FUJ00152138

Document Title: Pathway Security Solution Summary

Document Type: Management Summary

Abstract: A summary of the Pathway security approach, policy, strategy and implementation.

Status: Issued

Distribution:

Author: Martyn Bennett

Comments to: Martyn Bennett

Comments by:

FUJ00152138

0 Document control

0.1 Document history

Version	Date	Reason
0.1	19/5/98	Draft for review
0.2	21/5/98	Draft for review
1.0	22/5/98	Issued

0.2 Approval authorities

Name	Position	Signature	Date

0.3 Associated documents

	Reference	Vers	Date	Title	Source
[1]	Authorities' Agreement	8.1	9/3/98	Requirements Schedule (A)B04	DSS/POCL
[2]	Authorities' Agreement	8.1	9/3/98	Solutions Schedule (A)B05	Pathway
[3]	DSS Agreement	8.1	9/3/98	Requirements Schedule (D)A15	DSS
[4]	DSS Agreement	8.1	9/3/98	Solutions Schedule (D)A16	Pathway
[5]	POCL Agreement	8.0	13/11/97	Requirements Schedule (P)A15	POCL
[6]	POCL Agreement	8.1	9/3/98	Solutions Schedule (P)A16	Pathway
[7]	RS/ACS/002	1.1	30/3/98	Security Acceptance Test Specification	Pathway
[8]		01	30/11/95	BPS Security Statement - Pathway	BA/POCL
[9]		1.0	21/12/95	Benefit Payment Service - Security Proposal	Pathway
[10]	TSC/TAP/01		8/7/96	Pathway Security Report	Pathway
[11]	RS/POL/0002	3.0	8/10/96	Pathway Security Policy	Pathway

FUJ00152138

[12]	RS/FSP/0001	1.1	4/11/97	Security Functional Specification	Pathway
		3.0	3/12/97		
[13]	RS/POL/0003	1.0	17/4/97	Access Control Policy	Pathway
		2.0	24/2/98		
[14]	RS/SPE/0001	3.0	09/02/98	Fraud Risk Management Service Design	Pathway
[15]	DW/REQ/017	1.5	10/03/98	FRMS System Requirements Specification	Pathway
[16]	RS/SPE/0003	2.0	08/04/98	Extended Verification Process Requirement	Pathway
[17]	7074A/T/1	1.0	September 1997	Security Review	Admiral
[18]	7074A/T/2	1.0	March 1998	Penetration Testing	Admiral
[19]	VI/STR/0001	2.0	30/9/96	Testing & Integration Strategy	Pathway
[20]	TD/ARC/001	3.3	5/5/98	Technical Environment Description	Pathway
[21]	TD/DES/0031	1.3	3/4/98	Resilience and Recovery Strategy	Pathway
[22]	VI/TSC/105	2.0	28/1/98	Technical Integrity and Networking High Level Test Plan	Pathway
[23]	To be completed			Security Management Procedures	Pathway
[24]	PA/STR/0006	5.0	31/10/97	Release 1c Release Contents Description	Pathway
[25]	RS/RES/002	3.0	5/9/97	Security Exclusions from Release 1c	Pathway
[26]	PA/STR/009	2.0	24/2/98	Release 2 Release Contents Description	Pathway

0.4 Abbreviations

ACP	Access Control Policy
CAPS	Customer Accounting Processing Strategy
CNT	Core Negotiating Team
EVP	Extended Verification Procedures
FCMS	Fraud Case Management System
FRMS	Fraud Risk Management Service
FSG	Fraud and Security Group
PDA	Programme Delivery Authority
SFS	Security Functional Specification

FUJ00152138

0.5 Changes in this version

FUJ00152138

0.6 Table of content

FUJ00152138

1

FUJ00152138

Introduction

The overall Security objective of Pathway has been agreed with the Contracting Authorities:

'It is the policy of ICL Pathway Limited to protect its investment in IT assets, and to ensure the security of all information conveyed, processed or stored by the services'

This involves designing and implementing a system infrastructure that provides:

- Protection of the integrity, availability and confidentiality of information used by the services
- Business Continuity, ie resilience and recovery
- Fraud Risk Management (FRM)
- Compliance with legislative requirements

The system security has been developed to include technical, managerial, procedural and personnel controls to achieve these objectives. The approach has been to provide mitigation that is appropriate to the level of identified and evaluated threats and meets contractual and legislative requirements. The representatives of the Authorities, Fraud and Security Group (FSG), have been involved to a high degree of detail not only in the implementation of the solution, but in its definition as well.

The system security infrastructure can be considered to be composed of a number of components which integrate to achieve these objectives. The development of these and a summary of the components are described in this paper.

