing Post Office accounts and stock unit management (including allocation to clerks) Run diagnostics to check system and peripherals are functioning correctly. All counter clerk functions.	Post office only
Post Office Counter clerks (POCL)	Run the PO applications - APS, EPOSS, OBCS and BES. Do training. Contact the Payment Card Helpline when required.	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. Stock unit balancing etc. In training mode, special training data (counter clerk also uses special training benefits/APS cards so does not need a customer present)	as above
Post Office Supervisor (POCL)	All Counter Clerk functions plus other functions.	As Counter Clerk plus viewing stock, users.	as above
Customers	Transactions at Post offices e.g. buying stamps, collecting benefits, paying utility bills.	**Customers** do not access the system directly, though their benefit card is needed for benefit collection.	None directly, but card used for IT access

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
Payment Card Helpline staff (all Girobank staff at the PCHL area of the main Data Centre sites)			
Helpline Advisor	Handling calls about payment authorisations and cards from Post Office clerks, DSS/BA, customers and the general public. This could lead to, for example, stopping a payment or encashing a payment (under the responsibility of the Post Ofice clerk)	Oracle Forms to support helpline job functions using particular PAS & CMS tables as required for the authorised Oracle Forms (with sufficient write access to allow cards to be stopped, update call logging tables and change password.)	HS:PAS/CMS + training database
NSI Helpline Advisor	As above, plus can handle customer data with a Nationally Sensitive Indicator.	As above, plus can handle data with a Nationally Sensitive Indicator.	as above
Helpline supervisor	As above, plus extra functions, including local help desk ones	As a Help Desk Advisor, plus the ability to handle NSI data and other more restricted dialogues.	as above
Helpline Security Manager	Maintains information about the Helpline users both at the PAS/CMS and local systems	Functions as Helpline Advisors +create PCHL users and assign/re-assign their PCHL roles via authorised Oracle Forms accessing Oracle user and role tables	as above
BA staff on-line (all DSS staff at DSS sites using VME terminals/workstations)			
BA staff & DSS Help Desk staff	BA staff do on-line transactions, for example, to make emergency payments or stop cards or payments. DSS Help Desk staff do on-line queries e.g. on authorised payments.	Users of the CAPS on-line interface appear as a system user to the PAS/CMS application.	PAS/CMS
Corporate Management Roles			
Pathway Corporate Management Roles and associated support roles (all Pathway staff on secure LAN at Pathway management site)			
Pathway Management support	Managing the set-up of the management information services (e.g. setting up Business Object Universes and associated controls). Providing information to other Pathway	Business Object Universes (including supervisor functions); Read and update access to agreed MIS data including CON, SLAM, BPS;	DW; other MIS e.g. NT SLAM cache?

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
	Management users on request Also, providing the POCL and the DSS/BA interfaces for management information - including provision of management data regularly and on request.	Data required for download to workstations for reports (pathway, POCL, BA)	
Pathway Financial Management	Use of financial management information in the Common Charging System and elsewhere	Access to Common Charging System (CCS) and other financial information	DW
Pathway Contract Management	Use of contract management information in the Contract Management system (CON)	Access to CON service	DW
Pathway Business Development	Use of selected Data Warehouse information in development of the business	DW: read only access to Post Office information	DW
Pathway Customer Services, including Business Support (mainly Pathway staff on secure LAN at Pathway management site)			
Pathway Customer Support Managers	Service Level agreement management	Read only access to SLAM cache on NT only;	NT SLAM cache only
Business Support Manager	*Unit function* Handle financial reconciliation when there is a Pathway problem, for example a service breakdown. This could be reconciliation incidents for DSS benefit payments, or reconciliation incidents for in the Automated Payments Service for other POCL clients. *Role function* Inserting or adjusting payments and authorising them, subject to agreed procedures.	Access to the RED database holding data about cases needing reconciliation. For DSS payment reconciliation: PAS/CMS and OBCS, and TPS (PO transaction logs) For APS reconciliation: APS and TPS All update access is via specific Oracle forms applications. (Where larger volumes are concerned, relevant data may need to be downloaded at the request of Business Support to the SSC reference system and a flat file of transaction adjustments generated there for forward transmission to the Data Centre and back to CAPS by	HS: PAS/CMS, OBCS, APS Correspondence server RED database

