FUJ00119593

Document Title:	Pathway Release Contents Description
Document Type:	Definition Document
Abstract:	This document defines the functional content of Release 1c BPS, OBCS and EPOSS Services in relation to the development baseline document Service Architecture Design Documentation Version 2.0
Distribution:	PDA Members Pathway Management Team Pathway Library
Document Status:	Issued for Approval
Document Predecessor:	None
Associated Documents:	Service Architecture Design Documentation Version 2.0 Security Functional Specification (SFS) version 2.0.
Author:	Steve Warwick

Signatories:
Martyn Bennett
Dick Long
John Dicks
Barrie Vaughan
Alan Ward
Barrie Davies
Martin Riddell
Paul Curley

FUJ00119593

Document Title:	Pathway Release Contents Description
Document Type:	Definition Document
Abstract:	This document defines the functional content of Release 1c BPS and OBCS Services in relation to the development baseline document Service Architecture Design Documentation Version 2.0
Distribution:	PDA Members Pathway Management Team Pathway Library
Document Status:	Issued for Approval
Document Predecessor:	None
Associated Documents:	Service Architecture Design Documentation Version 2.0 Security Functional Specification (SFS) version 2.0.
Author:	Steve Warwick

Signatories:

For ICL Pathway Ltd:

For PDA:

FUJ00119593

1. DOCUMENT CONTROL

1.1 CONTENTS

FUJ00119593

FUJ00119593

1.2 DOCUMENT HISTORY

Version	Date	Reason
0.1	17/2/97	First Draft for Pathway and PDA discussion
0.2	18/2/97	Updated with comments received following initial review within Pathway.
0.3	18/2/97	Updated following Pathway Review on 18/2/97
0.4	19/2/97	Updated following further review on 19/2/97, in particular revisions to the FRM and BPS MIS section.
1.0	19/2/97	First formal issue following review within Pathway
1.1	23/4/97	Revised following comments from PDA and including agreed statements on the implementation of Access Control features
1.2	2/5/97	Updated to include comments received from PDA Product Management.
1.3	19/5/97	Updated for circulation to PDA and Pathway for comment, changes principally in the area of access control
1.4	21/5/97	Updated following cross-checks with Release1e and Release 2 RCDs. Description associated with SADD reference 4.1.1.10 clarified, comment at SADD reference 3.1.3.11.1.1 removed.
1.5	13/6/97	Updated following receipt of comments from PDA Product Management and further internal comment from Pathway in the areas of BPS and Security.
2.0	20/6/97	Updated following further comment from the PDA and issued for authorisation
3.0	27/6/97	Minor change to include reference to ABED at the request of PDA Product Management
4.0	22/9/97	Changes to incorporate the caveats expressed in the PDA acceptance letter for version 3.0 (including the addition of a Technical Infrastructure Annex) plus clarification of the Security Access controls as agreed in the document "Security Exclusions from Release 1c" (RS/RES/002 V3.0 dated 5.9.97)

1.3 CHANGES FORECAST

None.

FUJ00119593

1.4 ABBREVIATIONS USED

The terms and abbreviations used in this document are those defined in the AUTHORITIES Agreement (Schedule A01) and in the SADD (Version 2).

1.5 CHANGES HISTORY

Changes as documented in Document History, once baselined any changes will be maintained using side bars.

FUJ00119593

2. INTRODUCTION

In response to the request to consider a phased release of the Horizon system which would include a release of the system which provides only the Benefit Payment Service (BPS) and Order Book Control Service (OBCS), this document is intended to provide a definition of the functional contents believed by ICL Pathway as necessary to support such a release.

In the course of examining the minimum functional requirements of this release it has been found necessary to extend the functional scope beyond the BPS and OBCS services to include that minimal element of the EPOSS service necessary to support the primary services. This is necessary due to the integrated nature of the desktop components of the service and the consequential interdependency between the products.

3. SCOPE

This document is limited to the functional services required to support a release of the system which offers only the BPS and OBCS services at the counter, with the supporting infrastructure necessary to receive and process the encashment of Payment Authorisations and Control Notice files issued by the Benefits Agency (BA) and to return transaction files to the BA and to POCL via the ABED interface.