2 Pathway Approach

2.1 Requirements

The requirements for security within the Pathway solution fall into three categories:

Contractual:

Those requirements expressed in the contract and schedules which mandate certain security elements of the solution.

Legislative:

Pathways legal obligations to comply with certain Acts: Data Protection Act, Computer Misuse Act, Police & Criminal Evidence Act etc.

Derived:

The security requirements identified internally to mitigate program risks (cryptographic key management, firewalls, one-time passcode generators, security event management, etc.)

All these requirements and their solutions are embodied in the baselined

FUJ00152138

security documentation set: Security Policy, Security Functional Specification, and the Access Control Policy.

2.1.1 Contractual Requirements

The Authorities requirements, and Pathway's associated solutions are embodied in the contract in Requirements Schedules (A)B04 [1] and (A)B05 [2], (D)A15 [3] and (D)A16 [4], and (P)A15 [5] and (P)A16 [6]. Those that are relevant for Security are quoted below, as agreed and described in the Security Acceptance Test Specification [7]. Solutions summaries for each of these requirements have been produced, extensively discussed and agreed with the PDA prior to completion of the 'drop down' process post award of contract.

Requirement 698:

- The contractor shall minimise and control liabilities to itself and the AUTHORITIES.
- The CONTRACTOR shall, by a date consistent with the project plan agreed by the parties, such that the date does not adversely impact contractual milestones as defined in Clause 605.1 of the Authorities Agreement, set up an organised security infrastructure covering:

  (a) the agreement of a security policy;
  (a) allocation of security responsibilities;
  (a) security education and training;
  (a) reporting security incidents;
  (a) physical security control;
  (a) virus control;
  (a) business continuity;
  (a) control of Software;
  (a) safeguarding DSS and POCL records;
  (a) information classification;
  (a) compliance with data protection and other legislation;
  (a) information exchange control;
  (a) CONTRACTOR's sub-contractors and suppliers;
  (a) compliance with security policy;
  (a) the management of fraud and risk during Service operation.
- The CONTRACTOR shall be compliant with BS7799.

Requirement 722

- Card Authentication Methods shall be positive rather than negative, resistant to forgery or other unauthorised manipulation and shall include the mechanism set out in the solution to this requirement for identifying the attempted use of non genuine and / or invalid Cards and Temporary Tokens.

Requirement 723

- Cardholder Verification Methods shall be resistant to impersonation and shall include the mechanism specified in the solution to this requirement for identifying the attempted use of a Card or Temporary Token by a

FUJ00152138

person other than an Authorised Person.

Requirement 747

- All aspects of Card Management including production, storage, delivery and destruction of Cards shall be secure, auditable and allow the production of audit trails of all Cards and collateral material.

Requirement 828

- The confidentiality, integrity, validity and completeness of data shall be maintained throughout all storage, processes and transmissions, including during periods of Service Failure and recovery from Service Failure.
- The CONTRACTOR shall ensure that all data passed from PAS and CMS to CAPS adhere to the current DSS Business Data Standards Document and any future amendments.

Requirement 829

- The CONTRACTOR shall ensure that all relevant information produced by the Service Infrastructure at the request of the AUTHORITIES shall be evidentially admissible and capable of certification in accordance with the Police and Criminal Evidence Act (PACE) 1984, the Police and Criminal Evidence (Northern Ireland) Order 1989 and equivalent legislation covering Scotland.
- At the direction of the AUTHORITIES, audit trail and other information necessary to support live investigations and prosecutions shall be retained for the duration of the investigation and prosecution irrespective of the normal retention period of that information.

Requirement 830

- The CONTRACTOR shall ensure that all Services are supported by contingency plans including fallback Transactions that minimise or negate the impact of failure in any of the Services.
- The CONTRACTOR shall ensure that the contingency plans for each Service are compatible with an overall service continuity framework.
- The contingency plans shall be based on impact and risk assessments and agreed between the CONTRACTOR and the AUTHORITIES by a date consistent with the project plan agreed by the parties, such that the date does not adversely impact contractual milestones as defined in Clause 605.1 of the Authorities Agreement.
- Ownership of all contingency actions shall be identified in the contingency plans.
- The contingency plans shall include activation procedures and time periods within which the contingency measures shall be activated.
- The contingency plans shall include a testing strategy with two distinct parts:
    - Initial testing before commencement of Roll Out of Services;
    - Regular testing.
- The contingency plan shall include without limitation the following:

FUJ00152138

- Prevention measures.
- Preparedness measures.
- Contingency measures.
- Recovery of normal Service.
- Contact lists.