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
		SSC.)	
Business Support Analyst	Investigating incidents, and inserting or adjusting payment records (but not finally authorising them.)	Access to PAS/CMS, TPS etc and also to the reconciliation (RED) database - a secure server at the management site.	as above
Pathway Reference Data Management	Use of reference data in the Data Warehouse	Access to DW reference data	DW
Reference Data Change Manager	Kick off the transfer of validated reference data of classes 2 to 5 to TMS when all required dependencies have been met.	(Oracle role: user_change_control)	HS:RDMC
RDMC Loader	Manually initiated load of reference data files to RDMC	(Oracle role: user_loader)	HS:RDMC
RDMC user	Query and report on reference data, so read only access	(Oracle role: user_reports)	HS:RDMC
RDMC access administrator	Sets up users and assigns them their roles	(Oracle role: user_administrator)	HS:RDMC
Fraud Risk Management Related Roles			
Pathway Fraud Risk Manager (ICL Pathway staff, high security LAN, Pathway management site)	*Unit & role functions* Regular reports on aspects of the system which are relevant for fraud e.g. weekly trend analyses and daily exception reports and ad hoc selective reports according to agreement. Investigating fraud cases. Fraud investigations will also include collection of evidence. Some evidence will be collected by requesting information from other users, rather than direct FRM staff access.	Access to the Fraud Case Management System (FCMS), both to create and maintain cases originated by Pathway and to read case data about cases originated by BA Security. Access to Data Warehouse information, both pre-defined and ad-hoc queries. Exceptionally, access to other systems to investigate a potential fraud i.e. PAS/CMS data (mainly to the archives, not the operational system), the Riposte journal of Post Office activity, data transfer logs	DW: FCMS HS: PAS/CMS NT: TMS DW: logs

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
		Supervisor of FCMS and also FRM Business Object universes, so create/expire users in FCMS. Setting flags for transactions in FCMS (code user).	
FRM Analyst (ICL Pathway, as above)	Investigating fraud cases as FRM manager	Access to FMCS and other systems c.f. FRM Manager FRM supervisor functions as FRM manager	as above
FRM users (P'way, & Girobank FRM)	Handling fraud case information in FCMS	Read only access to Data Warehouse information in support of investigations.	DW:FCMS
BA Security (DSS, DSS secure site via encrypted link)	Investigating cases, including staff creating and maintaining their own cases in the Fraud case database.	Read and update access to cases initiated by BA Security; Read only access to cases initiated by Pathway FRM staff (but not access to Pathway specific information). Access to extracts of Data Warehouse information (extracted by Pathway FRM staff.); no direct DW access	DW:FCMS
Pathway Security and Cryptographic key roles			
Pathway Security Manager	Maintains the records of security tokens and their PINs and users.	Maintenance and audit functions at the ACE server	ACE server
Cryptographic Key Manager	Generating or obtaining cryptographic keys and organising their distribution.	Also viewing current situation re keys (KMA) and generating certificates to certify keys (CAW)	KMA, CAW
Cryptographic Key Custodian	Initial installation of cryptographic keys where this needs to be done manually. Periodic update of these keys.	Installing keys where needed (VME, PAS/CMS, interfacing PC (Data Centre and remote), KMA, (CAW), VPN??. Always local user, not remote.	See IT functions column
Cryptographic Key Handler (Note 3)	Handling part of a split cryptographic key when this needs to be re-installed e.g. when a system is rebooted.	Loading part key (normally from floppy) during load, so no logon, no individual authentication.	As key custodian

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
PO key recoverer (part of SMC team leader role)	Initiating recovery of a Post Office key from the Help Desk after a Post Office Manager has lost his card or PIN.	Authorised functions at KMA *[method for accessing this not yet agreed; e.g. is there trust between SMC and main Data Centre domain?]*	KMA
KMA Data Manager	Maintain validity of data within KMA database e.g. specify new client where keys are to be sent (but no key management roles)	Authorised functions at KMA	KMA
Auditor Roles			
Pathway Business Function Auditor	Overall auditing of the Pathway solution	(though not Post offices directly, as there are records of Post Office activity at the Pathway central site.) The Business Function Auditor mainly uses information to the archive server and to information extracted from other systems, though has limited access to other systems.	Archive server; exceptionally, correspondence servers, PAS/CMS etc
Pathway Security Event Auditor	Auditing the security of the Pathway system including monitoring, investigating incidents, reporting etc	• Operational and management logs of business transactions including Riposte journal for events at Post Offices and host application logs e.g. PAS/CMS • System logs of activities at Pathway systems such as user logon and administration and other security relevant events including system, network and firewall management. • Logs at relevant Pathway internal systems. • Archives of these at the archive server retrieved from the Legato tapes there • Manual records associated with IT access.	Most except Post offices

