FUJ00087988

Document Title:	Security Functional Specification
Document Type:	Specification
Abstract:	This Security Functional Specification (SFS) defines the security functionality that will be incorporated into the operational ICL Pathway system.
Distribution:	DSS POCL ICL Pathway ICL Pathway Library
Document Status:	Approved
Document Predecessor:	-
Associated Documents:	See section 0.2
Author/Editor:	Peter J Harrison and Tom Parker
Approval Authority:	Martyn Bennett
Signatures/Dates:	
Comments To:	Authors, copy to Martyn Bennett
Comments By:	-

FUJ00087988

0. CONTENT

0.1 Document History

Version	Date	Reason
0.1	15/8/96	Initial Draft for internal review
0.2	16/8/96	Incorporates comments from internal review
0.3	20/9/96	Incorporates comments from CASA
0.4	24/9/96	Incorporates comments from internal review
0.5	10/10/96	Incorporates comments from PDA
1.0	23/10/96	Submitted for formal approval
1.1	4/11/96	Minor changes incorporated
2.0	11/11/96	Approved
2.1	25/2/97	Incorporates Energis inter-site link, Data Warehouse, virus protection, etc
2.2	19/6/97	Incorporates revisions to Security of Links, Message Protection and Filestore Encryption.
2.3	15/7/97	Incorporates revisions to Audit and Alarms.
2.4	31/7/97	Incorporates revisions following review by PDA.
3.0	3/12/97	Approved

0.2 Associated Documents

Reference	Identifier	Vers.	Date	Title
SADD	CR/FSP/0004	2.0	27/9/96	System Architecture Design Document
SECPOL	RS/POL/0002	3.0	8/10/96	ICL Pathway Security Policy
SECOBJ	RS/REQ/0001	1.0	29/10/96	ICL Pathway Security Objectives
ACCPOL	RS/POL/0003	1.0	17/4/97	ICL Pathway Access Control Policy
AUDPOL	RS/POL/0004	0.4	3/4/97	ICL Pathway Audit Policy
AUDFS	CR/FSP/006	2.1	19/5/97	Audit Trail Functional Specification
CDS	RS/DES/0001	1.0	1/10/96	Cryptography High Level Design Specification
RIPSDS	*TBD*	-	-	Riposte Security Design Specification
TED	TD/ARC/0001	2.0	-	Technical Environment Description
SECSTD	*TBD*	-	-	ICL Pathway Security Standards
DBA	Oracle	-	-	Oracle Server Database Administrator's Guide
DYNIX	Sequent	-	-	Dynix Operating System - System Administrator's Reference Manual
WINNT	Microsoft	-	-	Microsoft Windows NT Resource Guide

FUJ00087988

ITSEC	ITSEC	-	28/6/91	IT Security Evaluation Criteria

0.3 Abbreviations

ACC	Area Computer Centre
API	Application Programming Interface
APS	Automated Payment Service
BA	Benefits Agency
BES	Benefit Encashment Service
BPS	Benefit Payment Service
CA	Certification Authority
CAPS	Customer Accounting and Payments Strategy
CAS	CAPS Access Service
CESG	Communications-Electronic Security Group
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Indication
CMS	Card Management System
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CRC	Cyclic Redundancy Check
DBA	Database Administrator
DLL	Dynamic Link Libraries
DLR	De La Rue
DSD	Distributed System Division (ex Sorbus, now CFM)
DSS	Department of Social Security
EDSC	European Development Support Centre
EPOSS	Electronic Point Of Sale Service
FRM	Fraud Risk Management
GRK	Global Roll-out Key
HAPS	Host Automated Payments System
ID	Identity
ISDN	Integrated Services Digital Network
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
KMS	Key Management System
LAN	Local Area Network
MIS	Management Information Services
NAO	National Audit Office
NDIS	Network Device Interface Specification
NMS	Network Management System
OBCS	Order Book Control Service
OLAP	On-line Analytical Processing
OLE	Object Linking and Embedding
OMG	Object Management Group
OPS	Office Platform Service
PAS	Payment Authorisation Service
PFI	Private Finance Initiative

FUJ00087988

PK	Public Key (for PK Certificate)
PO	Post Office
POCL	Post Office Counters Ltd
POM	Post Office Manager
PSI	POCL Service Infrastructure
PUN	Pick Up Notice
RPC	Remote Procedure Call
RCD	Release Contents Description
SADD	System Architecture Design Document
SFS	Security Functional Specification
SHA	Secure Hashing Algorithm
SIS	Strategic Infrastructure Service
SM	System Management
SMS	System Management Service
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
SQL	Structured Query Language
TFTP	Trivial File Transfer Protocol
TIP	Transaction Information Processing
TME	Tivoli Management Environment
TMP	Tivoli Management Platform
TMS	Transaction Management Service
UDP	User Datagram Protocol
VME	Virtual Machine Environment

Abbreviations of Post Office cryptographic key names have been included in Appendix C.

FUJ00087988

0.4 Table Of Contents

FUJ00087988

FUJ00087988

FUJ00087988

FUJ00087988

FUJ00087988

1. INTRODUCTION

1.1 Purpose

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

1.2 Context

There are three broad categories of security controls, as illustrated in Figure 1-1.

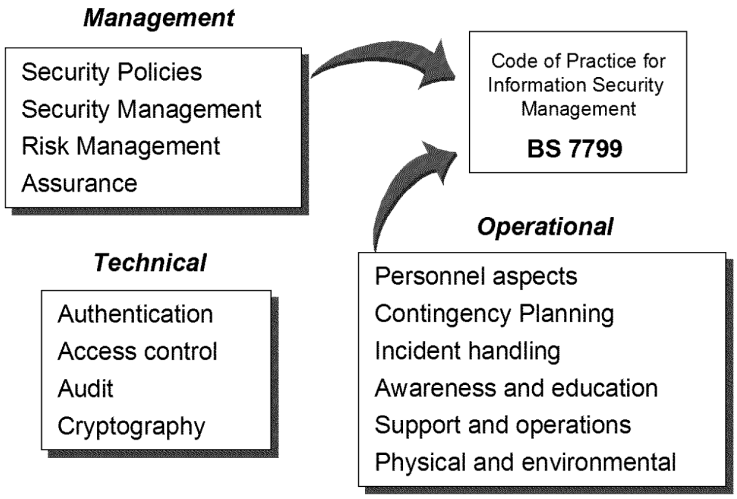

Figure 1 - 1 Security Control Categories

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

BS 7799, “A Code of Practice for Information Security Management”, is primarily concerned with management and operational controls. It will be supplemented with additional standards to define the management and operational controls used throughout ICL Pathway [SECSTD].

FUJ00087988

1.3 Scope

This Security Functional Specification (SFS) identifies the technical controls that will be used to implement the security functionality within the ICL Pathway system [SADD].

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

Commercial off-the-shelf (COTS) components have been used as the primary building blocks throughout ICL Pathway's solution. This will reduce the need for bespoke code and enable the suppliers' standard product documentation to be used.

An overview of the security functionality, provided by the security components (identified in section 4), has been included in order to define the security features and system options that will be used.

Details of the parameters required to provide secure operation of the system in various environments will be defined elsewhere [ACCPOL].

1.4 ICL Pathway's Security Policy

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

By implementing the agreed Security Policy, ICL Pathway will minimise and control liabilities to itself and the Authorities. The Security Policy also explains how ICL Pathway will comply with the controls defined in BS7799.

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

1.5 Document Structure

This document specifies security functionality within a framework of explanatory text. The response to each requirement, with any associated continuation paragraphs, is numbered and indented. The numbering scheme corresponds to fourth level headings so that responses, if extracted, can be related back to their original context.

References to the associated documents, listed in section 0.2, are indicated by the document reference name in square brackets (e.g. [SADD]).

FUJ00087988

Cross references, to the original BA/POCL Requirements, have been included, wherever possible, In Appendix B.

2. MANAGEMENT SUMMARY

2.1 About this Document

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

2.2 Security Domains

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

- DSS Service Environment Domain,
- PAS/CMS Service Domain,
- POCL Central Systems Domain,
- Office Platform Service Domain,
- De La Rue Card Services Domain,
- POCL and POCL Clients Domain,
- System Management Service Domain, and
- ICL Pathway Corporate Services Domain.

The Benefit Payment Service (BPS) maps onto the DSS Service Environment, PAS/CMS Service, POCL Central Systems, De La Rue Card Services and Office Platform Service (OPS) domains.

The DSS Service Environment Domain encompasses all ICL Pathway related equipment and services located at DSS/BA sites.

The PAS/CMS Service Domain encompases the Payment Authorisation Service (PAS) and the Card Management System (CMS).

The Office Platform Service Domain encompases the Electronic Point Of Sale Service (EPOSS), which supports all services, or products, provided by the counter clerk to the customer. For BPS, EPOSS supports the Benefit Encashment Service (BES) within the Post Offices.

FUJ00087988

The De La Rue Card Services Domain encompasses the production of cards and Pick Up Notices (PUNs).

The POCL and POCL Clients Domain will contain a variety of hosts associated with applications running in the OPS Domain.

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

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

2.3 Security Components

The security enforcing components within the ICL Pathway system are Windows NT, Dynix operating system (on Sequent platforms), Oracle 7 database products, networking components and encryption devices.

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

Virus protection facilities will be installed on selected workstations, primarily within the SMS Domain.

2.4 Identification and Authentication

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

This SFS, therefore, defines overall requirements for user identification and authentication followed by specific consideration of users of NT, Oracle, Help Desk operators, DSS/BA and POCL staff.

2.5 Logical Access Control

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

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

FUJ00087988

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

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

2.6 Audit and Alarms

The audit and alarm facilities provided by the ICL Pathway system will be a combination of application level transaction logs and lower level audit logs.

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

Patrol will be used to manage all Sequent systems and the Oracle applications which run on Sequent platforms.

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

2.7 Crypto Functionality

This SFS describes the cryptographic functionality, within the ICL Pathway system, used to protect:

- data on individual communications links,
- individual messages from creation to use (end-to-end), and
- data stored on physically insecure Post Office filestore.

Key management and the special requirements of roll-out are also covered.

The “CAPS Links”, from BA’s CAPS system to ICL Pathway’s CAPS Access Service, will be protected using strong cryptographic integrity protection. This will be provided using one of two means:

- use of Rambutan encryption hardware at each end of the link, or

FUJ00087988

- use of a Red Pike encrypted secure hash, produced using SHA, implemented in software at each end of the link.

For reasons discussed in section 8.1.2, ICL Pathway will use the Release Contents Description (RCD) mechanism to seek concessions to defer strong protection of this link until a subsequent release. The interim solution uses the CAPS generated Cyclic Redundancy Code (CRC) and the set of totals for financial data. These are be encrypted, using Red Pike, before transmission and checked upon receipt at the ICL Pathway campus. No protection will be provided on files sent from ICL Pathway to BA locations on the CAPS link.

The “CMS links”, used to transfer card production data to the card producer, will be protected using Red Pike. All data on these links will be encrypted for confidentiality and integrity.

ICL Pathway’s inter-campus links, between the Wigan and Bootle sites,
are very high speed (34Mbps) connections, which gives them a significant level of inherent security. There is, currently, no suitable encryption hardware capable of operating at this speed, so particularly sensitive data will be protected using Red Pike.

Integrity of data on the “POCL TIP link” will be protected through strong cryptographic means. This will be provided using one of two means:

- use of Rambutan encryption hardware at each end of the link, or
- use of a Red Pike encrypted secure hash, produced using SHA, implemented in software at each end of the link.

Rambutan encryption hardware capable of supporting high speed communications over ATM and Frame Relay links is not currently available. The Red Pike secure hash option will, therefore, be implemented.

ICL Pathway will use the RCD mechanism to seek concessions to defer strong protection of this link until a subsequent release.

The kilostream “POCL HAPS link”, to Farnborough, will be protected using Rambutan based encryption hardware.

FUJ00087988

The Host Automated Payments System (HAPS) is an interim solution, whereby all AP data will be sent to an existing POCL Tandem system sited at Farnborough. In the future, the ICL Pathway system will communicates directly with POCL customers (rather than indirectly via HAPS) using the "POCL links".

The "SM/SIS links" used, by ICL Distributed System Division (DSD) and ICL CFM, for support and system management, will be protected using Government approved point-to-point encryption devices employing the Rambutan algorithm.

Links from the ICL Pathway headquarters site, at Feltham, to the ICL Pathway campuses, at Wigan and Bootle, will also use Government approved point-to-point encryption devices.

The "Post Office ISDN links" from the POCL Central Services Domain to the Post Offices will use CHAP connection authentication, supplemented by CLI authentication of the Post Offices from the ICL Pathway campus.

The roll-out and key management aspects, particularly for the Post Office Integrated Services Digital Network (ISDN) links, have been given very careful consideration to achieve the optimum design.

2.8 Message Protection

All message protection will be performed using DSA with a 768 bit modulus. Each DSA signature requires a cryptographically strong random initialisation value, known as a K-value.

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

BES payment authorisations will be digitally signed on leaving the PAS/CMS machine. Signatures will be verified immediately prior to use by the BES application in individual workstations at the Post Offices.

Automated Payments will be signed in the Post Office for verification by a receiving agent at the POCL HAPS (and in the longer term, direct to POCL Clients).

FUJ00087988

2.9 Filestore Encryption in Post Offices

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

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

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

2.10 Administration of Security

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

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

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

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

3. SECURITY DOMAINS

3.1 Domain Definition

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

FUJ00087988

- type(s) of service provided,
- components used (e.g. VME, Oracle, Dynix, NT), and
- area of responsibility (e.g. ICL Pathway, BA, POCL).

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

The services offered by several domains combine to provide the end-to-end services, namely:

- Benefit Payment Service (BPS), and
- Post Offices Infrastructure Service(POIS).

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

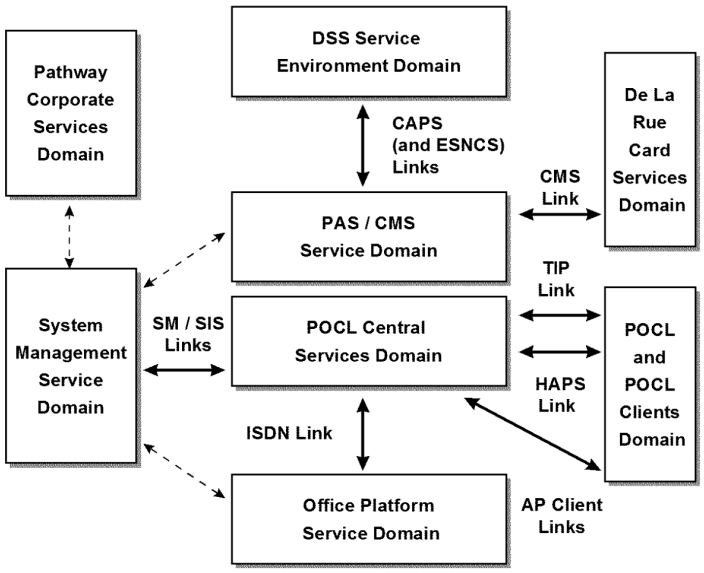

Figure 3 - 1 Communications Links Between Domains

Figure 3-1 illustrates the primary communications links between the domains. These links, which are the external connections to the ICL Pathway central sites, will be protected to preserve the integrity and confidentiality of information handled by the system.