- The contingency plans shall be subject to joint periodic review by the CONTRACTOR and AUTHORITIES by a process to be agreed by a date consistent with the project plan agreed by the parties, such that the date does not adversely impact contractual milestones as defined in Clause 605.1 of the Authorities Agreement, to ensure that they meet the AUTHORITIES' aims.
- When contingency operation is invoked as a result of a fault of the Services provided by the CONTRACTOR, then the provisions of Schedule B03 [Service Level Agreement Schedules] of the AUTHORITIES' Agreement shall continue to apply.

Requirement 872

- Information marked as Nationally Sensitive shall be handled in accordance with the Departmental IT Security Standards (reference DITSG/ITSS/0001.04, version 6.2 dated March 1996) [Version 6.3.1, 15/4/97].

Requirement 897

- The security policies of the CONTRACTOR in providing the Services shall be consistent with the security objectives and policies stated in the BPS Security Statement.
- The CONTRACTOR shall provide an appropriate countermeasure to each threat identified in the BPS Security Statement.

Schedule B08

In addition, Schedule B08 - Benefit Encashment Fraud, defines Pathway's responsibilities and liabilities in the event of a successful fraud attack on the Benefit Payment Service. It introduces the requirement for Extended Verification Procedures (included as part of the solution to Requirement 723).

2.2 Definition and Development of the Security Solution

The requirements were essentially very high level and broad in nature. For that reason, a considerable amount of effort was expended in clarifying them and understanding the Authorities concerns and true requirements both before and after the award of contract. The Authorities representatives, in the guise of the Fraud and Security Group (FSG) were involved in, and reviewed extensively, the development of the security solution.

FUJ00152138

2.2.1 Pre Award of Contract

2.2.1.1 Risk Responses

Prior to award of contract, Pathway provided responses to Risks raised by the PDA regarding the security of our proposed solution. The solution was clarified and discussed in depth with representatives of the Authorities (CNT). In all cases resolution was obtained such that the risks were either removed or represented no impediment to Pathway being asked to bid.

2.2.1.2 Benefit Payment Service Proposal

During the same period as Pathway was discussing the security risks with CNT, we were requested to respond to a BPS Security Statement - Pathway [8]. A full response was provided, the Benefit Payment Service - Security Proposal [9], which provided details of Pathway's approach in the areas of:

- Card Characteristics
- Card production and Personalisation
- Card and Pick Up Notice Distribution
- Card Usage
- Card Support Services
- Contingency
- Interfaces
- Service Development
- Service Transfer
- Fraud and Risk Management

This was subject to comprehensive review and demonstration, prior to Pathway being invited to bid.

2.2.2 Post Award of Contract - Security

2.2.2.1 Definition of the Security Solution

Immediately following the award of contract, Pathway commissioned a comprehensive internal threat analysis [10] by a senior ICL security architect. This was made available to the PDA Fraud and Security Group, and acted as a check for the detailed solution development.

The definition of the Pathway security solution has at all stages been extensively reviewed, commented on fully by the PDA Fraud and Security Group.

The high level Pathway security solution is defined by three key documents (see section 2.3):

- Security Policy [11]. This went through 3 versions and was finally signed off by the PDA on 8/10/96. It is currently undergoing an audit and review.
- Security Functional Specification [12]. This went through prolonged review

FUJ00152138

and revision and version 1.1 was signed off by the PDA on 4/11/96. Since then it has been updated, version 3.0 (3/12/97) being agreed, subject to minor caveats on 9/2/98.

- Access Control Policy [13]. This also went through prolonged review, with version 1.0 not being signed off until 17/4/97. Since then it has been updated, version 2.0(24/2/98) being agreed, subject to minor caveats, on 6/4/98.

The Fraud Risk Management Service is defined by three key documents (see section 2.3):

- Fraud Risk Management Service Design [14]. Version 3.0 (23/4/97) was agreed (3/7/97) after about 18 months of discussion.
- FRMS System Requirements Specification [15], is an internal document.
- Extended Verification Process Requirement [16]. Version 2.0 (8/4/98) is subject to a Change Control Note, and has evolved after extensive discussion of rule based EVP.

2.2.2.2 Design and Development

Architecture

Every element of the technical architecture from Data Centre hardware, operating systems and networks to individual workstations is capable of enforcing security and the entire technical environment is used to enforce the security of the Horizon solution.

Design

Pathways Technical Design Authorities devise secure solutions to support the identification, authentication, access controls, audit and cryptography necessary to safeguard the integrity and confidentiality of the data held in the system. Their High Level Designs are created with direct reference to the security documentation set.