FUJ00119593

4. RELEASE 1C CONTENTS

4.1 INTRODUCTION

In order to achieve a rapid understanding of the functional content included in the release, the tables in the following sections describe the functionality in two different ways. In the case of the Service Infrastructure, POCL Services, Security, Audit, BPS and OBCS, the description is represented as an exception list against the baseline functionality contained in the Services Architecture and Design Document (SADD). For EPOSS functionality, due to the restricted functions provided, the description is expressed as a positive statement of the functions from the SADD which are to be included. The baseline is the SADD (version 2) and the SFS Version 2.0; the section headings from these two documents have been used to structure the Release 1c Content paragraphs which follow this introduction. It should be noted that this approach introduces a degree of necessary duplication between the paragraph sections. The references in the descriptions are to the SADD or the SFS.

> The Related Agreements, the SADD and the SFS make reference to documents which form a necessary part of the functional baseline. These documents and their status at the time that the Release 1c Contents Definition was produced are listed at Annex 1 to this document. Not all of the documents have been agreed with the AUTHORITIES at the time that the document was prepared and in some cases ICL Pathway has had to develop the system using draft documents. It can not be assumed that when these documents are agreed by the AUTHORITIES that the functionality so defined can be included within Release 1c.

4.2 PFI SERVICE ARCHITECTURE

Except where specified below, all the requirements of the PFI Service Architecture will be met in Release 1c. It should be noted that at Release 1c only one of the Pathway Data Centres will be operational and that this data centre will communicate to 2 BA ACCs - Livingstone for the CAPS service and Washington for the OBCS service.

FUJ00119593

4.2.1 PFI SERVICE FUNCTIONALITY

SADD 2 Reference	Description
2.1 & 2.2 PFI Service Architecture	These sections contain references to the POCL Inventory Management. Detailed requirements for this facility have been withdrawn by the Authorities.
2.4.1 Contingency (see also 3.1.2.5.5)	CAPS Contingency payments will be available in Release 1c by generating payments (the last authorised amount) for all beneficiaries whose next payment due date matches the required date. A file of contingency payments will be sent to CAPS for reconciliation.
2.5 Security	The Security Functional Specification is defined in Section 4.10
2.5.2 Fraud Risk Management	The Fraud Risk Management Service Design Specification is defined in Section 4.11

FUJ00119593

4.3 CARD MANAGEMENT SERVICES

4.3.1 CMS FUNCTIONALITY

SADD 2 Reference	Description
3.1.1.3.2 Maintain Cardholder Details	The automatic issue of a bilingual card based on the card holder's location is dependent on knowing the post code of the cardholder. An algorithm has been implemented for Release 1c giving a close approximation of the card holder to England/Wales. But a better solution requiring data cleansing with DSS/CAPS is under discussion for Release 2.0
3.1.1.3.3 Maintain Card Status	Recording of the Reason for Card Impounds is not implemented at Release 1c
3.1.1.5 The PUN -	On production of the second reminder PUN, a process needs to be defined to get the details sent to DSS via the Horizon Customer Services Department.
3.1.1.6	Cards with an incorrectly calculated LUHN check digit (as issued for use in IGL) will continue to be accepted during Release 1c.
3.1.1.6.1 Customer Unable to Collect Card	Extension of the period of card validity, as oppose to the period during which the card can be collected, is not supported at Release 1c since cards will not expire for at least three years.
3.1.1.6.2 Replacement of existing card on card expiry-	For Release 1c, the card details which will advise the clerk of the presence of the new card after the old card has been swiped will not be available. This facility will not be required until 1998.
3.1.1.7.1 Inhibit card on failure to collect	The route by which CMS will report non-collection to DSS needs to be defined by DSS/POCL
3.1.1.8.4, 3.1.1.8.4.1	When the National Sensitivity indicator is present on a record, personal details are not displayed on the screen unless the user has the appropriate level of access privilege.