Where domains encompass two or more geographic locations, the external links between sites will be protected. This applies primarily to the inter-site links between ICL Pathway's sites at Wigan and Bootle.

FUJ00087988

The authentication, access control and audit functionality, described in sections 5, 6 and 7, will apply to all domains for which ICL Pathway has responsibility. The crypto functionality and message protection mechanisms, specified in sections 8 and 9, have been described for each type of link.

3.2 The DSS Service Environment Domain

The DSS Service Environment Domain is illustrated in figure 3-2.

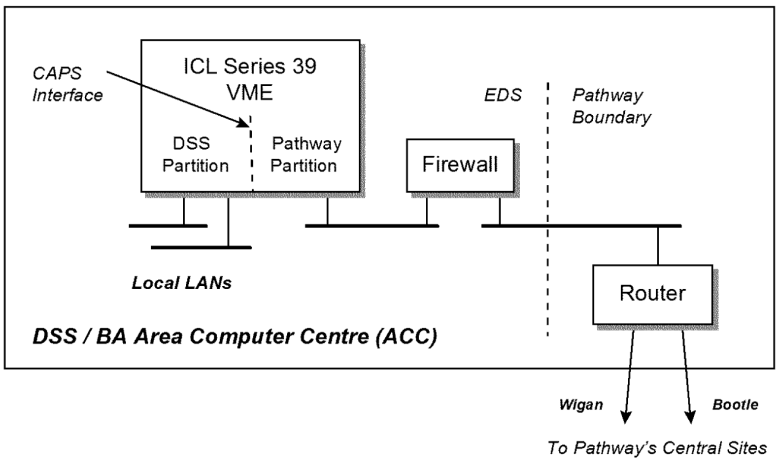

Figure 3 - 2 DSS Service Environment Domain

The ICL Series 39 machines are used for the DSS Customer Accounting and Payments Strategy (CAPS) system which handles automated payment authorisations. The associated DSS Electronic Stop Notice Control System (ESNCS) will handle Order books for benefits.

The network configuration illustrated in figure 3-2 is simplified and the ESNCS, which is at only one of the four ACC sites is not shown.

CAPS will be partitioned such that information, generated for and returned by ICL Pathway, has a clearly defined boundary. ICL Pathway's responsibility in this domain is to accept Benefit related data generated by CAPS (or ESNCS) and return data to CAPS (or ESNCS).

EDS, who will manage CAPS within the DSS/BA sites, will maintain firewalls to protect their mainframes from unauthorised access from the external (including ICL Pathway) sites.

FUJ00087988

3.3 The PAS/CMS Service Domain

The PAS/CMS Service Domain will span two sites (Bootle and Wigan) which are often referred to as ICL Pathway's Data Centres or campuses.

The logical components within this domain are illustrated in figure 3-3.

The CAPS Access Service (CAS) will support the file transfer to/from the DAA/BA systems in the PAS/CMS Service Domain.

The PAS and CMS applications will use the same Oracle database which runs on Sequent hardware with the Dynix operating system.

PAS Help Desks and CMS Help Desks will be based upon Windows NT platforms with the Client applications used to access the Oracle database.

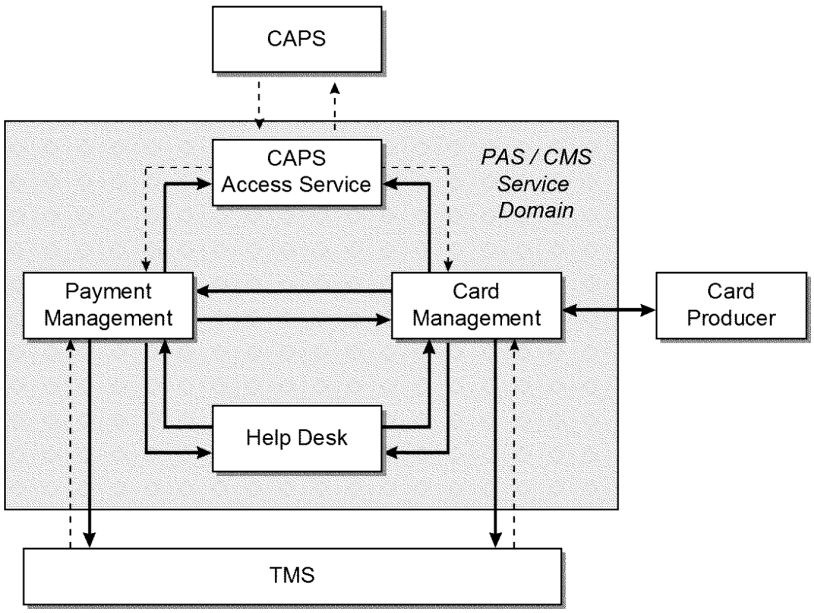

Figure 3 - 3 PAS/CMS Service Domain

3.4 The POCL Central Services Domain

The POCL Central Services Domain contains the ICL Pathway application hosts at the central ICL Pathway sites. These hosts support the Post Office APS, EPOSS and OBCS applications.

All applications will run on Sequent machines with Oracle databases.

FUJ00087988

The POCL Central Services Domain will interface with the PAS/CMS Service Domain and the OPS Domain as illustrated in figure 3-4.

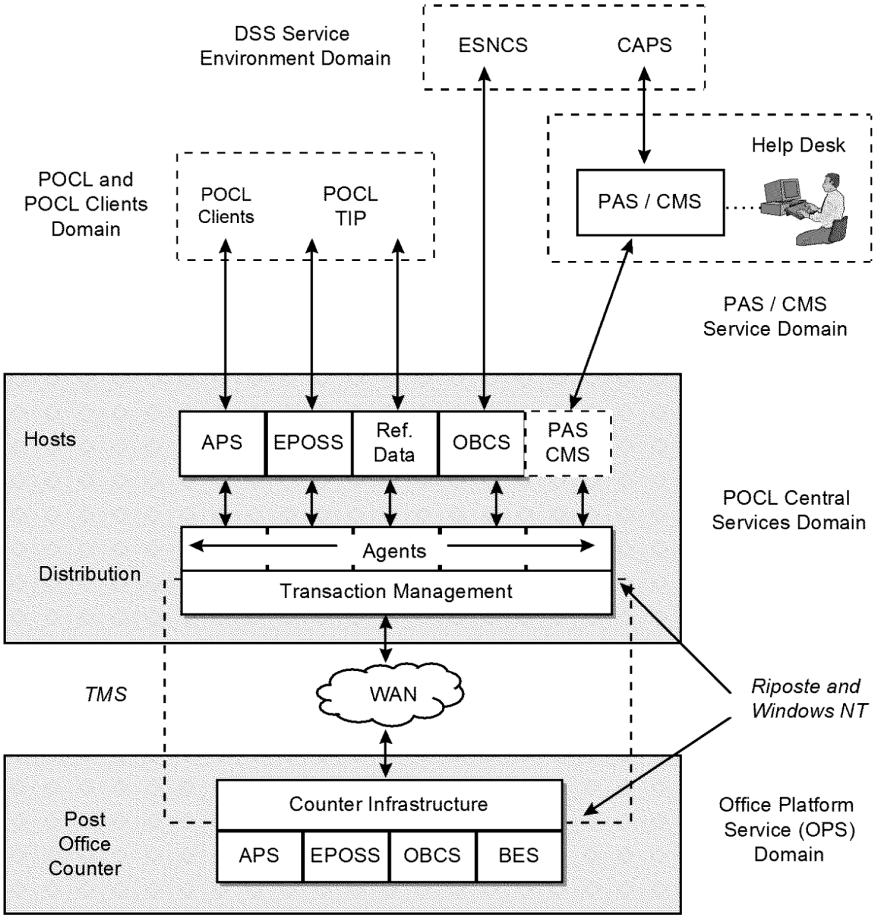

Figure 3 - 4 POCL Central Services and OPS Domains

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

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

PAS Agents and CMS Agents access the database on the Sequent platforms. This interface will contain Remote Procedure Call (RPC) mechanisms used to interface Dynix with Windows NT.

FUJ00087988

This domain includes the Key Management System used to generate and distribute keys within the Central Services Domain and to Post Offices. All PAS transactions will be “signed” by the PAS/CMS Agents, using the message protection facilities specified in section 9.

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

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

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

The Order Book Control Service (OBCS) is, commercially, a POCL service, but data is exchanged over the CAPS/ESNCS link to a DSS ACC. This can be viewed as the DSS hosting a POCL service.

3.5 The Office Platform Service Domain

The OPS Domain encompasses all Post Office sites as illustrated in figure 3-4. The applications, that will run on Windows NT workstations, support the:

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

BES will incorporate the security mechanisms used to verify the integrity of messages which are “signed” by PAS, described in section 9.

Reference data, sourced mainly from DSS and POCL, will be distributed to the target applications in the OPS domain. CRC based integrity checks and validation procedures will be incorporated.

Cryptographic mechanisms will be used to protect hard disks within the OPS Domain. Filestore encryption and the associated key management facilities are described in section 10.

FUJ00087988

3.6 De La Rue Card Services Domain

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

The links between the PAS/CMS Service Domain and the DLR Card Services Domain will be protected as specified in section 8.

3.7 POCL and POCL Clients Domain

The POCL and POCL Clients Domain contains the ICL Pathway system components which will provide the interface with POCL and POCL Clients (except DSS).

ICL Pathway will provide the POCL Transaction Information Processing (TIP) system with records of all transactions at Post Offices. The associated POCL system, which will shares the TIP link, provides reference data for the applications.

In the short term, the POCL Automated Payments (AP) system, which processes payments on behalf of POCL Clients, will use the existing POCL service (known as HAPS) that runs at the POCL site at Farnborough. This system will be responsible for forwarding data to POCL's AP clients, until it is replaced by direct links from ICL Pathway to each of the POCL Client systems.

Initially, the domain will contain the ICL Pathway PC(s) and associated communications components, installed on the Farnborough site, used to receive files sent from the ICL Pathway campus.

3.8 System Management Service Domain

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

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

The Strategic Infrastructure Service (SIS) and System Management Centre (SMC) Help Desks are within the SMS Domain.

FUJ00087988

3.9 ICL Pathway Corporate Services Domain

The ICL Pathway Corporate Services domain will support ICL Pathway's own management processes. The domain encompasses the Data Warehouse and ICL Pathway's managed services as illustrated in figure 3-5.

Inputs to the Data Warehouse, from the operational system, are provided by TMS, PAS/CMS, SMC and SIS.

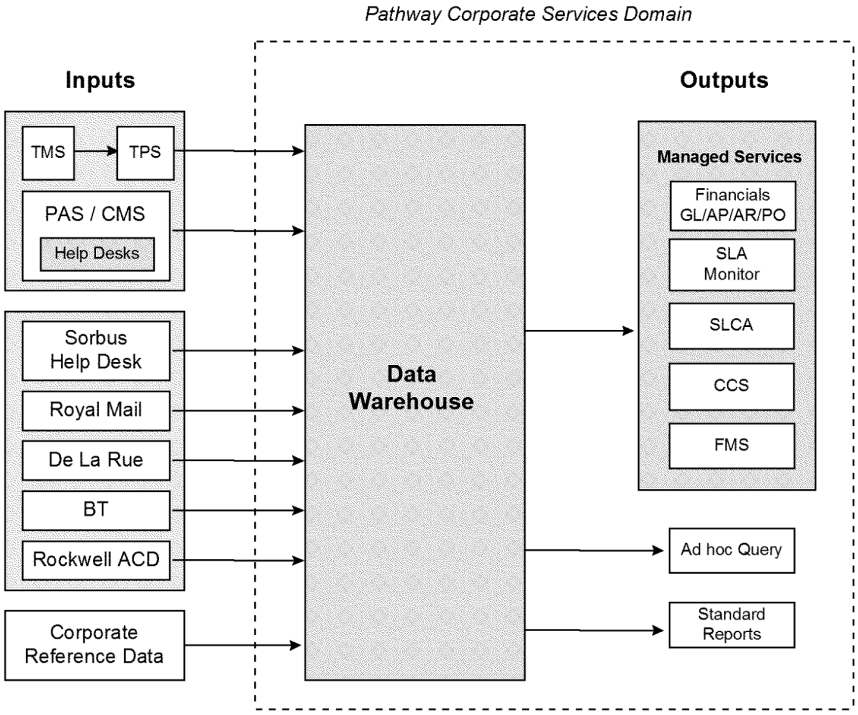

Figure 3 - 5 ICL Pathway Corporate Services Domain

The aggregated information stored within the Data Warehouse is used by ICL Pathway's Managed Services, including reporting on the operational system, accounting, monitoring service levels and fraud risk management.

4. SECURITY COMPONENTS

4.1 Security Enforcing Components

The security enforcing components within the ICL Pathway system are:

- Windows NT Workstation and NT Server,

FUJ00087988

- Dynix operating system (on Sequent platforms),
- Oracle 7 database products,
- Riposte (see below),
- networking components (including firewalls and routers),
- encryption devices, and
- virus protection products.