Development

All software development is bound by the security documentation set which specifies the standards for identification and authentication, and the roles and functionality allowed for each user. Developers write their lower level specifications from High Level Design Specifications to ensure that consistent application of security standards is achieved during the development lifecycle.

Where development is undertaken on Pathways behalf by a third party, exactly the same security standards apply. In all cases, conformance to requirements is assured during the testing process.

2.2.2.3 Testing

A dedicated 'Secure Test' team has been appointed and operates from a dedicated facility in Bracknell. The team is made up of ICL staff and Consultants who represent the interests of the two sponsor organisations. In this way the scope and results of security tests are visible to all relevant parties.

FUJ00152138

High Level Test Plans and Low Level Test Specifications map directly onto the security requirements and are designed to ensure that the identification, authentication, access controls, audit and cryptography described in the security documentation set are present, complete and accurate. The complete approach is described in the Testing & Integration Strategy [19].

2.2.2.4 Implementation

Pathway Implementation Team are responsible for the configuration, building and installation of all hardware in the Pathway solution except networks which are managed by another division of ICL (CFM). Configuration scripts are created to ensure that the identification, authentication, access controls, audit and security functionality described in the security documentation set are implemented.

Many sub-contractors are employed in the distribution and installation of Horizon equipment within the POCL estate. The Pathway Security function with the Horizon Service Management ensure that all staff requiring access to POCL outlets are stringently vetted before issuing an identity card which is required to gain access. Pathway administer the database of authorised staff which controls all aspects of the identity cards.

2.2.2.5 Operation

Pathway has established an infrastructure to minimise and control liabilities to itself and its suppliers, the DSS and POCL. This infrastructure enables Pathway to protect the integrity, availability and confidentiality of information used by the services. This includes making adequate provision for:

- Business Continuity, including resilience and recovery
- Audit,
- Compliance,
- Security Management
- Fraud Risk Management.

In the Security Policy, Pathway states its commitment to ensuring that it encompasses the very best commercial practices for security. Pathway's aim is to be compliant with BS7799, A Code of Practice for Information Security Management.

The manual operation of the Pathway systems is provided by ICL CFM as a managed service. Again, the hardware and networks for which they have responsibility are built and configured strictly in accordance with the security policies and functional specifications. A programme of security audits enables Pathway and sponsors representatives to satisfy themselves that technical, management and operational processes are in place and functioning correctly. All operational sites were visited prior to Release 1c authorisation, and all sites are scheduled to be visited at least once more during 1998 (prior to New Release 2).

A dedicated team of Pathway Customer Service Managers ensure that those third parties who operate managed service on Pathways behalf do so within the limits imposed by Pathway security policies.

FUJ00152138

The Pathway Fraud and Security functions have contributed to the ICL Peritas training programme to ensure that fundamental security messages are included in all training events for users of the Horizon system. Work is in progress to initiate a programme to ensure that counter staff remain informed of their responsibilities for fraud prevention and security awareness.

2.2.3 Post Award of Contract - Resilience and Recovery

2.2.3.1 Definition of Solution

The Pathway solution is defined in the Technical Environment Description [20]
and the overall strategy is documented in the Resilience and Recovery Strategy [21].

2.2.3.2 Architecture

The Pathway architecture is based on the principal of providing a totally resilient solution based on dual site implementation with every platform duplicated at each site. The Data Centres are connected by resilient high bandwidth communications links which are used to support the replication of all critical data between sites.

2.2.3.3 Design and Development

High Level Designs exploit the resilience within the architecture. Applications are designed to produce event messages for exception conditions, these events are reported to the System Management software which then in turn alerts the Support Centre. Where recovery time is critical then automatic procedures have been developed that detect failures, perform recovery scripts and alerts operations staff that a failure has occurred.

2.2.3.4 Testing

The testing of all aspects of resilience and recovery are covered in the Technical Integrity and Networking High Level Test Plan [22]. Testing covers all Data Centre platforms, remote platforms, counter platforms and communications links. Full System Management is enabled to test correct reporting of events.

A scaled down version the target live configuration has been built with EMC disks to enable the testing of fail over after host failure and complete Data Centre failure.

2.2.3.5 Operation

A number of operational manuals are being produced to cover the operational recovery/failover processes which will be employed in NR2. ICL Outsourcing (formerly CFM) are the major (but not the only providers) of this documentation. They will be produced through analysis of the individual recovery/failover design documents produced and by involvement in the testing process. This includes Bootle/Wigan site failure failure of supplier sites eg DLR, HSHD.

The above consider the technical aspects of failover and recovery. Another aspect which is being addressed is business continuity ie when a specific unit

FUJ00152138

fails, what is the effect this has on the service (if any) and what specific actions have to be carried out. This will be presented as the Contingency Map, and the approach is being discussed with the Authorities.