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
		Many events are collected centrally using Tivoli (via Patrol and Openview where needed). The technician monitoring the systems management workstation will alert the Security Event Auditor of specified types of significant events. However, some event records will remain in local audit logs.	
POCL Auditor	Auditing operation of a Post office	Authorised Riposte functions after authentication using one shot password	Post offices only
POCL Emergency Manager; POCL Investigator	Taking 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.	Post office start up functions Authorised Riposte functions after authentication using one shot passwords	Post offices only
External Auditor	A POCL, DSS or NAO Auditor auditing the operation of Pathway	External auditors have (indirect) access via Pathway Auditors, rather than direct access to the Pathway systems. There are some differences in data available to different External Auditors. For example, DSS staff cannot access POCL specific data.	None
Implementation Roles with Data Centre access			
Implementation Help Desk /Roll-out support/help desk advisors (P'way)	Handle calls from Pathway suppliers and Post Offices - forwarded from Horizon system help desk. Queries and limited updates to RODB depending on call	Query and update access to RODB as permitted by RODB client	RODB at Pathway management site
Auto-configuration user (Pathway)	Implementation staff managing the data going through the auto-configuration database (ACDB). This includes some update access.	Query access plus update as permitted by ACDB/client	ACDB
ACDB data	Administering the central services site	Query access plus update as permitted by	ACDB

Role (Organisation)	***Main job functions***	***IT functions & data access***	***Systems accessed***
administrator	information in the ACDB	ACDB/client	
Horizon Field Support Officer (POCL?)	Handling migration - two roles for manual and ECCO migration	For manual migration, migration application at Post Office. For ECCO migration, job to transfer ECCO data to TMS journal	PO counter; laptop, & via PO gateway to migration server
Installation engineer	Start-up Post offices	auto-configuration application only	PO links to boot server
System and Operational Management and support			
Operational Management			
Computer Operator	Local operation of the machine such as media handling.	On Sequent, the ability to run pre-defined jobs, such as back-ups. On NT, media handling only, including legato tapes used for archiving	
Operational management/ System Administrator (ICL Outsourcing)	Management of the operating system; On Sequent, any action needed concerned with replication between campuses and local archiving. Job scheduling (Sequent & NT) using Maestro workstation. Code updates when required quickly (prior to update via configuration management) and authorised	Access to required operating system functions. On Sequent, this can allow use of ROOT, UNIX commands and Oracle dba functions under controlled conditions (see 5.2) Operational monitoring/management using Patrol workstations.	All Seq all NT (except PO) all Solaris
Security Management (ICL Outsourcing)	Administering UNIX/NT user information, including group membership for all users; also, on Sequent, in secure menu system.	User administration and related functions	All Seq NT (not PO) Solaris

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
	Administering Oracle database administrator users and associated roles and privileges.?? Security monitoring		
Secure menu administrator (Sequent only)	Configuration of the secure menu system, including addition of new functions	Pre-defined agreed functions	Seq
System Monitoring (Sequent only)	Monitoring the operational system.	Patrol via an appropriate workstation	Seq
Engineer	Hardware diagnostics and repair	Access to diagnostics and, if needed, data on suspect hardware	all systems except PO
Base Installation and configuration	Initial installation and configuration the base system - Sequent and Oracle databases. Later updates to these.	As job function for Data Centre systems and Pathway managed systems, except Pos where there is a special installtion engineer	
Dynix 3rd line support	Operational management of Dynix by Sequent staff when CFM cannot cure problem.	UNIX, which can include ROOT access?	Seq
Database monitor	Monitoring Oracle databases	Read only access; on Oracle, use of SQL*Plus, svrmgr	Seq
Operational management/ Database administrator	Oracle database administrator for database structure - setting up views, space allocation etc.	Dba functions for specified applications (CFM_DBA role)	Seq
Oracle database 3rd line support	Operational management of Oracle on Sequent when CFM cannot cure problem. This may sometimes require updating the database.	Read only access; Oracle dba and limited UNIX functions	Seq
Legato Administration	Managing the audit archives	Legato archives via Legato client	Archive server

Role (Organisation)	***Main job functions***	***IT functions & data access***	***Systems accessed***
System Management - SMC roles			
System Management Centre	*Unit functions* System management activities are: • planned system management actions, for example, the distribution of software or the implementation of Post Offices. • monitoring the system and taking action when this is needed. • resolving technical problems passed on by the Horizon System Help Desk They also handle PO key recovery.		
SMC technician or technical specialist	Monitoring the system - software distribution, the auto-configuration process and other system management events. For software distribution, select targets for distribution from those authorised and report of progress. Run pre-defined, pre-allocated tasks. Raise alarms on pre-defined conditions	Tivoli/Oracle facilities for authorised functions. (No NT/UNIX tools) Pre-defined Tivoli tasks can be used for a variety of system management tasks including Riposte administration at the Correspondence servers.	Tivoli servers via Tivoli client
SMC technical team leader	For software distribution, authorise targets for distribution, change priorities or cancel distribution and report on progress. Other system management tasks as SMC technician. Authenticating users at the Post Office using	Tivoli/Oracle facilities for authorised functions. (No NT/UNIX tools) For one-time password authentication, special security system with access to special application only For PO key recovery, application at KMS	Tivoli servers via Tivoli client; (KMA for PO recovery)