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

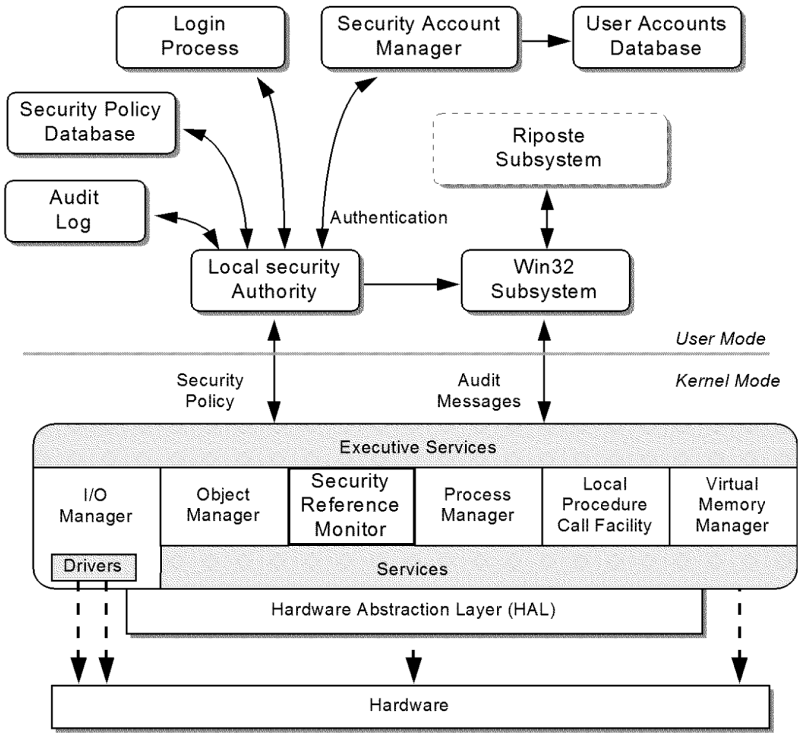

Figure 4 - 1 Windows NT Security Components

4.2 Windows NT Security Functionality

Microsoft's Windows NT Workstation and Windows NT Server have security functionality which can be described as ITSEC F-C2 [ITSEC]. Currently, only NT version 3.51, in a specific configuration, has been formally evaluated and certified.

4.2.1.1 ICL Pathway will use proven current version(s) of Microsoft's Windows NT products (rather than earlier evaluated versions).

FUJ00087988

4.3 Dynix Operating System Security Functionality

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

4.3.1.1 ICL Pathway will use the current version(s) of DYNIX/PTX.

4.4 Database Management Systems

Oracle is a Relational Database Management System.

4.4.1.1 ICL Pathway will use current version(s) of Oracle products.

4.5 Network Security

The ICL Pathway solution incorporates five main components for enforcing network security:

- Firewalls,
- Routers (Cisco products),
- ISDN adapter (developed by EICON),
- Encryption devices (incorporating Rambutan), and
- Cryptographic services incorporating the Red Pike algorithm.

4.5.1 Firewalls

Firewalls will be used to protect the ICL Pathway system from:

- unauthorised access via external networks, and
- other local networks collocated within the ICL Feltham site.

Protection will be provided by a combination of packet filtering functionality within router components and application level firewalls.**Routers**The routers used will be standard Cisco products (from Cisco's 7500, 4500 and 2500 series) and Access Servers.Control of access to these components is specified in section 6.5.

4.5.2 Security of ISDN (or equivalent) Adapters

This section considers Integrated Services Digital Network (ISDN) links.

Specific security controls include:

- CHAP Authentication - where a Challenge Handshake Authentication Protocol (CHAP) challenge is issued on inbound and outgoing calls when the connection is established.

FUJ00087988

- Call screening - where a list of valid callers is configured in the central Router and all other calls are rejected.

The list of valid caller information will be subject to access controls and maintained using Tivoli.

An ISDN adapter will be installed in the gateway workstation at every Post Office location which uses ISDN.

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

- it will only accept incoming calls from phone numbers for which entries exist in an incoming allowed list,
- it will only call phone numbers which exist in the NDIS configuration data,
- it only passes network traffic at the IP level,
- it acts as a CHAP authenticator on every call,
- it reissues the CHAP challenge every n seconds where n is a configurable parameter stored in the NDIS configuration data,
- it stores the CHAP secret in the NDIS configuration data using a symmetric encryption algorithm , and
- it protects the NDIS configuration information.

All NDIS configuration data will be stored in the Windows NT Registry. The files used will be protected by the Windows NT access controls and the filestore encryption (described in section 9).

Use of CHAP keys is specified in section 8.6.

4.5.3 Encryption Devices

The encryption devices in ICL Pathway's solution are types ED600RTS and ED2048R3 supplied by Zergo.

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

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

The use of encryption is specified, on a link by link basis, in section 8.

FUJ00087988

4.5.4 Red Pike

ICL Pathway will use a CESG approved implementation of Red Pike to provide the protection of selected links, as described in section 8.

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

The Team Crypto product, used to protect Post Office filestore, also incorporates Red Pike, as described in section 10.

4.6 Riposte

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

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

4.6.1 Riposte User Authentication

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

Riposte will be used to provide the Post Office user logon interface as specified in section 5.2.3 and [RIPSDS].

4.6.2 Riposte Messages

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

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

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

- Riposte,
- audit information,
- security properties,

FUJ00087988

- system management information,
- system administration information, and
- application information.

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

Riposte Servers use Windows NT services for:

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

4.6.3 Riposte Message Servers

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

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

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

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

If a message store is lost, all messages will be recovered from other members of the group. For a single terminal configuration, the associated correspondence servers at the central site provide this backup.

FUJ00087988

4.6.4 Riposte Correspondence Servers

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

Correspondence Servers are used to provide:

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

4.6.5 Riposte Agents

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

Examples of how the ICL Pathway system uses Riposte Agents include:

- provision of the interface with the PAS/CMS database applications,
- transaction harvesting, and
- Riposte related system management activities.

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

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

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

When Agents are restarted, they will co-ordinate recovery with external systems and restore their state information. Restart is automated by the System Management facilities (described in section 11.2). Recovery will include processing messages which may have arrived when the Agent was down.

The use of Riposte Agents with POCL Clients, AP host(s) and TIP host(s) is illustrated in figure 3-4.

4.6.6 Riposte Communications

FUJ00087988

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

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

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

4.6.7 Riposte Desktop

Each Riposte user application:

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

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

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

4.7 Virus Protection

This section considers the threat of virus infection and identifies the components needed to provide an appropriate level of protection.

4.7.1 Threat of Virus Infection

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

- Windows NT is used throughout the Office Platform Service Domain,
- all PAS/CMS Help Desks use Windows NT platforms running dedicated client software,
- floppy disk drives cannot be used within Post Offices,
- there are no E-mail connections to external systems,
- MS Word documents (which could contain Word macro virus) are not normally imported,

FUJ00087988

- operational files transmitted by file transfer contain data rather than executable code, and
- the main processing platforms are Unix based.

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

- any Windows 95 workstation connected to the system,
- executable files introduced for maintenance purposes, and
- HTML documents containing user Help information.

The use of Windows 95 is not expected to be widespread but in some cases workstations used for system management functions will be Windows 95 based rather than Windows NT.

4.7.2 Virus Protect Measures

4.7.1.1 All workstations running Windows 95 will have virus protection software (e.g. Dr Solomon's WinGuard) installed.

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

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

4.7.1.3 All executable code will be virus checked prior to being imported into any part of the ICL Pathway system.

4.7.1.4 All MS Word files (including HTML files) will be checked for macro viruses prior to being imported into any part of the ICL Pathway system.

4.7.1.5 Anti-virus software will be maintained by installing current upgrades as they become available.

4.7.1.6 As an additional safeguard, ICL Pathway will ensure that the ICL Pathway system has adequate facilities for recovery in the event of a virus being detected.

5. IDENTIFICATION AND AUTHENTICATION

5.1 Identification and Authentication Requirements

FUJ00087988

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

Reliable identification and authentication is essential in order to:

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

Authentication is based upon the information received, so the ICL Pathway system will protect both:

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

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

5.1.1 User Identification

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

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

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

5.1.1.2 Wherever possible, a User id should be sufficient to trace the identity of the particular individual who has been authenticated.

In some cases, however, the same User id will be used for infrequent access by users in particular roles. This will apply, for example, to POCL Auditors who will be required to authenticate with the Help Desk before getting a one-shot password.

5.1.1.3 The ICL Pathway system will not allow (normal) users to change their User Id.

FUJ00087988

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

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

In all cases, the standards used by ICL Pathway [SECSTD] will provide guidelines to cover operational aspects, including:

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

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

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

5.1.2 User Authentication

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

5.1.2.1 All users will be authenticated before any access is granted to the ICL Pathway system.

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

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

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

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

In all cases the logon failure will be recorded.

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

FUJ00087988

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

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

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

5.1.2.5 On successful logon, the system will display the date and time of the user's last successful logon.

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

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

5.1.3 Passwords

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

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

5.1.3.2 An initial password will be made known to each individual. The system will mark these initial passwords as expired.

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

5.1.3.3 The format of passwords will depend upon the platform(s) used and the server used for authentication.

In all cases, the standards used by ICL Pathway [SECSTD] will provide guidelines on the use of passwords, including:

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

FUJ00087988

5.1.3.4 The system will use volatile memory for operations associated with password checking. When the checking is complete all “in clear” password information will be overwritten.

5.1.3.5 Passwords will never be visibly displayed by the system.

5.1.3.6 Passwords will not be transmitted “in the clear” to or from any location outside the central ICL Pathway sites.

5.1.3.7 Passwords will not be transmitted “in the clear” within ICL Pathway sites unless the link used is entirely within a physically protected area.

5.1.3.8 An appropriate one-way algorithm will be used to encrypt password information before storage or transmission.

By definition, it will not be possible to derive passwords from their one-way encrypted form (except by the use of massive computing power over an extensive period).

5.1.3.9 All Routers will be configured in the mode that ensures that password information is stored in encrypted format.

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

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

5.1.3.11 The OPS will provide facilities to enable the Post Office Manager to establish new users and set an initial password for all users in their Post Office.

5.1.3.12 If a user forgets their password the Post Office Manager will be able to reset the password.

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

5.1.4 Use of Tokens

FUJ00087988

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

5.1.4.1 Tokens will be allocated to named individuals for their sole use.

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

5.1.4.3 The system will be capable of selectively revoking the validity of tokens.

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

Tokens which generate a one-time password, thereby protecting against password replay, will be used.

5.1.4.5 Each token will have an associated PIN which is used to activate the device, as defined in [ACCPOL].

5.1.4.6 Personnel who are authorised to access the ICL Pathway system from remote locations will be required to identify themselves using hand held tokens.

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

ICL Pathway Headquarters site at Feltham (see section 8.10) is categorised as being a “remote location”. ICL Pathway personnel who require access to the operational system and/or Data Warehouse will be required to use tokens.

5.1.4.7 Personnel who are authorised to access the ICL Pathway system using UNIX root privilege will be required to identify themselves using hand held tokens.

5.1.4.8 Personnel who are authorised to access the ICL Pathway system as a database administrator (DBA) will be required to identify themselves using hand held tokens.

5.2 Authentication of Windows NT Users

5.2.1 Authentication Methods

FUJ00087988

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

- PAS/CMS Help Desk clients within the PAS/CMS Service Domain,
- platforms within the POCL Central Services Domain,
- workstations within the Office Platform Service Domain,
- servers within the De La Rue Card Services Domain, and
- servers within the POCL and POCL Clients Domain.

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

In both cases:

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

5.2.1.2 All users will be named individuals with their own password.

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

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

5.2.1.3 The standard Windows NT password algorithms will be used.

5.2.2 Standard Windows NT Logon

The Windows NT logon process is illustrated in figure 5-1. For users in domains (defined in 5.2.1) which use this form of logon:

5.2.2.1 The trusted logon process (as illustrated in figure 5-1) will be used to authenticate users, based upon their User Id and password.

FUJ00087988

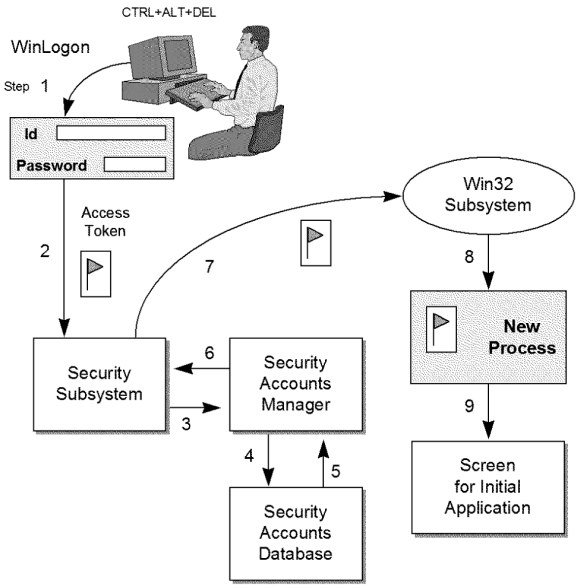

Figure 5 - 1 Windows NT Logon Process

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

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

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

The exact interval will be configurable and will depend upon the user's role and location.

5.2.2.4 The Windows NT Account Policy controls will be used to set the parameters which apply to all users. [ACCPOL] will define values for all parameters, including:

- password expiry period,
- minimum password length,
- minimum password age (before change),
- remember password history (number of passwords per user),
- number of consecutive failed logon attempts before lockout, and
- whether to reset logon count after a delay period (see 5.1.2.3).

FUJ00087988

5.2.3 Logon at Post Office Locations

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

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

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

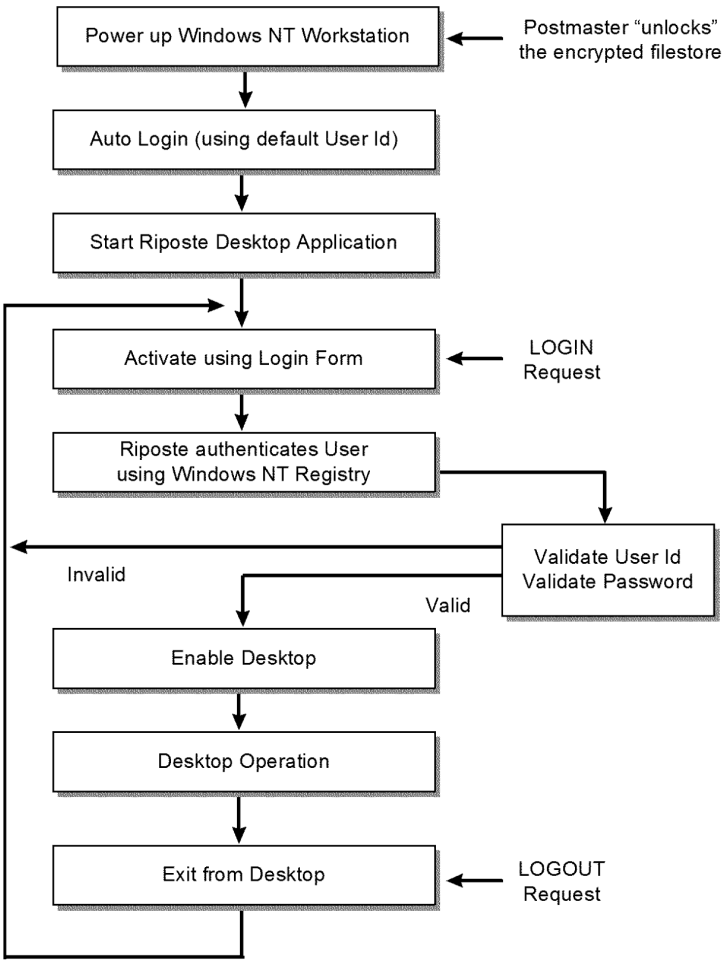

Figure 5 - 2 Logon Sequence at Post Offices

FUJ00087988

The logon sequence used is illustrated in figure 5-2. For simplicity, filestore encryption logic (described in section 10) associated with initial power up is not shown.