In addition, plans for Disaster Recovery are being produced, which address the actions required to cope with and recover form a major incident to the non-operational areas of the business for example loss of an administration site (eg Feltham), terrorist threat or major fraud.

2.3 Security Document Structure

There is a set of four documents which describes the security infrastructure and functionality and on which the detailed solution design is based. These are:

- Pathway Security Policy. The purpose of this document is to lay the foundation that enables Pathway to protect the integrity, availability and confidentiality of all assets associated with the services. It also enables Pathway to comply with legislative and commercial requirements. Its structure is based on the recommendations of BS7799.
- Security Functional Specification. This document defines the security functionality that will be incorporated into the operational ICL Pathway system. It is primarily concerned with the technical features rather than the surrounding management or operational controls.
- Access Control Policy. This document defines the policy for controlling access to resources in the operational ICL Pathway system. Effective control depends on having a clear definition of the roles and responsibilities of all personnel who need some form of access to the system. It defines the operational, management and support roles required in the Pathway system, and the main functions which people in those roles carry out. It then defines how the security functionality described in the Security Functional Specification will be used to enforce the required controls in the Pathway environment.
- Security Management Procedures [23]. The ICL Pathway Security Management Procedures are for use as a reference document by managers and employees who are responsible for initiating, implementing and maintaining information security within ICL Pathway. They are based upon British Standard BS7799, “A code of Practice for Information Security Management.”

In addition, three documents describe the FRM and EVP high level solution on which detailed design was based:

- Fraud Risk Management Service Design [14], describes the ICL Pathway Fraud Risk Management Service including: Service functionality, availability and Contracting Authorities requirements.
- FRMS System Requirements Specification [15] details the functional specification of the Fraud Case database.
- Extended Verification Process Requirement [16] describes the EVP requirement for the ICL Pathway solution including the definitions of class

FUJ00152138

of Customer and Transaction type upon which EVP may be invoked. The document also outlines the method by which the Contracting Authorities inform ICL Pathway of the class of Customer or Transaction type on which they require the EVP process to be carried out.

2.4 Security Acceptance

This is achieved by a number of test types as described in the Security Acceptance Test Specification [7], which refers directly back to individual requirements. This is currently under review. The acceptance methods include physical tests, document reviews and site visits.

2.5 Independent Evaluation

Two independent security reviews of the system have been carried out by Admiral Management Services Limited:

- Release 1c, September 1997 [17]. This consisted of an examination of the documentation, supplemented by discussions with Pathway staff. The objectives were to compare Horizon with current best practice in financial sector and government systems of comparable size. It concluded that 'We have no reasons to doubt that the Horizon development is comparable to current best practice', with some reservations regarding technical design and implementation activities. These have since been addressed.
- Penetration Testing, March 1998 [18]. The objectives of this review were to identify the most vulnerable areas of the security architecture and to recommend how best to employ penetration testing resources. It concluded that 'No vulnerabilities with a 'high' potential likelihood of exploitation have been found'. It recommended a series of penetration test scenarios, which are currently being impacted for Release 2 / 2+.

3 System Security Components

3.1 Data Security

Appropriate security measures have been designed in to ensure confidentiality, integrity and availability of data, whether in transit or in storage. A number of approaches have been used to tackle the identified threats to the links, Customer requirements and Pathway's internal exposure.

3.1.1 Security of data on individual communications links

This involves cryptographic protection on eg:

- CAPS links; using Red Pike encrypted secure hash initially, subsequently moving to hardware encryption.
- CMS links for card production data and PUN information to De La Rue; encryption using Red Pike algorithm.
- POCL TIP link; integrity of data will be protected in the same way as

FUJ00152138

CAPS; AP records will be digitally signed to provide end-to-end integrity protection.

- HSH Help Desk and System Management Workstations; integrity protection and one-time passwords; in particular all remote operational access require encrypted links and one-time passcode generators eg CFM Belfast.
- Post Office ISDN/PSTN/GSM links; CHAP initial connection authentication, supplemented by CLI authentication of the Post Offices to the ICL Pathway campus. No link encryption can be provided.
- Post Office LAN's; no link level protection. Some exchanged data is be protected using Red Pike and Escher native CRC's.

3.1.2 Message protection

In addition, protection is provided by the encryption of individual messages from creation to use (end to end). All message protection will be performed using DSA. Standard public key technology will be used.

- BES payment authorisations are digitally signed on leaving the PMS/CMS machine. Signatures are verified prior to use by the BES application in individual workstations at Post Offices.
- AP will be signed at the Post Office for ultimate verification by a receiving agent at the POCL TIP site.