FUJ00119593

SADD 2 Reference	Description
3.1.1.8.4.7, 3.1.1.8.4.8 Emergency Order of Temporary Tokens	The implementation of Temporary Token is awaiting CAPS interface support and agreement of the ICL Pathway document "Temporary Token Overview and Usage".
3.1.1.8.5.2	A Card batch can be suspended, cancelled or re-ordered even when booked in. These facilities are to be restricted to Card batches in production or in dispatch in Release 2.
3.1.1.9 Temporary Token Production and Issue	The whole of this section refers to the implementation of Temporary Tokens. This is awaiting CAPS interface support. All other references to Temporary tokens are subject to the same limitation.

FUJ00119593

4.4 PAYMENT AUTHORISATION SERVICE

4.4.1 PAS FUNCTIONALITY

SADD 2 Reference	Description
3.1.2.4 Amendment to Cardholders Details. 3.1.2.10.4 Notification of change of address.	The automatic issue of a bilingual card based on the card holder's location is dependent on knowing the post code of the cardholder. An algorithm has been implemented for Release 1c giving a close approximation of the card holder to England/Wales. But a better solution requiring data cleansing with DSS/CAPS is under discussion for Release 2.0
3.1.2.4.2	The Appointee role will not be supported in Release 1c.
3.1.2.5.4 Urgent payments -	Urgent payment facility within PAS is not included as it requires the CAPS on-link which is currently not supported by CAPS. All urgent payments at Release 1c will be via Green Girocheque
3.1.2.5.4.2	The Appointee role will not be supported in Release 1c.
3.1.2.5.5 Contingency payment	CAPS Contingency payments will be available in Release 1c by generating payments (the last authorised amount) for all beneficiaries whose next payment due date matches the required date. A file of contingency payments will be sent to CAPS for reconciliation.
3.1.2.6.1 Encashment Infringement	The Geographical Restriction Indicator (GRI) is not implemented at Release 1c. At Release 1c potential infringements are prevented by the system but not reported.
3.1.2.9 Enquiry on Payment Details	The CAPS on-line interface is not currently supported by CAPS.
3.1.2.11.3 DSS Viewpoint	When the National Sensitivity indicator is present on a record, personal details are not displayed on the screen unless the user has the appropriate level of access privilege.

FUJ00119593

SADD 2 Reference	Description
3.1.2.11.3.2 CAPS/ CAPS access Facility not available	The on-line interface is not supported by CAPS at Release 1c
3.1.2.11.4.4	Change of Nominated Post Office via the Help Desk is not supported at Release 1c

FUJ00119593

4.5 COMMON CMS AND PAS SERVICE ELEMENTS

4.5.1 COMMON CMS AND PAS FUNCTIONALITY

SADD 2 Reference	Description
3.1.3.5 Maintain Post Office references..	Pathway's proposals for Release 1c and subsequent releases are contained in "Post Office not available for Benefit Encashment" Version 6.
3.1.3.7.1 Beneficiaries	There is no facility to archive and delete entries that notify details of NINOs designated no longer of interest after 90 days. This facility will be incorporated into Release 2.
3.1.3.8 DSS Management Information	DSS management Information is addressed in section 4.11 below.
3.1.3.8.1.7	The Appointee role will not be supported in Release 1c.
3.1.3.9.1 CAPS access system -	The CAPS on-line interface is not currently supported by CAPS
3.1.3.11.1.1 Card-related reconciliation	Card related reconciliations - the facility to communicate these reports is not yet defined by DSS/POCL.
3.1.3.11.1.2 Card-related reconciliation	The implementation of Temporary Token is awaiting CAPS interface support in a future CAPS Release.