When the Windows NT workstation is powered up, the Windows NT facility for automatic logon is initiated instead of the normal manual NT user logon sequence. This will enable a dummy user with username (u1) and password (p1).

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

In particular, use of the Shift key to escape whilst booting Windows NT will not be enabled.

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

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

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

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

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

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

FUJ00087988

When the user logs off from the desktop, the desktop logon form is displayed whilst the desktop remains active in the security context of username u1. This allows the PO user to subsequently logon without incurring the (typically 30 second) delay arising from loading the desktop.

5.3 Authentication of Oracle Users

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

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

5.3.1.1 Oracle will be used to authenticate all database users (e.g. PAS/CMS Help Desk) in the operational ICL Pathway system.

5.3.1.2 The Sequent Dynix operating system, which will provide the platform for Oracle, will be used for authentication of all Operational Support users (e.g. Security Manager) in the operational ICL Pathway system.

5.3.1.3 The Card Management Service (CMS) and Payment Authorisation Service (PAS) will use a Client - Server architecture with the Oracle DBMS server component running on the Sequent platform.

5.3.1.4 All tables associated with the CMS and PAS will be owned by a single “Pathway” user on the corresponding Sequent platform.

5.3.1.5 Database access from the POCL Central Services Domain is provided by Riposte Agents running on Windows NT. Each agent will be associated with a Port (or multiple Ports) on the Sequent machine.

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

5.4 Authentication of Help Desk Operators

5.4.1.1 Help Desks for CMS and PAS will be client applications running on Windows NT. Groups of clients (typically 50 to 100) will be connected to Windows NT based servers which provide the connection to the Sequent machines.

5.4.1.2 All Help Desk users will be named individuals in a user group associated with a Database Role.

FUJ00087988

The roles used (e.g. Manager, Supervisor and Advisor) will be defined in [ACCPOL].

5.4.1.3 Each Help Desk user will be allocated a User Id and initial password. This will enable them to connect to the database provided they have a valid username defined in the database.

These users are permitted to access the database by running an application (such as Oracle Forms).

5.4.1.4 Help Desk personnel will be able to authenticate to Post Office counter staff, thereby confirming that requests are being handled at an authorised Help Desk.

Help Desk information, on which actions are taken by a Post Office, will be accompanied by an additional value related to the proposed authorisation code. This authentication information, provided verbally by the Help Desk advisor, will be validated automatically at the Post Office workstation.

The authentication information needs to be updated frequently (typically daily) and specific to the calling Post Office.

Contingency arrangements will be provided, as defined in [SECPOL], to cover the cases where some components of the system are not operational.

5.5 Authentication of DSS/BA Staff

DSS/BA telephone callers will be carefully authenticated prior to accepting any instruction or advice.

The mechanisms needed to authenticate DSS/BA staff are currently under review and will be the subject of discussions with the authorities concerned. These mechanisms will be described in a later version of this document.

5.6 Authentication of POCL Staff

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

The mechanisms needed to authenticate POCL staff are currently under review and will be the subject of discussions with the authorities concerned. These mechanisms will be described in a later version of this document.

FUJ00087988

6. LOGICAL ACCESS CONTROL

6.1 Access Control Requirements

There are three aspects to access control:

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

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

6.1.1 Access Control Policy

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

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

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

6.1.2 Privileges and Roles

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

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

6.1.2.1 ICL Pathway will apply the principle of least privilege when assigning privileges to roles and users.

FUJ00087988

6.1.3 Separation of Duty Controls

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

There will also be administrative and procedural controls defined within ICL Pathway's operational procedures.

6.1.4 Two Person Controls

Two person controls have been considered for system and database management operations but are not proposed.

6.1.5 Use of Discretionary Access Controls

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

6.1.6 Control of Access to Files and Directories

Access to each file or directory will be controlled by the owner of the object who will be able to grant access rights to other users or groups of users. The types of access supported will be:

- Read,
- Write,
- Append (for audit files),
- Execute,
- Delete,
- Change Permissions, and
- Take Ownership.

6.2 Control of Access to Databases

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

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

6.2.1 Schemas and Users

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

FUJ00087988

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

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

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

- whether user authentication information is maintained by the database or the operating system (see section 5.3),
- resource limits, defined in a profile (see section 6.2.3), and
- the privileges and roles (see section6.2.4) that provide the user with appropriate access to objects needed to perform database operations.

6.2.2 Changing User's Parameters

A user's security domain can be altered using:

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

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

6.2.3 Profiles

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

6.2.4 Oracle Privileges and Roles

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

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

FUJ00087988

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

Within the ICL Pathway system all privileges will be associated with roles rather than being explicitly assigned to individual users. This will provide more effective management control of both system privileges and object privileges.

6.3 Access Controls Supported by Windows NT

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

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

6.3.1 Configuration of Windows NT

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

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

6.3.1.1 Windows NT based platforms will be configured strictly in accordance with [ACCPOL] prior to roll-out.

6.3.2 Windows NT Access Control Lists

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

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

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

6.3.3 Windows NT Tools Used to Control Access

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

FUJ00087988

6.3.3.1 The ability to access Windows NT tools will be removed on the basis of roles, in accordance with [ACCPOL], prior to roll-out.

6.3.4 Windows NT File and Directory Access

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

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

6.3.5 Windows NT Privileges and Roles

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

6.4 Access Controls Supported by Dynix

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

6.4.1 Configuration of Dynix

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

6.4.2 Dynix Access Controls

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

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

6.4.3 Dynix Tools Used to Control Access

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

6.4.4 Dynix File and Directory Access

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

6.4.5 Dynix Privileges and Roles

The use of Dynix privileges and roles will be defined in [ACCPOL].

FUJ00087988

6.5 Control of Access to Routers

6.5.1 Access Methods

Cisco provides four methods of access for controlling routers:

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

6.5.1.1 Console access mode will be disabled by router configuration.

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

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

6.5.1.3 SNMP access will be used for remote system management of routers (as defined in section 11).Use of TFTP will be controlled in accordance with [ACCPOL].

6.5.2 Privileged Mode Access

Provided Console or SNMP mode of access is used (as defined in section 6.5.1) the use of privileged mode access can be controlled, as follows:

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

FUJ00087988

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

6.5.2.1 Session Timeout values will be selected to limit the period of time allowed for operation of a console in privileged mode.

6.5.3 Access Lists

The parameters to an Access List allow IP addresses to be specified along with protocols (ip, udp, tcp and icmp) and port numbers.

6.5.3.1 Access lists will be used to define the actual traffic that will be permitted or denied through a Router.

6.5.3.2 Only traffic associated with IP addresses that are explicitly defined in Access Lists will be permitted.

6.5.3.3 Constraints associated with particular port numbers will be defined in [ACCPOL].

6.5.3.4 Constraints associated with particular protocols will be defined in [ACCPOL].

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

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

FUJ00087988

7. AUDIT AND ALARMS

7.1 Audit and Alarm Requirements

The audit and alarm facilities provided by the ICL Pathway system must satisfy the business level audit and security audit requirements of "external" auditors (including DSS, POCL, NAO and the Authorities' Auditors) and ICL Pathway's "internal" monitoring (including Security Audit and Fraud Risk Management).

The Audit Trail Functional Specification [AUDFS], which is primarily concerned with addressing business level audit requirements, specifies audit trails as three "tracks" (namely DSS, POCL and System Management) which can be selectively viewed by the appropriate auditors.

7.2 Sources of Audit Events

Auditable events will be recorded in application level transaction logs and lower level audit logs. Figure 7-1 illustrates the main sources of system generated events.

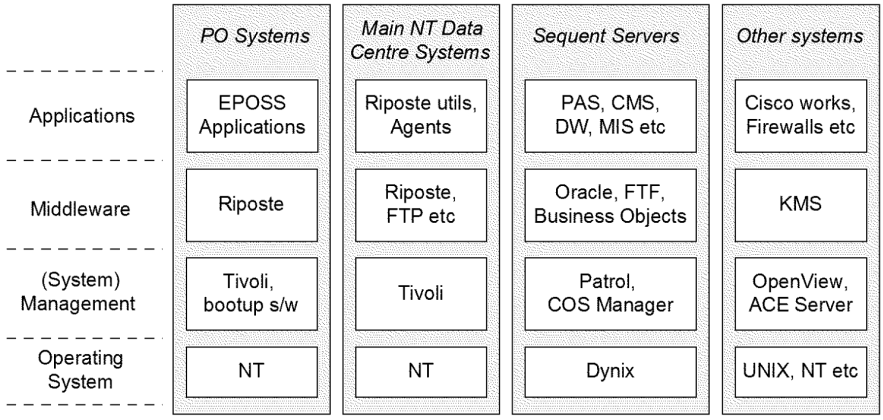

Figure 7 - 1 Sources of Auditable Events

Riposte provides an ideal basis for logging all transactions to give a complete picture of actions within the Benefit Encashment Service and Post Offices Infrastructure Service. It will be used within the POCL Central Services and OPS Domains to provide a complete record of all transactions.

FUJ00087988

Applications running on the Sequent servers generate logs of the business transactions and file transfers. The Oracle databases, used for CMS/ PAS, associated Help Desk applications, the Data Warehouse and MIS, have the ability to audit security relevant events which are recorded in tables.

Patrol will be used to monitor all Sequent systems and the Oracle applications which run on Sequent platforms. The audit events an alarms gathered by Patrol will be captured, for recording and analysis, via a Patrol Tivoli event adapter (as outlined in section 11).

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

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

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

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

7.3 Auditable Events

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

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

FUJ00087988

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

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

7.4 Application Level Audit

7.4.1.1 The principal audit log associated with the DSS track will be the TMS journal. This will be used to record data traversing between:

- PAS - TMS,
- CMS - TMS,
- BES - TMS, and
- Order Book Control Service (OBCS) - TMS.

7.4.1.2 The audit log will include the following:

- file receipt from/despatch to CAPS, including file sequence numbers and record control totals,
- file receipt from/despatch to PAS/CMS, including file sequence numbers and record control totals,
- control checkpoints and any restarts during file transfer operations between CAPS and PAS/CMS,
- userid, date and time,
- all systems access, and
- all exception conditions (e.g. file sequence or control total failures).

7.4.2 Audit at the CAPS Interface

7.4.2.1 The audit log of transfers between CAPS and the File Reception system will be held at the CAPS site of operation with a copy transferred to ICL Pathway (at the site of PAS/CMS operation). All other audit log data for BPS will be held at the PAS/CMS site.

7.4.2.2 For file based data transfers, the audit log will record:

- all transfers of files at entry and exit to BPS,
- all transfers between subsystems of the BPS, and
- the processing of files.

7.4.2.3 Transactions recorded in the BPS audit log will identify the auditable event itself, date and time, and the cause, effect and owning organisation or individual as appropriate.

FUJ00087988

7.4.2.4 The audit log will allow activities that utilise more than one of the services to be traced from start to finish, or from an intermediate point in any direction.

7.4.2.5 The audit log will provide information to allow the original transaction to be recreated.

7.4.2.6 ICL Pathway will provide BA/POCL with reasonable access to the BPS audit log. Facilities will be provided for secure interrogation of the audit log under appropriate access control privilege.

7.4.3 Audit Logs within the Database

Audit information, directly related to actions upon the database, will be held in a table within the Oracle database.

7.4.3.1 As payment authorisation data is transferred from PAS to TMS, the transaction log database within PAS will be updated and new authorisation records will be created within TMS.

7.4.3.2 When encashment or expiry transactions are transferred from TMS to PAS, the PAS transaction log database will be updated.

7.4.3.3 The scope of PAS and CMS extends to their respective help desks and transactions handled in these sub-services will also be recorded in the transaction log.

7.4.3.4 Within PAS each individual payment authorisation will be logged in the database to support transaction level audit and reconciliation.

7.4.4 Riposte Transaction Log

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

7.4.4.1 For transactional based data transfers, logging will be provided at the message level.

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

7.4.4.3 The format of this journal entry will vary according to the transaction type, [RIPSDS] but will typically contain:

- Post Office ID,

FUJ00087988

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

7.4.4.4 Each counter PC will contain a journal and all journal entries will be automatically replicated to all other members of the workgroup. This will include remote Correspondence Servers that form part of the TMS.

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

7.4.4.6 A complete audit log of all transactions and other significant events will be maintained within the Post Office systems. It will be available automatically for analysis by value added services which are linked to TMS.

7.4.4.7 All events that occur either in TMS or in OPS will be written to a journal. The journal message content is identified in section 7.4.4.3.

7.4.5 Logging in Fall-back Mode

7.4.1.1 The audit log will be maintained during periods of fallback and recovery.

7.4.1.2 The integrity of the audit log will be maintained during periods of partial or complete service loss or failure. Starting and restarting transactions will make appropriate audit log entries.

7.4.1.3 The distributed nature of the ICL Pathway TMS will enable an Audit log to be maintained and accessed during any recovery of a TMS server.

7.5 Application Level Audit Analysis

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

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

FUJ00087988

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

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

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

7.5.1.2 PAS will produce a full set of operational and audit reports as specified by the BPS MIS requirements [SADD].

7.5.1.3 PAS will provide secure access facilities to interrogate the status of all payments from payment receipt to return of encashment or expiry data to CAPS.

These enquiries will use the standard operational Help Desk facilities.

7.5.1.4 The PAS transaction log database and related MIS will be available for access, subject to appropriate security clearance, by standard tools for query, reporting and data analysis.

7.6 Protection of Audit Logs

7.6.1.1 The audit log will have a level of security such that it cannot be altered or deleted.

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

7.6.1.2 ICL Pathway will keep copies of vital files, including the audit log, at the alternate central site. The frequency of transferring backup copies will be defined in [ACCPOL].

7.7 Audit of Systems Management Functions

The Systems Management function will provide the audit log with a record of operational events, inventory, distribution and remote operations.

7.7.1.1 The Systems Management Service will provide a repository for recording all physical events affecting the platforms which support the SIS, namely TMS and the OPS.

FUJ00087988

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

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

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

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

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

7.7.1.5 Audit events will be viewed through the appropriate audit analysis applications.

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

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

7.8 Windows NT Audit

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

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

7.8.1 Selection of Auditable Events

For each audit category the selection criteria can include:

- audit successful events,
- audit failed events, and

FUJ00087988

- audit both successful and failed conditions.