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
	one-shot passwords. Assisting in Post Office key recovery.		
SMC MSS technical support	Handle receipt of software and auto-configuration information. Configure Tivoli event management - configure the view of events by others and task event relationships and add new Sentry monitors. Create Tivoli tasks and allocate to SMC technicians. System administration of the SMC workstations and Tivoli servers (NT and UNIX systems) including backup/recovery.	Tivoli/Oracle facilities for authorised functions. Authorised NT/UNIX tools	Tivoli servers via Tivoli client
SMC Security Manager	User administration - adding SMC and other users to the SMC domain and to Tivoli. Allocating users' rights e.g. roles, groups.	Tivoli and OS user and role administration	Tivoli servers via Tivoli client
Software Distribution			
Software Distributor	Initiates transfer of software to the depot/ Tivoli at the Data Centre for distribution to the operational system after authorisation by CS Release Manager.	Functions at signing server to initiate transfer *[is this split between CM and signing server still correct?]*	signing server? at Pathway project site
Network Management			
Network Technician (CFM)	Monitoring the network	Specified Open View and Cisco Works/CiscoView functions and the NMS only. (No direct UNIX access)	NMS
Network Manager (CFM)	Monitoring the network. Updating router configuration information e.g.	Open View and Cisco Works network management functions, but no direct UNIX access at the NMS	NMS

Role (Organisation)	*Main job functions*	*IT functions & data access*	*Systems accessed*
	- Post Office information e.g. ISDN address - Access Lists of permitted addresses, protocols, ports. Updating information about routers available when needed (including confirming bringing a mended one back on line - see 8.5.5 below)		
Network Management Configurer (CFM)	Configuring NMS including Open View e.g. - what to display to whom - actions to be taken on certain events Configuring Tivoli Event Adapter	Open View configurer functions only (no UNIX access)	NMS
Network 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	User administration functions	NMS
Cisco support	nth line support of routers	Telnet access to routers	routers
Firewall Management			
Firewall Manager	Maintains the firewall configuration and policy data	Defined as NT & Enterprise centre user; Authenticated with token to NT workstation, and authenticated to the Enterprise Centre application.	Enterprise Centre on Solaris system
Firewall Monitor	Read access to alerts, logs and the rule base	as above	as above
Technical Help Desk and Application and other Support			
Horizon Systems Help Desk	Receiving technical queries from all IT users of Pathway (internal and external) and answering	These users has no access to the main Data Centre and other operational systems.	Internal systems only

Role (Organisation)	***Main job functions***	***IT functions & data access***	***Systems accessed***
	queries on these calls. Answering some technical queries and forwarding other calls on to the appropriate 2nd line support unit. Notes, this includes forwarding calls on PO key and password recovery to SMC.	They have access to supporting services such as Powerhelp for call handling and special versions of Pathway (Post Office) applications (without real data etc) to assist answering calls from Post office staff.	
Application support user	Supporting applications on Sequent - both Oracle applications and Access services.	Read only access to event logs and other relevant files and databases. (This does not include the Post Office counters, and Tivoli server access is restricted to pre-authorised tasks to extract diagnostic info for POs *[any others?]*) (Oracle MONITOR role on Sequent)	Most NT Sequent; test rigs
Application support manager	Supporting applications as above, plus correcting data when required and authorised under controlled conditions.	As above, plus controlled write access to application data (Oracle SSC role on Sequent)	as above
Application support - VME applications	Support of applications in the Pathway VME partition	Using Sonnet on Sequent to access the Pathway partition on DSS VME systems	Sequent VME
Application 3rd line support	Supporting Oracle applications	Read only access	Seq
Other hardware and system support			
EMC	Handling problems with Symmetrix discs	Access to EMC disc controller (and to discs) using special EMC client	EMC

Notes:

1. This table does not include the Software distribution related roles at the Configuration Management system, as these as the CM is not on the secure LANs covered by the ACP. Roles are

  - CS Release Manager (authorising software (new software and fixes), configuration information etc for release (after testing at the test rigs)
  - Configuration librarians (maintaining the library of software at the Configuration Management system and initiating signing and distribution of software after authorisation)

2. This table also does not include RODB roles, since that is now intended to remain at the Pathway management site (with firewalls protecting other sites from it, and the implementation suppliers). Roles are:
   - Roll-out/RODB users (Implementation staff viewing information in the roll-out database)
   - RODB data administrators (Implementation staff also able to update RODB data, for example, change the date for a Post office installation.)
   - Implementation suppliers (bulk transfer only from Pathway managed PCs)
3. The Key Handler role needs to be performed on-site whenever systems are rebooted, so is generally performed by the organisation at that site e.g. EDS at DSS sites, POCL at their sites, De La Rue at their sites

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

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

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