FUJ00119593

4.6 BENEFIT ENCASHMENT SERVICE

4.6.1 BES FUNCTIONALITY

SADD 2 Reference	Description
4.1.1.4.2 Steady State Provision	At Release 1c, after the Card Activation the clerk will have to swipe the card again to access Benefit Encashment screen if payments are due
4.1.1.4.4 Collection of Card by Agent	At Release 1c Housebound PUN holders with no alternate payee will contact the CMS Help Desk to record their inability to collect their card. Procedures will be put in place to allow benefit collection via Green Girocheque.
4.1.1.5 Extended Verification Procedure	Extended Verification Process for Release 1c is defined in Section 4.6.3 below.
4.1.1.6 Impoundment of card/Temporary Token	Recording of the reason for Impounding Temporary Tokens is not implemented at Release 1c.
4.1.1.6.3	The system will only generate the receipt for impounded PUN or Card on request.
4.1.1.7.2 Steady state service provision-	For Release 1c, the functionality of the screens that remind the clerk of the location to which reports and associated items should be forwarded in connection with impounded PUNs, cards and temporary tokens is not available.
4.1.1.8.2 Steady state service provision-	Payment Description code length awaiting resolution by DSS of request of 22 character description for printing on receipt. The payment description code length will be defined as 12 for Release 1c.
4.1.1.8.2, 4.1.1.9.2, 4.1.1.11.2	Prompt to clerk does not include :- "Pay customer, return and issue bottom copy of receipt" "Place receipt in drawer" These have been omitted for performance reasons and

FUJ00119593

SADD 2 Reference	Description
	because there is no room on the screen. Help will be provided instead.
4.1.1.9 Foreign Encashment	Point of note :- There is no support for the exclusion of Social Fund Payments within the restrictions relating to Foreign Encashments as in accordance of Requirement 770. Social Fund Payments are not intended to be one of the benefits payable at Release 1c
4.1.1.9.2 Foreign Encashment :- "Steady State Provision"	At Release 1c, if an attempt is made by a customer with a Restricted Post Office to make a foreign encashment a message will be displayed rather than a prompt to refer to nominated Post Office
4.1.1.10	At Release 1 Casual Agent encashments are not supported. Procedures will be put in place to allow collection via Green Girocheque.
4.1.1.11.2 Steady State Service provision .	Requirements and detailed procedures are to be agreed in connection with group permanent and signing agents and will not be in Release 1c.
4.1.1.14.2 Steady State Provision	At Release 1c, after Change of Nominated Post Office the clerk will have to re-swipe the card to access Payments Screen
4.1.1.14.2 Steady State Provision	At Release 1c, change of Nominated Post Office screen will not contain "message for the clerk, if applicable" as the source for additional messages has not been defined. The change of nominated Post Office does not take effect until the message notifying the change has been processed centrally and the payments associated with the card have then been re-directed to the new nominated office. In cases where the beneficiary wishes to encash at the new office but cannot due to having exceeded the allowable number of Foreign Encashments, a payment may be authorised via the Help Desk.

4.6.2 LIMITATIONS AGAINST FS VERSION 6.0 AND SADD2

SADD 2 Ref.	Description

FUJ00119593

4.1.1.13	This section refers to the production of Duplicate Receipts. This requirement has been withdrawn and is currently not scheduled for any Release

FUJ00119593

4.6.3 EXTENDED VERIFICATION PROCEDURES

Release 1c Functionality

The headings refer to the appropriate heading in the main body of the Extended Verification Process Requirement document ref. RS/SPE/0003.

INFORMATION REQUIREMENT

The following information will be used in Release 1c:

- First Name
- Day of Birth
- Month of Birth

QUESTION GENERATION

Questions will be randomly generated from the following information:

- First Name
- Day of Birth
- Month of Birth

NUMBER OF QUESTIONS AVAILABLE FOR USE AT THE COUNTER

- Three questions will be available for use at the counter.

NUMBER OF QUESTIONS USED AT THE COUNTER

Three questions will be used at the counter incorporating the following information:

- First Name
- Day of Birth
- Month of Birth

ANSWER GENERATION

Alternative answers will be generated for the following:

- First Name
- Day of Birth
- Month of Birth

GENUINE ANSWERS

This will be implemented in Release 1c.

ALTERNATIVE ANSWERS

FUJ00119593

This will be implemented in Release 1c subject to the data used i.e. First Name, Day of Birth, Month of Birth.

SEQUENCE OF QUESTION EVENTS

This will be implemented in Release 1c.

INFORMATION PROVIDED TO THE COUNTER CLERK

This will be implemented in Release 1c.

SCREEN FORMAT OF EVP - MULTIPLE CHOICE

This will be implemented in Release 1c.