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

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

7.8.2 Audit of File and Directory Actions

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

Selection of auditable events is addressed in [ACCPOL].

7.8.3 Audit of Registry Actions

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

Selection of auditable events is addressed in [ACCPOL].

7.8.4 Audit of Printer Actions

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

Selection of auditable events is addressed in [ACCPOL].

7.9 Alarm Conditions

Auditable events which require immediate investigation will be used to trigger alarms in real time.

Events will be selected in accordance with ICL Pathway's Security Policy [SECPOL].

8. SECURITY OF LINKS

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

- data on individual communications links, and

FUJ00087988

- individual messages from creation to use (end-to-end).

Key management and the special requirements of roll-out are also covered. A more detailed description is provided in [CDS].

Figure 8-1 illustrates the overall communications configuration to be protected:

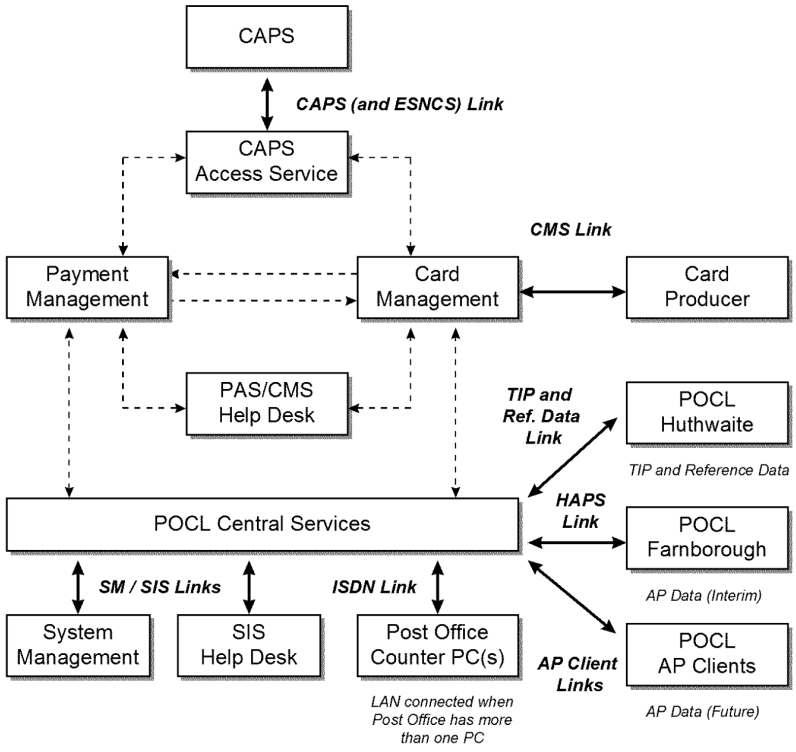

Figure 8 - 1 Links to be Considered for Protection

The link protection mechanisms, described in the following subsections, incorporate the changes needed as a result of moving to the Energis ATM network.

For each client, ICL Pathway will implement link protection as each client interface is agreed.

Appendix C contains a summary of the cryptographic key types used in the solution.

8.1 CAPS (and ESNCS) Links

FUJ00087988

These are the links used to transfer files, containing mainly payment authorisations, stop notices and customer personal details (including instructions to bring customers onto the service), from BA's CAPS system to ICL Pathway's CAPS Access Service (CAS). Information sent back from ICL Pathway to CAPS will include benefit encashments and expired payments.

8.1.1.1 The Electronic Stop Notice Control System (ESNCS) used by the Order Book Control Service (OBCS) will use one of the CAPS links.

8.1.2 Protection

The protection on the CAPS link is aimed at reducing the financial risk to ICL Pathway and the Contracting Authorities.

8.1.2.1 The purpose of this protection is integrity and origin authentication. Strong cryptographic integrity protection is needed for this link.

This will be provided using one of two means:

- use of Rambutan encryption hardware at each end of the link, or
- use of a Red Pike encrypted secure hash, produced using SHA, implemented in software at each end of the link.

Rambutan hardware capable of supporting ATM and Frame Relay communications is not currently available.

ICL Pathway has also determined that use of an SHA-style hashing on the CAS VMS machine at the ACC would impose an unacceptable processing load. This could be overcome by the use of additional Windows NT hardware at each ACC.

ICL Pathway will, therefore, use the Release Contents Description (RCD) mechanism to seek concessions to defer strong protection of this link until a subsequent release, by providing an interim solution using the CAPS computed CRC, as follows:

- Files sent from the BA location to ICL Pathway locations are protected against changes which affect financial totals. ICL Pathway will verify that each file origin is an agreed BA location.
- The file passed to the CAS component on the BA system has a 32 bit CRC included and a set of totals for financial fields. This CRC and total fields are encrypted using Red Pike and the encrypted value is sent with the file to the CAS components at each ICL Pathway Campus. This component computes the CRC and totals for the received file, encrypts them and checks that they match the encrypted fields associated with the received file.

FUJ00087988

- No protection is provided on files sent from ICL Pathway to BA locations on the CAPS link.

8.1.3 Key Management

8.1.3.1 Key material, supplied from the Key Management System (KMS), will be loaded manually and locally into the Series 39 (VME) and Sequent platforms at each end of the CAPS links.

New key variables will be installed, by the authorised custodian, who will type them in using an alphanumeric format specified in [CDS]. A checksum will be included in the key material to detect typing errors.

8.1.3.2 Keys will be stored in a file with file access restricted by use of the operating system access controls. Read and modify access will be permitted for the approved custodian with no access permitted for all other users.

The cryptographic functions on each machine will run in privileged mode.

8.1.3.3 Key changes will be performed at intervals agreed with the Contracting Authorities, based on advice from CESG, for integrity protection.

8.2 CMS Links

These are the links used to transfer card production data and PUN information to the card producer.

8.2.1 Protection

There is no explicit Contracting Authority requirement for protection of CMS links. The protection defined here is solely aimed at reducing ICL Pathway's financial risk.

All data on CMS links will be encrypted, for confidentiality and integrity, using Red Pike. This enables ISDN lines to be used rather than dedicated links.

8.2.1.1 Protection will be provided at application level using bespoke development incorporating the Red Pike algorithm.

8.2.1.2 At the ICL Pathway end, the CMS file will be transferred to a Windows NT platform where the entire file will be encrypted using Red Pike. The file will be transmitted to the target CMS, where it will be decrypted again at application level.

FUJ00087988

The use of Windows NT platforms at each end of the link allows reuse of crypto functionality.

8.2.1.3 Decrypted files at the target CMS will be validated to ensure that only integrity checked data is used for card and PUN production.

8.2.1.4 Data transferred from CMS to ICL Pathway will also be protected, using Red Pike, and validated before use.

8.2.2 Key Management

The key management arrangements for the CMS link will be similar to those described in section 8.2.3, the main differences being:

- Windows NT platforms are used at both ends of the CMS link, and
- the key change interval may differ.

8.2.2.1 The Red Pike keys will be installed (by typing them in) into the ICL Pathway server and DLR server.

The key values will be generated in the same form as the CAPS link keys together with a checksum to detect typing errors.

8.2.2.2 The application will accept the keys in alphanumeric format and store them persistently on a disc file which is protected under the Windows NT file system so that only one user can access that file.

8.2.2.3 The Windows NT platforms used will be located in physically protected environments.

8.3 POCL TIP (and Reference Data) Link

These are the links used to transfer information to/from POCL. They carry the entirety of POCL's outlet transaction business and stock data, plus reference data back to ICL Pathway. There is an explicit Contracting Authority requirement for integrity protection of this link, in addition to the end-to-end protection of AP records, as defined in section 9.4.

8.3.1 Protection

8.3.1.1 The integrity of data transferred on this link will be protected by DSA signatures in both directions. This protection will also be provided for traffic to and from the disaster recovery site.

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

FUJ00087988

8.3.1.3 The same end-to-end integrity protection will be used, where appropriate, to protect other low volume data such as Post Office reconciliation totals.

8.3.2 Key Management

8.3.2.1 Key management will be done by introducing the signing key and public key certificate from floppy at intervals agreed with the Contracting Authorities, based on advice from CESG. Each end will have a different signing key.

POCL HAPS Link The link between ICL Pathway and the Host Automated Payments System (HAPS) is an interim solution, whereby all AP data will be sent to an existing POCL Tandem system sited at Farnborough. This HAPS system is then responsible for onward routing the data to their AP clients.

This file transfer product will run on a dedicated ICL Pathway Windows NT platform at each campus and POCL's Tandem AP Host. Windows NT platforms will be used, rather than Sequent, to avoid adding complexity to the Sequent systems.

8.3.3 Protection

8.3.3.1 Confidentiality and integrity protection is provided for this POCL Farnborough link using Rambutan based encryption hardware.

8.3.4 Key Management

8.3.4.1 The standard key management facilities, provided by the bought-in devices, will be used.

8.4 POCL AP Client Links

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

The above includes both files sourced by ICL Pathway and files sent out that were generated from data received from the POCL HAPS link during the period of cut over from HAPS to direct client communication.

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

8.5 Post Office ISDN Links

FUJ00087988

These are the ISDN links from the POCL Central Services Domain to the Post Offices.

8.5.1 Protection

8.5.1.1 CHAP initial connection authentication will be provided, with refresh, supplemented by CLI authentication of the Post Offices from the ICL Pathway campus. CHAP re-authentication will be applied to all calls (however initiated).

8.5.1.2 There will be no link related protection of operational data.

8.5.2 Roll-out

8.5.2.1 Every gateway PC will be rolled out containing (on filestore):

1. A Post Office Key value (POK) with a unique identifier (POK-Id).
1. Ten Certification Authority (CA) public keys (CAPU) with identifiers. These correspond to the CA's current private key (CAPR) and nine spares.
1. Ten software issue validation public keys (SIPU) in certificates signed by CAPU, the last nine of which are spares.
1. Ten payment authorisation validation public keys (PAPU) in certificates signed by CAPU, the last nine of which are spares.
1. Ten Diffie-Hellman prime and base values (PB-Values) supplied by CESG, the last nine of which are spares.

The spares are reserved for future use.

8.5.2.2 The need to change Post Office key values will be minimised by installing a stock that will be used in turn at intervals as agreed with the Contracting Authorities, based on advice from CESG.

With the exception of the CA keys, changes can be made if necessary through a routine key refreshment procedure (described in [CDS]). The same procedure will be used to verify that the CA public keys held at the Post Offices have not been tampered with.

8.5.2.3 At roll-out, following auto-configuration, the KMS will form an interactive TCP/IP connection with the KMS in order to establishe a communications key (CK) with the Post Office Gateway PC.

8.5.2.4 The Diffie-Hellman exchange used has been extended to protect against man-in-the-middle attacks. The KMS will sign its message and the Post Office will encrypt the reply using POK.

8.5.2.5 The public key certificate for the Key Issue Private/Public Key pair (KICert for KIPR and KIPU) will be sent with the key data.

FUJ00087988

8.5.2.6 The communications key (CK) will be used to encrypt confidential key material sent to the Post Office. The key material will arrive in one of two ways depending on the type of key.

In a key package sent over the TCP/IP connection:

- a key encryption seed for use in protecting the contents of the POM's Memory Card (KES),
- the filestore encryption key for the Post Office (FEK),
- the application level communications key (ACK).

In a Riposte message sent to the Post Office:

- secret values for use by specific Post Office counter applications,
- replacement public key certificates for the ones issued at roll-out,
- CA public key values for verifying that the stored values have not been changed,
- the private key for that Post Office (APPR), and
- the corresponding PK certificate containing the public key signed by the CA (AP-Cert containing APPU).

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

The trigger, for the KMS key material package to be sent, is a request message from the Post Office gateway PC as a standard part of the personalisation protocol. In a multi-workstation Post Office, the received package will be passed on, by the Post Office Manager (POM), to all workstations.

The mediums used to transfer keys will be the POM's Memory Card and Riposte message replication, as described below.

8.5.2.8 The key material in the TCP/IP message, and the value of CK, will be written to the Memory Card on the gateway PC.

It is encrypted on the card under:

- a key (KEK) generated from the KES value sent in the key package, and
- a dynamically generated PIN value that the POM must enter at the keyboard in order to use the Memory Card values.

FUJ00087988

8.5.2.9 The PIN, which is a non-memorable value, will be printed on a slip of paper at the time it is generated. The PIN and the card will be stored separately and securely in accordance with Post Office procedures.

8.5.2.10 The POM installs the Riposte message key material in each PC by inserting the Memory Card. The software there uses the CK value on it to decrypt the values in the Riposte message. The filestore encryption key is also extracted from the card for use on the PC.

8.5.2.11 All Keys issued to Post Offices will be generated by the KMS (using cryptographic quality random numbers provided by a hardware supported random number generator).

8.5.3 CHAP Key Management

8.5.3.1 Prior to roll-out, the KMS (or similar secure key generation server) will produce a one-off "List of CHAP Values" with 40,000 entries indexed in an "Index in CHAP List". These lists will be sent (in a secure manner) to the Boot-server machines and to CFM for configuration in the Routers.

The Boot-servers and CFM are the only two places where the List of CHAP Values and the Index in CHAP List for a Gateway PC coexist.

The number of values chosen is twice the number of ISDN PCs, to allow for potential reconfigurations without reusing the CHAP values.

8.5.3.2 The Auto-configuration database system will automatically assign the first free Index in CHAP List for a particular Gateway PC and pass this to:

- the Boot-servers in the 'boot details' for the Gateway PC, and
- CFM as a report.

The Index in CHAP List ranges from 1 to 40,000.

8.5.3.3 CFM will configure the Routers used by the Gateway PC with the CHAP value corresponding to the assigned Index in CHAP List (provided in the Auto-configuration database report to CFM).

8.5.3.4 When the Gateway PC boots for the first time and receives its initial Boot details from the Boot-server, it will also be passed the actual CHAP value associated with its Index in CHAP List.

FUJ00087988

Since the complete CHAP password is transmitted over a public network, it is obscured using a simple ad-hoc encryption algorithm which is also understood by the Gateway PC configuration application. It will, therefore, be able to decrypt it and configure the ISDN driver.

8.5.3.5 As soon as key material has been sent to the Post Office as part of the roll-out process, the value of the CHAP key will be changed to a one-way function of the CK used to protect the key transfer.

From roll-out onwards there are always two CHAP keys to try, an older value (initially the one indexed from the Index in CHAP List) and a newer one (the first derived from CK).

Details of the protocol used to ensure synchronisation of CHAP key utilisation at Post Offices and the central routers are given in [CDS].

8.5.3.6 CHAP keys will be replaced at least as frequently as the most frequent other key issue. In each case they will be derived from the communications key set up for that issue.