3.1.3 Filestore encryption in Post Offices

There is a threat to confidentiality of data stored on hard disks at the counter, resulting from theft of PC's. Red Pike is used to protect this information and the filestore is automatically encrypted at disk access level. The workstations do not have operable floppy disk drives.

3.1.4 Key generation, distribution and management

The use of cryptography requires that Keys are generated, distributed securely to relevant sites, and renewed regularly. Relevant procedures to manage this are being developed. This applies in particular at the Post Offices, where a number of keys are required (eg filestore encryption, communications, AP signature).

3.2 Access Control

3.2.1 Logical access control.

To provide effective control of system resources, an Access Control Policy has been defined and implemented. This identifies all roles authorised to access any part of the system and the access rights to be permitted. Users are associated with one or more roles so that persons are individually accountable for their actions. It includes access to files, directories and databases. Roles include:

- Operational eg BA, PAS/CMS Help Desk, De La Rue, Postmaster and Counter Clerks

FUJ00152138

- Systems Management eg Manager (CFM/Sorbus), Database Administrator (CFM/Oracle), Network Manager (CFM) and Encryption Key Custodians (Pathway and CFM)
- Support Roles eg Manager, Help Desk and Installation Engineer

3.2.2 Identification and authentication

Mechanisms are required to ensure that all users are uniquely identified, with only authorised users being granted access to the system. Identification is based on a combination of what the user knows (eg password) and what the user possesses (eg smart card). Authentication is concerned with establishing the validity of the user's claimed identity; eg human users will be allowed a predetermined number of attempts to logon, failure being recorded and alarm messages being raised. Tokens will be used when protection provided by passwords alone is not considered to be sufficient. Identification and Authentication includes the following users:

- Logon at Post Offices (Postmasters and Counter Clerks) uses Riposte desktop facilities.
- Oracle is used to authenticate all database users.
- Help desk users are named individuals in a user group associated with a database role, permitted to access the database by running an application.
- Mechanisms are provided for authentication of DSS/BA and POCL staff.

3.2.3 Physical access control

This is tightly defined for all aspects of the system, and restricted to staff (both Pathway and subcontractor) on a strictly need to access basis. Physical security audits are conducted regularly at relevant sites that include for example:

- Central sites (Wigan & Bootle)
- Feltham
- Support sites (CFM Belfast, Sorbus, Oracle)
- De La Rue (Tewkesbury)

3.3 Audit and Alarms

Audit mechanisms are included to monitor and detect events that might threaten the security of the Pathway services or any service(s) to which it is connected. Regular analysis of audit trails is essential to facilitate the identification and investigation of security breaches.

Alarm mechanisms alert security personnel of the occurrence of security violations and will be used to trigger prompt investigation and remedial action in order to minimise the impact of any security breach.

Auditable events include:

- authentication actions,

FUJ00152138

- exception conditions,
- system start-up,
- change of user rights,
- write access to selected files,
- system management activities

Audit and alarm facilities use a combination of application level transaction logs and operating system audit logs:

- Riposte for logging of all transactions
- Patrol to monitor all Sequent systems and Oracle applications
- Oracle database for CMS and PAS
- Windows NT

3.4 Technical Administration of Security

Maintaining the integrity of the services and software components is also an essential part of the Pathway security. Systems management includes:

- Cryptographic Key Management - using CESG approved bespoke Crypto applications
- 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.

3.5 Security Processes and Procedures

3.5.1 Responsibilities for Security

Figure 1 illustrates the security organisation used within Pathway and the activities subcontracted to Girobank. Senior management is supported by experienced specialists and technical staff with specific expertise in the areas of IT, security, fraud prevention and risk management.