8.6 Post Office LANs

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

8.6.1 Protection

There is no link level protection on these LANs.

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

8.6.1.1 Payment Authorisation and AP messages will have the digital signature applied on their respective source machine (hence they will be integrity protected over the LAN).

8.6.2 Key Management

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

FUJ00087988

8.6.1.2 Keys will be replaced at a Post Office, by a routine key refreshment procedure, at intervals agreed with the Contracting Authorities, based on advice from CESG.

This involves the KMS initiating the same protected Diffie-Hellman exchange as was done at roll-out, using the current value of POK. This creates a CK value that is used to protect issued key material, again as at roll-out. Receipt of the new key material causes the POM to be alerted. At a convenient time, the POM will insert his Memory Card into the Gateway PC, pick up the new keys, and move from PC to PC in the Post Office propagating them to the other PCs, and decrypt and install the key material from the Riposte key distribution messages.

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

the Post Office Manager will verbally authenticate to the Help Desk,

the Help Desk will authorise the KMS to send a special recovery key package to the Post Office. The package contents will be similar to the key material issued during a routine key change, but the keys will be the existing ones.

the KMS will send recovery information to the Post Office using the Post Office link as a (virtually) normal routine key refreshment procedure.

the material will then be loaded onto a new Memory Card for which a new PIN is dynamically generated.

8.7 ICL Pathway Inter-campus Links

These are the links between the two ICL Pathway campuses, at Wigan and Bootle, illustrated in figure 8-7.

FUJ00087988

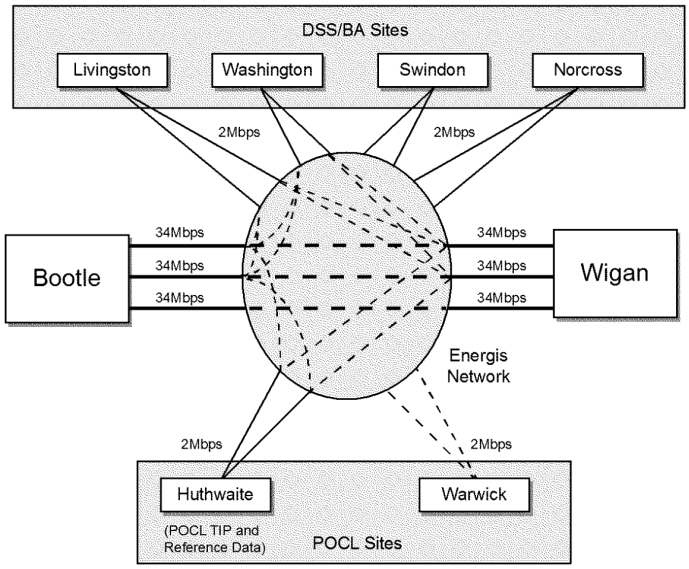

Figure 8 - 7 Inter-Campus (and other Inter-site) Links

8.7.1 Protection

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

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

8.7.2 Key Management

8.7.2.1 The KMS to KMS key will be established automatically using an exchange protected by the DSA private keys owned by the KMSs.

8.8 SIS Help Desk and System Management Links

In addition to the ICL Pathway inter-campus links (described in section 8.8), there are a number of dedicated links into the Wigan and Bootle sites that need to be protected. The network configuration is illustrated in [TED].

8.8.1.1 All links from the ICL DSD sites to the Wigan and Bootle campuses will be encrypted.

8.8.1.2 All links from the ICL CFM site to the Wigan and Bootle campuses will be encrypted.

FUJ00087988

8.8.1.3 ProtectionSystem modifications (e.g. fault reporting) will be done through SIS. SIS authentication will, therefore, be strong and proofed against eavesdropping.All data will be encrypted for confidentiality and integrity using bought-in Government approved point-to-point encryption devices employing the Rambutan algorithm (see section 4.5.3).System management functions, which could cause changes to security sensitive data on campus machines forming a serious security threat, will be protected.

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

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

8.8.2 Key Management

8.8.2.1 The standard key management facilities, provided by the bought-in devices, will be used.

8.9 Links with ICL Pathway Headquarters

There will be dedicated links into the Wigan and Bootle sites from the ICL Pathway Headquarters at Feltham.

8.9.1.1 All links from the ICL Pathway Headquarters site (FEL01) to the Wigan and Bootle campuses will be encrypted.

8.9.1.2 The European Development Support Centre (EDSC) and Roll-out Database systems will have controlled access for maintenance purposes only.

8.9.1.3 The Fraud Risk Management (FRM), On-line Analytical Processing (OLAP) and Oracle Financials connections will only provide client access to the respective applications that run at Wigan on the Management Information System(MIS).

8.9.1.4 The EDSC and Roll-out Database platforms will use a different LAN segment from that used by the FRM, OLAP and Oracle Financials.

A router will be used to prevent access between the two LAN segments. The network configuration is illustrated in [TED].

Links used by ICL Pathway to retrieve Track and Trace data from the Royal Mail will not be protected. The ISDN dial-up, initiated by ICL Pathway from Wigan or Bootle, will be to a dedicated PC at the Royal Mail site at Chesterfield.

FUJ00087988

8.9.2 Protection

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

8.9.3 Key Management

8.9.3.1 The standard key management facilities, provided by the bought-in devices, will be used.

8.10 Key Generation

Cryptographic keys will be generated in one of the following ways:

8.10.1.1 Where government approved hardware devices have been purchased, key material will be provided in whatever standard approved way is normally recommended for that product.

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

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

8.10.1.4 The stock of Diffie-Hellman values to be used will be supplied by CESG.

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

9. MESSAGE PROTECTION

9.1 Technology

All message protection will be performed using DSA with a 768 bit modulus. Each DSA signature requires a cryptographically strong random initialisation value, known as a K-value.

FUJ00087988

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

9.2 Key Management

9.2.1 Public Key Technology

Standard simple public key technology will be used, as outlined below.

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

The "CA private key" will have a corresponding public key called the "CA public key".

9.2.2 Public Key Certificates

ICL Pathway's "PK certificates" will be semantically based upon the X.509 standard.

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

9.2.2.2 The CA private key will be held securely on a PC in a secure room not connected to the ICL Pathway network.

9.2.2.3 Whenever a signed message is sent from a Post Office, the PK certificate, containing the public key needed to verify that message, is sent with it. Software, receiving such a signed message, verifies the signature and expiry date on the PK certificate. It also checks the Post Office FAD code identified in the certificate to ensure that the public key corresponds to the sending Post Office's private key. It then verifies the message itself using the public key (now known to be correct) in the certificate. Suitable caching of known valid public key certificates will enable receivers to omit the certificate validation step.

9.2.2.4 Similarly, when the KMS sends out a signed message, the public key certificate for the signing key (KICert) is sent with the signed data.

9.2.3 Constraints

FUJ00087988

Signed messages from the ICL Pathway campuses (payment authorisations in the first release) cannot be handled in the same way as Automated Payments. The impact on traffic volumes of sending a certificate with each authorisation would be too heavy. For centrally signed data, each Post Office will, therefore, be installed with a stock of public keys corresponding to a set of central signing private keys. Similar provision is made for software issue signing keys.

Each of the private keys has a life of 2 years. The Post Offices can, therefore, step through them over the years as each one expires (during which time a new key renewal strategy will be devised).

Notwithstanding this, provision is made in the design to change these key values through the routine key replacement mechanism.

9.3 BES Payment Authorisations

9.3.1.1 Payment authorisations will be digitally signed on leaving the PAS/CMS machine. Signatures will be verified immediately prior to use by the BES application in individual workstations at the Post Offices.

The initial public key stock, used for signature verification in the Post Offices, will be pre-installed at roll-out as described in section 8.6.2.

9.4 Automated Payments

9.4.1.1 Transactions digitally signed at post offices will be signature verified at the harvesting agent that takes the transaction from the correspondence servers and transfers it to the AP host. The signature will be carried forward into the AP Host database, along with the rest of the transaction, giving the capability for checking downstream if required.

9.4.1.2 The format of the signed AP data will be so arranged that it can be verified outside the attribute grammar format used within TMS .

9.4.1.3 Until the transition AP data feed from HAPS dries up, the individual transaction digital signatures will not be verified at the client sites. However, this facility will be enabled for AP once the HAPS flow has ceased.

For new integrity-critical products, the same overall architecture will still hold. It entails signing in the post office, verifying at the harvester, with the signature continuing to be available for checking on a true "end to end" basis at the client-end PC if required. For these products, the issue of a separate feed of unsigned data from HAPS does not apply.

FUJ00087988

9.4.1.4 Post Office private keys will be replaced at intervals agreed with the Contracting Authorities, based on advice from CESG, using the routine key replacement mechanism.

9.5 Software Distributed to Post Offices

New software releases will be distributed to Post Offices over the ISDN links (specified in section 8.6).

9.5.1 Tivoli

9.5.1.1 All messages initiated by the Tivoli management mechanism will be digitally signed, for protection in transmission, using the Software Issue Private Key (SIPR) and verified on receipt using the corresponding Public Key (SIPU). The signature will use 512 bit DSA.

9.5.2 Riposte

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

9.5.2.2 The private key used in the signature will be held in a high security environment at an ICL Pathway central site.

This protection regime will use standard Microsoft cryptographic interfaces.

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

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

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

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

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

FUJ00087988

9.6 Other Message Types

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

With the infrastructure defined for Automated Payments, it is technically possible to provide end-to-end protection of a message travelling from one Post Office to another. The functionality is straightforward, enabling the quality of security provided to be significantly improved (as a future prospect).

10. FILESTORE ENCRYPTION IN POST OFFICES

10.1 Data Confidentiality

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

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

The whole of the swap file will be encrypted prior to the loading of any externally supplied key material. The key used will be internally generated by the TeamCrypto product using its own entropy, and will be different for each boot-up of the PC.

The algorithm used will be Red Pike.

10.2 Functionality

FUJ00087988

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

Protection will be applied after delivery on site.

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

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

10.3 Security Considerations

Some basic security considerations of the solution are :

10.3.1.1 The KMS will be the source of the keys for all files except the swap file, for which a new key will be dynamically established on each PC on each boot-up.

10.3.1.2 The product used will be Team Crypto, for which CESG approval is required.

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

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

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

More detail is given in Section 8.7.2.3 and in [CDS].

10.3.1.5 It will be possible, at intervals agreed with the Contracting Authorities, based on advice from CESG, to change the filestore encryption key.

FUJ00087988

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

11. ADMINISTRATION OF SECURITY

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

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

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

11.1 Management Roles and Responsibilities

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

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

The following subsections provide a simplistic overview of the operational, system management and support roles, based upon the initial pilot system(s).

11.1.1 Operational Roles

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

- BA (ICL Series 39 system) operations (EDS),
- PAS/CMS Help Desk Advisor (ICL Pathway/Girobank),
- DLR CMS operations (De La Rue),
- Post Office Manager (POCL), and
- Post Office Counter Clerks (POCL).

A PAS/CMS Help Desk hierarchy of Manager, Supervisor and Advisor will be used.

The DLR CMS operations personnel, located on De La Rue premises, will use the output from CMS for the production of cards and generation of Pick-Up Notices (PUNs).

FUJ00087988

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

11.1.2 Systems Management Roles

The system management roles will be assigned to personnel who keep the system running for the "users" in the operational roles. In simple terms, these are the roles for which CFM will have main responsibility, as follows:

- System Manager (ICL CFM/ICL DSD),
- System Operator (ICL CFM),
- Database Administrator (ICL CFM/Oracle),
- Network Manager (ICL CFM), and
- Encryption Key Custodians (ICL CFM, EDS and DLR).

Encryption key custodians will have responsibility for the use and safekeeping of encryption keys. These keys will be used to enable the Rambutan based encryption devices at each site. For simplicity, CFM will manage all keys used in ICL Pathway's central Data Centre site. EDS are expected to manage the keys at the BA end of the CAPS links and De La Rue will manage the keys used at their Card Production sites.

11.1.3 Support Roles

The support roles will be primarily concerned with keeping all equipment operational. These activities, which include monitoring and exception handling, will be supported, primarily, by ICL DSD, as follows:

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

11.2 Systems Management Components

Systems management services will be based upon three main products, namely:

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

Tivoli will handle all services on NT systems, software distribution to UNIX systems and central event management services.

FUJ00087988

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

Patrol will be used to manage all Sequent systems and the Oracle applications which run on Sequent platforms.

11.2.1 Tivoli

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

Within TME, Tivoli provides applications which support:

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

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

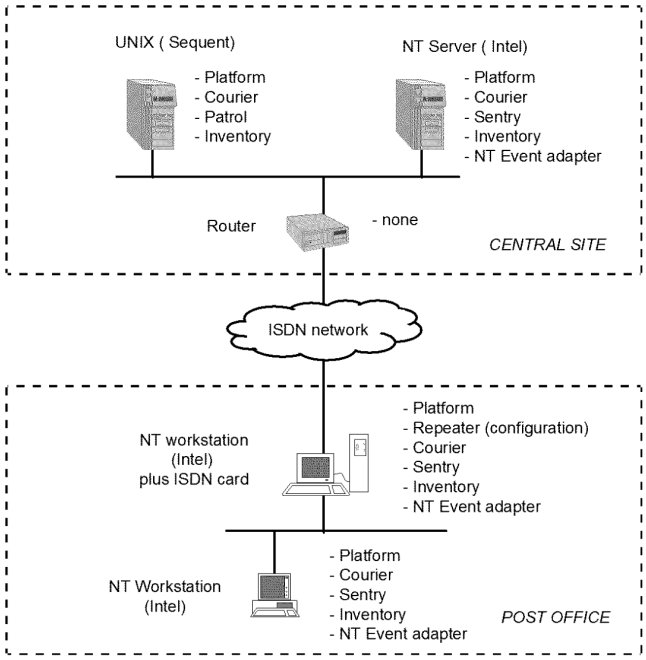

Figure 11 - 1 Deployment of Tivoli Products

Tivoli products will be deployed as illustrated in figure 11-1.

FUJ00087988

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

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

11.2.2 HP OpenView

HP OpenView will be used to provide the network management service.

11.2.3 Patrol

Patrol will be used to manage the Sequent platforms and the Oracle applications which run on those platforms.

11.3 Systems Management Services

The services provided will include:

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

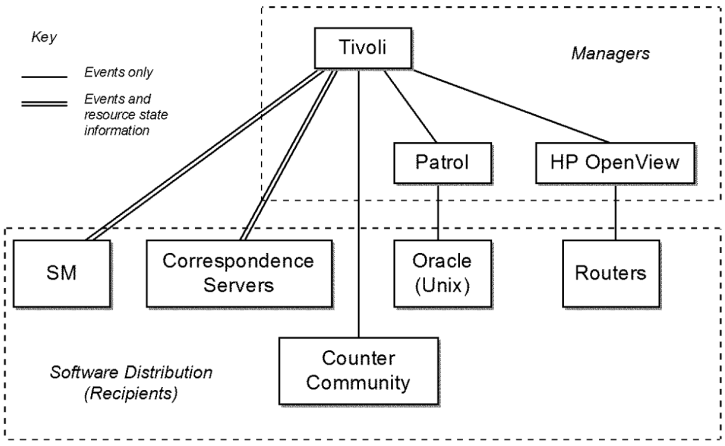

Figure 11 - 2 Systems Management Components

The three system management products (described in section 11.2) will be combined as illustrated in figure 11-2.

FUJ00087988

11.3.1 Software Distribution

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

The Tivoli Courier management application will provide the means of managing and distributing software across a multi-platform network that includes Unix machines and Windows NT platforms.

11.3.1.1 The software distribution system will be used to manage end systems in order to distribute, activate and delete software products.

11.3.1.2 Tivoli will run within the authentication and access controls specified in earlier sections of this document.

11.3.1.3 Tivoli Courier will provide a full audit log of all distributions.

This will indicate whether distributions were successful and whether any failures occurred. The time of successful distributions/failures will also be included together with identification of the individual who initiated the distribution.

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

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

This supporting infrastructure will also provide:

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

The four stages in the release management process, which includes package distribution, are illustrated in figure 11-3.

FUJ00087988

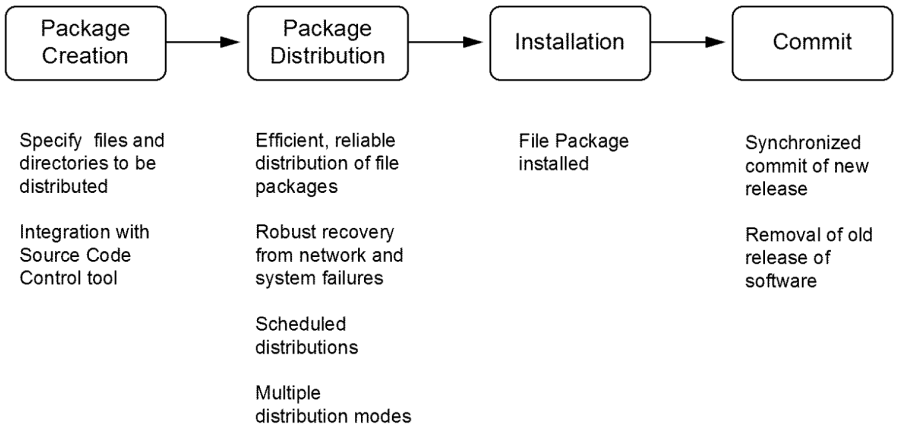

Figure 11 - 3 Release Management Process

Tivoli Courier will provide the ability to run programs:

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

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

11.3.2 Event Management

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

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

11.3.2.2 The event logs used by Windows NT will be integrated with the system management components.

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

FUJ00087988

11.3.3 Network Management

Network management will be run from a central service providing facilities for :

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

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

1. The backbone network - comprising the LAN hubs and LAN attachments at the ICL Pathway central sites, the links between the ICL Pathway sites, links to DSS and POCL, with associated routers.

1. The branch ISDN network - terminated at the central routers and at the gateway PC at each outlet.

1. The office LAN at each outlet - comprising the PC LAN attachments and local Ethernet hub (present where three or more PCs are installed).

Management of the underlying ISDN switched circuit network will be provided by British Telecom. It is envisaged that the implementation of Network Management will include interfacing to the Network service supplier to obtain a structured data feed regarding the state of the whole network including ISDN.

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

11.3.4 Resource Monitoring

11.3.4.1 The resource monitoring facilities will be used to establish criteria for monitoring an individual resource.

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

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

11.3.5 Inventory Management

11.3.5.1 The Tivoli Inventory application will be used to manage the software and hardware inventory.

FUJ00087988

11.3.5.2 A central repository will hold persistent records identifying the software products installed on each managed node.

11.3.5.3 The data recorded will be obtained by evaluating the software signature for each software product on the managed nodes.

11.3.5.4 The central repository will hold persistent records identifying the hardware associated with individual managed nodes and its attached peripherals.

11.3.5.5 Where appropriate, asset numbers will be held for the individual components.

11.4 User Management

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

11.4.1 Administration of User Accounts

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

Each Post Office Manager will manage the small group of Post Office Counter Clerks within his Post Office as a local community. The interface used will be provided by Riposte which will map to the underlying Windows NT functions.

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

11.4.2 Administration of Access Controls

Access controls will be configured in accordance with [ACCPOL] using the facilities outlined in section 6.

Appendix A Windows NT Audit Events

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

Windows NT File and Directory Access

FUJ00087988

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

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

Table A-1 Windows NT File and Directory Access

Windows NT Registry Audit

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

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

Table A-2 Interpretation of Windows NT Registry Audit Options

Appendix B Mapping to Security Requirements

This appendix contains a matrix indicating how the functions described within the Security Functional Specification map to the security requirements.

Security requirements, which ICL Pathway has documented in [SECOBJ], have been extracted from several documents (including Schedule B-01).

FUJ00087988

SFS Section	Subject	Test No.	Objective Reference	Origin	Source Reference
4.2 and 4.2.1.1	Windows NT Security	A1	2.1 CMS1/1 5.14 CMS7/2		
4.3 and 4.3.1.1	Dynix Operating System	A2	2.2 CMS1/1 5.14 CMS7/2		
4.4 and 4.4.1.1	Database Management System	A3	2.3 CMS1/1 5.14 CMS7/2		
4.7.2.1	Virus Protection	A4		-	-
4.7.2.2	Virus Protection	A5		-	-
4.7.2.3	Virus Protection	A6		-	-
4.7.2.4	Virus Protection	A7		-	-
4.7.2.5	Virus Protection	A8		-	-
4.7.2.6	Virus Protection	A9		-	-
5.1.1	User Identification	B1	5.4 BPS7.1 9.2.3 PSR9.1.6		
5.1.1.1	User identification	B2		-	-
5.1.1.2	User identification	B3		-	-
5.1.1.3	User identification	B4		-	-
5.1.1.4	User identification	B5		-	-
5.1.1.5	User identification	B5a		-	-
5.1.1.6	User identification	B5b		-	-
5.1.2	User Authentication	B6	5.5 BPS7.1 9.2.3 PSR9.1.6		
5.1.2.1	User authentication	B7		-	-
5.1.2.2	User authentication	B8		-	-
5.1.2.3	User authentication	B9		-	-
5.1.2.4	User authentication	B10		-	-
5.1.2.5	User authentication	B11		-	-
5.1.2.6	User authentication	B12		-	-
5.1.3.1	Passwords	B13		-	-
5.1.3.2	Passwords	B14		-	-
5.1.3.3	Passwords	B15		-	-
5.1.3.4	Passwords	B16		-	-
5.1.3.5	Passwords	B17		-	-
5.1.3.6	Passwords	B18		-	-
5.1.3.7	Passwords	B19		-	-
5.1.3.8	Passwords	B20		-	-
5.1.3.9	Passwords	B21		-	-
5.1.3.10	Passwords	B22		-	-
5.1.3.11	Passwords	B23	4.19 **REQ473**	B-01	473
5.1.3.12	Passwords	B24	4.19 **REQ473**	B-01	473

FUJ00087988

5.1.3.13	Passwords	B25	4.19 **REQ473**	B-01	473
5.1.4.1	Use of Tokens	B26		-	-
5.1.4.2	Use of Tokens	B27		-	-
5.1.4.3	Use of Tokens	B28		-	-
5.1.4.4	Use of Tokens	B29		-	-
5.1.4.5	Use of Tokens	B30		-	-
5.1.4.6	Use of Tokens	B31		-	-
5.1.4.7	Use of Tokens	B32		-	-
5.1.4.8	Use of Tokens	B33		-	-
5.2.1.1	Authentication of NT users	B34		-	-
5.2.1.2	Authentication of NT users	B35		-	-
5.2.1.3	Authentication of NT users	B36		-	-
5.2.2.1	Windows NT logon	B37		-	-
5.2.2.2	Windows NT logon	B38		-	-
5.2.2.3	Windows NT logon	B39		-	-
5.2.2.4	Windows NT logon	B40		-	-
5.2.3.1	Logon at PO locations	B41		-	-
5.2.3.2	Logon at PO locations	B41a		-	-
5.3	Authentication of Oracle Users	B42	2.6 CMS1/1 5.14 CMS7/2		
5.3.1.1	Authentication of Oracle users	B43		-	-
5.3.1.2	Authentication of Oracle users	B43a		-	-
5.3.1.3	Authentication of Oracle users	B44		-	-
5.3.1.4	Authentication of Oracle users	B45		-	-
5.3.1.5	Authentication of Oracle users	B46		-	-
5.4.1.1	Authentication of Help Desk users	B47		-	-
5.4.1.2	Authentication of Help Desk users	B48		-	-
5.4.1.3	Authentication of Help Desk users	B49		-	-
5.4.1.4	Authentication of Help Desk users	B50		-	-
5.5	Authentication of DSS/BA	B51	5.6 PSR8.7 (3)		
5.6	Authentication of POCL	B52	5.1 PSR8.9.1 PSR8.9.2 (2) 5.7 CMS3/3 5.8 CMS34/1 5.8 CMS7/2 5.16 PSR8.9.2 (3) 5.17 PSR8.10.3		
6	Logical Access Control	C1	4.9 REQ473 5.10 PSR8.9.3		

FUJ00087988

			5.10 (3) 5.10 BPS7.1 5.11 BPS7.1 6.11 PSR8.10.1(1) 9.2.12 PSR9.1.6 9.2.13 PSR9.1.7		
6.1.1.1	Access Control Policy	C2		-	-
6.1.2.1	Privileges and Roles	C3		-	-
6.1.4	Two Person Controls	C4	5.5 PSR8.9.3 (3)		
6.2	Control of Access to Database	C5	5.4 PSR8.9.3 (2)		
6.3	Access Controls - NT	C6			
6.3.1.1	Configuration - Windows NT	C7		-	-
6.3.2.1	Windows NT ACLs	C8		-	-
6.3.3.1	Windows NT tools used for access control	C9		-	-
6.4	Access Controls - Dynix	C10	2.14 CMS1/1 5.14 CMS7/2		
6.4.2.1	Dynix Access Controls	C11		-	-
6.4.2.2	Dynix Access Controls	C12		-	-
6.5.1.1	Routers - access methods	C13		-	-
6.5.1.2	Routers - access methods	C14		-	-
6.5.1.3	Routers - access methods	C15		-	-
6.5.1.4	Routers - access methods	C16		-	-
6.5.2.1	Routers - privilege mode access	C17		-	-
6.5.3.1	Routers - access lists	C18		-	-
6.5.3.2	Routers - access lists	C19		-	-
6.5.3.3	Routers - access lists	C20		-	-
6.5.3.4	Routers - access lists	C21		-	-
6.5.3.5	Routers - access lists	C22		-	-
7	Audit and Alarms	C23	4.15 BPS8.2.1 4.16 BPS8.2.2 4.17 REQ472 5.18 CMS3/3 5.19 CMS34/1 **9.10.20** BPS9.1.5 9.10.2 BPS9.2.5 9.10.4 BPS9.4.5 9.10.21 BPS9.5.5 9.10.22 BPS9.6.5 12.1 REQ699		
7.3.1.1	Auditable events	C24		B-01	942

FUJ00087988

7.3.1.2	Auditable events	C24a		B-01	942
7.4.1.1	Application level Audit	C25		B-01	942
7.4.1.2	Application level Audit	C26		B-01	699
7.4.2.1	Audit at CAPS interface	C27		B-01	699
7.4.2.2	Audit at CAPS interface	C28		B-01	699
7.4.2.3	Audit at CAPS interface	C29		B-01	699
7.4.2.4	Audit at CAPS interface	C30		B-01	699
7.4.2.5	Audit at CAPS interface	C31		B-01	699
7.4.2.6	Audit at CAPS interface	C32		B-01	699
7.5.3.1	Audit logs within the database	C33		B-01	699
7.4.3.2	Audit logs within the database	C34		B-01	699
7.4.3.3	Audit logs within the database	C35		B-01	699
7.4.3.4	Audit logs within the database	C36		B-01	699
7.4.4.1	Riposte Transaction log	C37		B-01	699
7.4.4.2	Riposte Transaction log	C38	4.18 **REQ472**	B-01	472
7.4.4.3	Riposte Transaction log	C39	4.18 **REQ472**	B-01	472
7.4.4.4	Riposte Transaction log	C40	4.18 **REQ472**	B-01	472
7.4.4.5	Riposte Transaction log	C41	4.18 **REQ472**	B-01	472
7.4.4.6	Riposte Transaction log	C42	4.18 **REQ472**	B-01	472
7.4.4.7	Riposte Transaction log	C43		B-01	478
7.4.5.1	Logging in fall-back mode	C44		B-01	699
7.4.5.2	Logging in fall-back mode	C45		B-01	699
7.4.5.3	Logging in fall-back mode	C46		B-01	699
7.5.1.1	Application level audit analysis	C47		B-01	699
7.5.1.2	Application level audit analysis	C48		B-01	699
7.5.1.3	Application level audit analysis	C49		B-01	699
7.5.1.4	Application level audit analysis	C50		B-01	699
7.6.1.1	Protection of audit logs	C51		B-01	699
7.6.1.2	Protection of audit logs	C52		B-01	699
7.7.1.1	Audit of SM functions	C53		B-01	699
7.7.1.2	Audit of SM functions	C54		B-01	699
7.7.1.3	Audit of SM functions	C55		B-01	699
7.7.1.4	Audit of SM functions	C56		B-01	699
7.7.1.5	Audit of SM functions	C57		-	-
7.7.1.6	Audit of SM functions	C58		-	-
8	Crypto Functionality	D1	2.22 BPS6.3		
8.1	Crypto - CAPS Links	D2	2.1 CMS1/1		
8.1.1.1	Crypto - CAPS Links	D3		-	-
8.1.2.1	CAPS Link Protection	D4		-	-
8.1.3.1	CAPS Link Key Management	D5		-	-
8.1.3.2	CAPS Link Key Management	D6		-	-