FUJ00152138

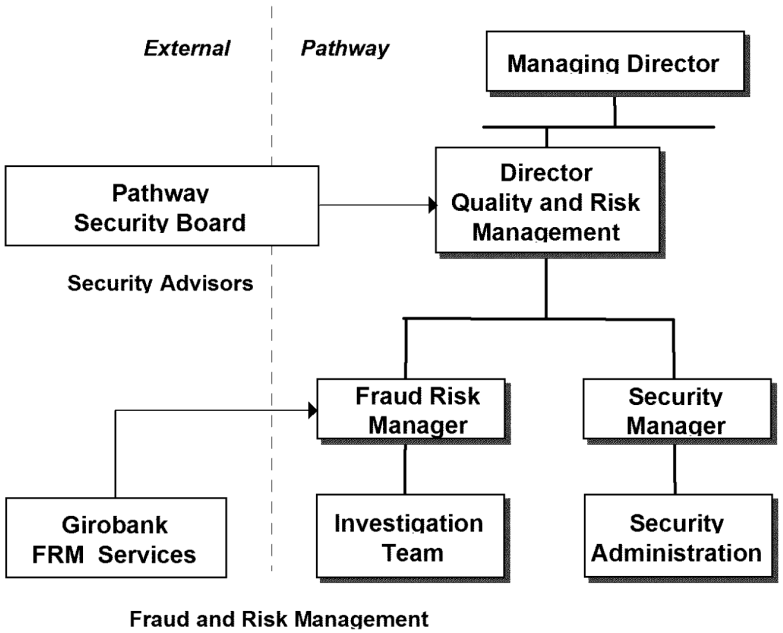

Figure 1 Pathway's Security Management Structure

3.5.2 Security processes

Processes have been developed, within Pathway, with BA/DSS and subcontractors, which encompass:

- Incident reporting, of potential security breaches in the systems either raised through system alarms or by human users
- Investigation of potential security breaches including co-operation with BA and POCL to identify liability
- Legislation compliance is monitored on an ongoing basis, including in particular Data Protection Act (1984) and Computer Misuse Act (1990). Pathway also complies with appropriate sections of the Police and Criminal Evidence Act.
- Pathway and subcontractor staff security. All Pathway staff are subject to a security vetting process that includes id, reference and credit checks and criminal record self declaration. All subcontractors are requested to conduct equivalent staff checks.

3.5.3 Fraud Risk Management

The Fraud Risk Management Service (FRMS) deals with the identification, monitoring and management of all fraud associated with / relevant to the ICL Pathway system and service via appropriate and effective controls (technical, managerial, procedural and personnel). Additionally FRMS provides information to support the investigation of individual fraudulent Benefit encashment transactions when informed that an investigation is in progress.

The FRMS comprises three core elements:

- A management information system, to analyse trends, fraud losses and to profile data patterns. This is part of MIS.

FUJ00152138

- A fraud monitoring system, to profile abnormal or irregular activity and identify potential or actual fraud incidents.
- Organisation, infrastructure and procedures to operate the service effectively and provide support for Contracting Authorities fraud control.

The FRMS incorporates a database that has the following functionality:

- Transaction data identified as representing real or suspected fraud is copied from the Data Warehouse to the Fraud Case Management System (FCMS).
- It accesses and retrieves information relating to actual and suspected fraud, identified by the Contracting Authorities.
- When investigations into actual and suspected fraud have been completed, flags attached to these transactions are altered to allocate the transaction to a loss category. This system allows full accounting, fraud analysis and assists in the determination of liability.
- It accesses and retrieves additional data required to support Fraud Risk Management from other ICL Pathway systems.
- It provides for ad hoc trawls of the FCMS to monitor emerging trends and patterns of criminal activity.
- It provides for the production of a range of standard and exception reports.

3.5.4 Extended Verification

This is a key process as additional authentication of benefit claimants. The majority of Benefit Encashment Transactions will be genuine and therefore the risk involved in simple identity verification is small. However, some types of transactions carry a higher level of risk and therefore require a more robust verification procedure. The Extended Verification Process is designed to deal with these transaction types. The process is applied in two forms:

- Basic EVP - under which the additional verification is applied, at all outlets, to a generic set of transaction types considered to be either critical to the integrity of the service or carrying a higher risk of fraud, to Payment Card issue and activation, and transactions in fallback.
- Rule-Based EVP - under which the process is targeted to, at the BA's discretion, to those transaction profiles identified as higher risk. This provides for targeting by transaction type, customer type by benefit.

In combination with the objective to minimise fraud risk EVP is also used to transfer fraud risk from the contracting authorities to ICL Pathway in return for an increased transaction charge.

EVP is based on a multiple choice question and answer process at the Post Office. Questions are formulated from personal data provided from BA via CAPS. The system only allows the transaction to proceed on satisfactory completion of EVP.

3.5.5 Business Continuity and Disaster Recovery

The system is designed to be inherently robust:

FUJ00152138

- NT Platform failure : - All platforms are designed to be resilient with multiple network routes and back up systems.
- TMS Hosts :- Copies of the TMS journal are kept at each site and are reliably synchronised to ensure that there is always a consistent view of the data at each Data Centre.
- Networks: - There are multiple network routes to all remote sites that need to communicate with the Pathway Data Centre. The network is designed in such a way that failure of routers and links are reported to Network support staff and any connection is automatically re-routed without operator intervention.
- Sequent Host Failure:- All possible single points of failure have been removed. All data is mirrored both locally and remotely using EMC disk technology. Disk updates are synchronously copied to the remote disk array giving a guarantee that all data is secured before committing any transactions.
- Site Failure:- Because all platforms are duplicated at both sites and copies of the data are replicated it is possible to recover from a site failure without the loss of any transaction data. The architecture is sized to ensure that there is sufficient capacity at a single site to run the complete workload.
- Counter Platforms :- The Riposte message store is reliably replicated to all PCs in multi counter Outlets. Failed base units are replaced by new systems and the message store is copied from one of its neighbours. At single counter Outlets there is a second exchangeable disk that “mirrors” the message store. This disk is used to recover the system in the event of a unrecoverable error on the hard disk.
- The Gateway PC in the Outlets will automatically retry the communications link using a different target router if the normal route is not available. If the second attempt fails then it will try a third route to a router at the alternative Data Centre.

Business continuity processes are being developed to contain the potential SLA penalties for performance shortfall in the eventuality of partial system breakdown, and provide for recovery actions.

A Disaster Recovery management structure and processes (including media communications) are being developed for events that could potentially significantly impact Pathway’s survival, eg:

- Feltham non-availability; a stand-by site has been established
- Significant security breach or major fraud event; communication with Contracting Authorities, investigation and impact analysis.
- Terrorist threat; how to deal with, communications.

4 Phasing of the Security Solution

The implementation of the security solution has involved phasing by release according to:

- business functionality, and
- risks associated with the nature of the release

FUJ00152138

4.1 Release R1c

The components included in the Release 1c BPS and OBCS end-to-end systems, as identified in the Release Contents Description [24], are:

- CAPS Access Service Software running in a secure user partition on the BA VME environment at Livingstone ACC, protected by a 'firewall' system;
- CAPS Link protection utilising Red Pike encrypted secure hash produced using SHA implemented in software at each end of the link;
- OBCS Access Service Software running in a secure user partition on the BA VME environment at Washington ACC;
- 2 Mbit communications connections between the Livingstone and Washington ACCs and the Pathway Release 1c host system running at the Wigan Data;
- PAS/CMS , OBCS and Reference Data Oracle Databases running on a Sequent processor under the control of the Dynix operating system;
- Dynix and Oracle RDBMS standard access control facilities;
- central layer of the TMS message store (correspondence server) running Riposte software under the Windows NT 4.0 operating system and utilising the Riposte and NT 4.0 security and access control functionality and the Riposte secure message replication facilities;
- entropy servers running under NT4.0 and utilising NT4.0 security and access control functionality;
- communications gateway PCs for access to the Card Management facilities operated by De La Rue via Red-Pike encrypted ISDN links, running under NT4.0 and utilising NT4.0 security and access control functionality;
- TMS 'Agent' software running on an NT 4.0 platform and utilising NT4.0 security and access control functionality;
- ISDN communications links connecting the central TMS message store with the local 'gateway' PC located at each Post Office outlet, utilising CISCO routers configured using CISCO Works and implementing Challenge Handshake Authentication Protocol (CHAP) and Call Line Identity Protocol (CLIP);
- ISDN Terminal Adaptors at each Post Office Outlet 'gateway' PC, utilising EICON software to implement CHAP and CLIP;
- Post Office outlet PCs ('gateway' and non-'gateway') running Riposte and NT4.0 and utilising the Riposte (including implementation of 'roles') and NT 4.0 security and access control functionality and the Riposte secure message replication facilities;
- filestore encryption on the Post Office outlet PCs;
- smart token authentication of the PostMaster logon, including authentication to 'unlock' the filestore encryption.

The exclusions (against the full solution defined in the SFS and ACP) were

FUJ00152138

also originally identified and described in the Release Contents Description.

In addition, as a result of testing, a number of additional, more detailed exclusions were identified. Mitigation actions were identified by Pathway to minimise the associated risks [17]. These were discussed in detail with the PDA and agreed, before Release Authorisation was given. During Release 1c there have been no fraud incidents.

4.2 Release NR2

Developments that are on target for Release 2 include:

- A common NT Secure build including bespoke developments which restrict the attributes of privileged NT users.
- Robust NT user and resource domain definitions to further control access;
- A secure Sequent build to provide strong access controls and a comprehensive audit capability, and bespoke developments to ensure quality user identification and authentication checks.
- SecurID - one time passcode generators to enhance access controls for remote users with authorised access.
- Security Administration functions

These developments will address the majority of the exclusions in Release 1c.

The exclusions for Release 2 are described in the Release Contents Description [18], which has not yet been signed off by the Authorities. The major items include;

- Signing of Automated Payments
- Full Key Management System
- Some authentication and password control mechanisms

4.3 Release NR2+

It is intended that the full security functionality will be included in this release.