FUJ00087988

8.1.3.3	CAPS Link Key Management	D7		-	-
8.2	Crypto - CMS Links (to DLR)	D8	2.1 CMS1/1		
8.2.1.1	CMS Link Protection	D9		-	-
8.2.1.2	CMS Link Protection	D10		-	-
8.2.1.3	CMS Link Protection	D11		-	-
8.2.1.4	CMS Link Protection	D11a		-	-
8.2.2.1	CMS Link Key Management	D12		-	-
8.2.2.2	CMS Link Key Management	D14		-	-
8.2.2.3	CMS Link Key Management	D15		-	-
8.3	Crypto - POCL TIP Link	D16	9.7.6 BPS9.6.1		
8.3.1.1	POCL TIP Link Protection	D17		-	-
8.3.1.2	POCL TIP Link Protection	D18		-	-
8.3.1.3	POCL TIP Link Protection	D18a		-	-
8.3.2.1	POCL TIP Link - Key Management	D18b		-	-
8.4.1.1	POCL Farnborough Link - Protection	D18c		-	-
8.4.2.1	POCL Farnborough Link - Key Management	D18d		-	-
8.5.1.1	AP Client Links	D18e		-	-
8.5.1.2	AP Client Links	D18f		-	-
8.6	PO ISDN Links	D23	9.2 REQ467		
8.6.1.1	PO ISDN Link Protection	D24		-	-
8.6.1.2	PO ISDN Link Protection	D25		-	-
8.6.2	PO ISDN Link Roll-out	D26	4.23 PAS2.13		
8.6.2.1	PO ISDN Link Roll-out	D26a		-	-
8.6.2.2	PO ISDN Link Roll-out	D26b		-	-
8.6.2.3	PO ISDN Link Roll-out	D26c		-	-
8.6.2.4	PO ISDN Link Roll-out	D26d		-	-
8.6.2.5	PO ISDN Link Roll-out	D26e		-	-
8.6.2.6	PO ISDN Link Roll-out	D26f		-	-
8.6.2.7	PO ISDN Link Roll-out	D26g		-	-
8.6.2.8	PO ISDN Link Roll-out	D26h		-	-
8.6.2.9	PO ISDN Link Roll-out	D26I		-	-
8.6.2.10	PO ISDN Link Roll-out	D26j		-	-
8.6.2.11	PO ISDN Link Roll-out	D26k		-	-
8.6.3	CHAP Key Management	D27	9.2.8 PSR9.4		
8.6.3.1	CHAP Key Management	D28		-	-
8.6.3.2	CHAP Key Management	D28a		-	-
8.6.3.3	CHAP Key Management	D28b		-	-
8.6.3.4	CHAP Key Management	D28c		-	-
8.6.3.5	CHAP Key Management	D28d		-	-
8.6.3.6	CHAP Key Management	D28e		-	-
8.7.1.1	PO LAN Protection	D29		-	-
8.7.1.2	PO LAN Protection	D30		-	-

FUJ00087988

8.7.2.1	PO LAN Key Management	D31		-	-
8.7.2.2	PO LAN Key Management	D32		-	-
8.7.2.3	PO LAN Key Management	D33		-	-
8.8.1.1	Inter-campus Link Protection	D34		-	-
8.8.2.1	Inter-campus Key Management	D35		-	-
8.95	Crypto - SIS Help Desk Links	D36	5.5 PSR8.9.3 (3)		
8.9.1.1	SIS/ Help Desk and SM Links	D37		-	-
8.9.1.2	SIS/ Help Desk and SM Links	D38		-	-
8.9.2.1	SIS/SM Link Protection	D39		-	-
8.9.2.2	SIS/SM Link Protection	D41		-	-
8.9.2.3	SIS/SM Link Protection	D42		-	-
8.9.3.1	SIS/SM Link Key Management	D44		-	-
8.10.1.1	Links with ICL Pathway HQ	D45		-	-
8.10.1.2	Links with ICL Pathway HQ	D46		-	-
8.10.1.3	Links with ICL Pathway HQ	D47		-	-
8.10.1.4	Links with ICL Pathway HQ	D48		-	-
8.10.2.1	Links with ICL Pathway HQ - Protection	D49		-	-
8.10.3.1	Links with ICL Pathway HQ - Key Management	D50		-	-
8.11.1.1	Key Generation	D51		-	-
8.11.1.2	Key Generation	D52		-	-
8.11.1.3	Key Generation	D53		-	-
8.11.1.4	Key Generation	D54		-	-
8.11.1.5	Key Generation	D55		-	-
9	Message Protection	E1	2.24 BPS6.3 3.25 PSR8.5.2 3.11 REQ799 9.26 REQ467 9.27 REQ934 9.27 REQ935/ BPS9.1 9.27 PAS3.3 9.71 BPS9.1.1 9.72 BPS9.2.1 9.28 BPS9.3.1 9.29 BPS9.4.1 9.29 BPS9.5.1 9.29 BPS9.6.1 9.8.30 BPS9.3.3 9.8.30 BPS9.4.3 9.8.30 BPS9.5.3 9.8.30 BPS9.6.3 9.11.31 BPS9.1. 6		

FUJ00087988

			9.11.4 BPS9.4.6 9.11.32 BPS9.5.6/ PAS3.6 9.11.32 BPS9.6.6 9.2.33 PSR9.1.4 9.2.34 PSR9.1.5 9.2.5 PSR9.2.2		
9.2	DSA - Key Management	E2	9.2.8 PSR9.4		
9.2.2.1	Public Key Certificates	E3		-	-
9.2.2.2	Public Key Certificates	E4		-	-
9.2.2.3	Public Key Certificates	E5		-	-
9.2.2.4	Public Key Certificates	E6		-	-
9.3.1.1	BES Payment Authorisations	E7		-	-
9.3.1.2	BES Payment Authorisations	E8		-	-
9.4.1.1	Automated Payments	E9		-	-
9.4.1.2	Automated Payments	E9a		-	-
9.4.1.3	Automated Payments	E9b		-	-
9.4.1.4	Automated Payments	E9c		-	-
9.5.1.1	Distributed to POs - Tivoli	E11		-	-
9.5.2.1	Distributed to POs - Riposte	E12		-	-
9.5.2.2	Distributed to POs - Riposte	E13		-	-
9.5.2.3	Distributed to POs - Riposte	E14		-	-
9.5.3.1	Protection of Non-desktop Software on Post Office PCs	E15		-	-
9.5.3.2	Protection of Non-desktop Software on Post Office PCs	E16		-	-
10	Filestore encryption	F1	4.35 PAS214 9.2.7 PSR9.3		
10.1	Data Confidentiality	F2	5.11 BPS7.1		
10.3.1.1	Filestore encryption - Security	F3		-	-
10.3.1.2	Filestore encryption - Security	F4		-	-
10.3.1.3	Filestore encryption - Security	F5		-	-
10.3.1.4	Filestore encryption - Security	F6		-	-
10.3.1.5	Filestore encryption - Security	F7		-	-
11.2	System Management	G1	9.16.36 BPS9.1.14 9.16.36 BPS9.2.14 9.16.36 BPS9.3.14 9.16.36 BPS9.4.14 9.16.36 BPS9.5.14		

FUJ00087988

			9.16.36 BPS9.6.14 10.37 PSR10 10.38 PSR11		
11.2.1.1	SM - Tivoli	G2		-	-
11.3.1.1	SM - software distribution	G3		-	-
11.3.1.2	SM - software distribution	G4		-	-
11.3.1.3	SM - software distribution	G5		-	-
11.3.2.1	SM - event management	G6		-	-
11.3.2.2	SM - event management	G7		-	-
11.3.2.3	SM - event management	G8		-	-
11.3.4.1	SM - resource monitoring	G9		-	-
11.3.4.2	SM - resource monitoring	G10		-	-
11.3.5.1	SM - inventory monitoring	G11		-	-
11.3.5.2	SM - inventory monitoring	G12		-	-
11.3.5.3	SM - inventory monitoring	G13		-	-
11.3.5.4	SM - inventory monitoring	G14		-	-
11.3.5.5	SM - inventory monitoring	G15		-	-

Appendix C Tables of (Cryptographic) Keys

This appendix provides a summary of the cryptographic keys used in the solution. For further details refer to the Cryptography High Level Design Specification [CDS].

C1. Link Level Keys

Table C-1 identifies the keys used to protect communications links on a point-to-point basis. Key material handled as part of the Post Office key management scheme are identified in the next section.

Crypto Service type or instance	Crypto Service	Key Material Classification	Type	Key vector occurrences (note 1)	Keys (note 6)
Link Level Encryption	LLE	Rambutan - K	KEK	K_{LLE1} .. K_{LLE2n} where n is a count of links protected	2n
Link Level Encryption		Rambutan - D	DEK	D_{LLE1} .. D_{LLE2n} where n is a count of links protected	n
CAPS link protection	CAPS	Red Pike - CAS	DEK	D_{CAPS1} .. D_{CAPSn} where n is a count of ACCs	n
		Red Pike - PAS	DEK	D_{CAPS1} .. D_{CAPSn} where n is a count of ACCs	n
CMS link protection	CMS	Red Pike - CMS	DEK	D_{CMS1} .. D_{CMSn} where n is a count of DLR locations	n

FUJ00087988

		Red Pike - DLR	DEK	D_{CMS1} .. D_{CMSn} where n is a count of DLR locations	n
Certification Authority signing	CA	CA - Public	DEK	D_{CAPUB1} .. D_{CAPUBn} where n = Number of Campus locations + number of PO counters	1
		CA - Private	DEK	$D_{CAPRIV1}$ .. $D_{CAPRIVn}$ where n = Number of Campus locations	n
		CA - System	Param.	D_{CASYS1} .. D_{CASYSn} where n = Number of Campus locations + number of PO counters	1
Software distribution signing	SD	Software Distribution - Public	DEK	D_{SDPUB1} .. D_{SDPUBn} where n = Number of Campus locations + number of PO counters	1
		Software Distribution - Private	DEK	$D_{SDPRIV1}$ .. $D_{SDPRIVn}$ where n = Number of Campus locations	n
		Software Distribution - System	Param.	D_{SDSYS1} .. D_{SDSYSn} where n = Number of Campus locations + number of PO counters	1
PO Filestore encryption	PF	PO Filestore	DEK	D_{PF1} .. D_{PFn} where n = Number of Campus locations + number of PO counters	n
*****	KEK-PO	PO Counter Key	KEK	K_{PO1} .. K_{POn} where n = Number of Campus locations + number of PO counters	n
Payment Authorisation Message protection	PA	Payment Authorisation - Public	DEK	D_{PAPUB1} .. D_{PAPUBn} where n = Number of Campus locations + number of PO counters	1
		Payment Authorisation - Private	DEK	$D_{PAPRIV1}$ .. $D_{PAPRIVn}$ where n = Number of Campus locations	n
		Payment Authorisation - System	Param.	D_{PASYS1} .. D_{PASYSn} where n = Number of Campus locations + number of PO counters	1
Automated Payment protection	AP	Automated Payments - Public	DEK	D_{APPUB1} .. D_{APPUBn} where n = Number of Campus locations + number of PO counters	1
		Automated Payments - Private	DEK	$D_{APPRIV1}$ .. $D_{APPRIVn}$ where n = number of PO counters	n
		Automated Payments - System	Param.	D_{APSYS1} .. D_{APSYSn} where n = Number of Campus locations + number of PO counters	1

FUJ00087988

Network Key Management	KEK-NM	Network endpoint Key	KEK	K_{NM1} .. K_{NMn} where n = Number of Campus locations + number of PO counters	n
		Secret Receive Key	DEK	D_{NM-SR1} .. D_{NM-SRn} where n = Number of Campus locations + number of PO counters.	N
		Public Receive Key	DEK	D_{NM-PR1} .. $D_{NM-PR2n}$ where n = Number of Campus locations + number of PO counters	2n
		Secret Send Key	DEK, Session		
		Public Send Key	DEK, Session		n
CHAP	CHAP	Chap shared Secret	*****	D_{CHAP1} .. D_{CHAPn} where n = Number of PO locations + Number of non PO ISDN locations to communicate with	n
Roll-out	GRK	Global Roll-out Key	DEK	D_{GRK1} .. D_{GRKn} where n = Number of Campus locations + number of PO counters	1 per change of value during roll-out.

Table C - 1 Summary of Link Level Key Usage

Notes

1. Key material elements are vectors (since they need to support non synchronised key changes).

1. Terminology and Abbreviations:
   KEK = Key Encryption Key
   DEK = Data Encryption Key
   Param. = System wide values

1. The term “link” is used very generally in the above table. It either refers to a network level link or one of a number of logical links between applications.

1. Initialisation vectors have not been included in the above table.

1. Number of different key vectors (n refers to corresponding value in previous column).

FUJ00087988

C2. Keys Used in the Post Office Key Management Scheme

The keys used in the Post Office Key Management Scheme are summarised in Table C-2.

Symmetric keys provided for the Red Pike algorithm are 64 bits. Asymmetric DSA keys are 192 bits (private) and 768 bits (public).

FUJ00087988

Key	Use
ACK	Symmetric communications key for protecting application data passed over the link (also to be used as the Post Office LAN encryption key).
APCert	Public Key Certificate signed by CAPR containing APPU.
APPR	Private DSA key under which Automated Payments will be signed at the Post Office.
APPU	Public DSA key corresponding to APPR.
CAPR	The private DSA key of the Certification Authority. This very long lived key is not held on-line anywhere in the ICL Pathway system.
CAPU	Public DSA key corresponding to CAPR.
CHAP	Challenge Handshake Authentication Protocol key.
CK	Symmetric communications key used for encrypting key material sent from the KMS to a Post Office.
DH-Value	Secret random value used in Diffie-Hellman exchanges to generate a shared key between a Post Office and the KMS.
FEK	Symmetric filestore encryption key for Post Office PCs.
KEK	Symmetric key, derived from KES and PIN, used to encrypt other keys on the Post Office Manager's Memory Card.
KES	Symmetric encryption key seed value used later to protect FEK on Post Office PCs.
KICert	Public Key Certificate signed by CAPR containing KIPU.
KIPR	Private DSA key held at the KMS, used for signing key material issued by the KMS.
KIPU	Public DSA key corresponding to KIPR.
PACert	Public Key Certificate signed by CAPR containing PAPU.
PAPR	Private DSA key for signing payment authorisations.
PAPU	Public DSA key for verifying payment authorisations (corresponding private key is PAPR).
PBValues	Fixed non-secret values used as prime and base values in Diffie-Hellman exchanges. The same values are used throughout the ICL Pathway system.
PIN	Secret value, known by the Post Office Manager, used to unlock the Memory Card.
POK	Symmetric key installed in PCs prior to rollout.
POK-Id	Identifier for the Post Office Key POK.
SICert	Public Key Certificate signed by CAPR containing SIPU.
SIPR	Private DSA key used for signing software issued to the Post Offices.
SIPU	Public key for verifying software issue (corresponding private key is SIPR).

Table C - 2 Summary of Keys used in Post Office KMS