CIRCUMSTANCES UNDER WHICH EVP INVOKED

EVP will be invoked only in the following circumstances:

- Card Issue
- Keyed Input of Card/PUN Details
- At the counter clerks discretion (with the exception of casual agent transactions and change of nominated Post Office)
- Foreign Encashment
- Change of Nominated Post Office in those instances where an outstanding payment record is present.

REPORTING

Reports available at Release 1c will include the following details by Post Office and Nationally:

- Number of transactions subject to EVP
- Number of transactions subject to EVP as a percentage of total transactions
- Number of transactions failing EVP.
- Number of transactions failing EVP as a percentage of total number of transactions subject to EVP

CONTRACTING AUTHORITIES RESPONSIBILITY

No criteria selection/targeting facility will be available in Release 1c.

FUJ00119593

4.7 ELECTRONIC POINT OF SALE SERVICE

The statements within this section identify only those elements of the EPOSS service which will be delivered for Release 1c

4.7.1 EPOSS FUNCTIONALITY - INCLUSIVE LIST

SADD 2 Reference	Description
4.1.3.1.3 & 4.1.3.1.4 Customer Sessions	This section relates to the implementation of customer sessions. In the context of Release 1c, customer sessions are supported for BES and OBCS transactions only. Transactions will appear on the Desktop transaction 'stack'. The stack is cleared by selection of the 'finish' option.
4.1.3.1.7 Transaction selection	The only desktop transactions to be provided will be to support user administration (see 4.10.4 below), BPS and the OBCS services.
4.1.3.1.2 Settlement	Settlement of transactions will be supported through the use of the 'Finish' option on the desktop. In Release 1c settlement will be assumed to be via 'Cash' and no options to select Method of Payment will be supported
4.1.3.1.16 Commit Transactions	Committal of transactions will be supported. Transactions will only be committed following selection of the 'Finish' option on the desktop
4.1.3.1.17 Start a new customer session	Fully supported
4.1.3.2 EPOSS Counter Transactions	Product reference data sufficient to support the EPOSS product items used for BES and Pension and Allowance transactions will be required. Reference data will also be required to support the menu hierarchy, menu buttons and the token definitions needed to support the BES payment cards and the BES and OBCS bar-code structures.
4.1.3.3.3 Access Control	The functions to support the creation of users, creation of passwords, allocation of roles and the maintenance of these items will be supported.

FUJ00119593

4.8 ORDER BOOK CONTROL SERVICE

With the exception of the item listed below, the functionality of OBCS for Release 1c will be as required in SADD Version 2.0.

SADD 2 Ref.	Description
4.1.4.1	There is no functionality to check the status of order book on re - direction. This is documented in the OBCS Business Processing Rules and will not be implemented (at any Release)
4.1.4.2.1	The functionality to provide an adhoc comparison of a complete BA Control Notice file against the Pathway Control Notice file, with discrepancies written to an exception report, is not supported at Release 1c
4.1.4.2.3.1.1	No 'Last Book' option is provided to terminate the 'Receipt' session. This was agreed during the Joint Working Team reviews of the product.
4.1.4.2.3.1.1 4.1.4.2.3.2.1 4.1.4.2.3.3.1	Reading of a valid Bar-code is indicated audibly. Scanning of an invalid bar-code is not signified in any way since the system has no definition against which it can match the scanned code. This feature has been reviewed and accepted during Joint Working.
4.1.6.2.1.3	This section of the SADD has not been implemented and is the subject of further clarification of the sponsors requirements. For Release 1c, a report facility is provided to enable the outlet to print a copy of the local Control Notice file. This printed list should be used to check for control notices against order books when the system is unavailable for use.

FUJ00119593

4.9 POCL SERVICES

With the exception of the item listed below, the POCL Services functionality for Release 1c will be as required in SADD Version 2.0.

SADD 2 Reference	Description
4.1.5.1.2, 4.1.6.4 Standard Configuration Details	The counter hardware configuration supports the use of Smart tokens at Release 1c but the APS functionality to exploit this facility is not supported at Release 1c.
4.1.5.4.2 Inventory Management	These sections contain reference to Inventory Management which is still to be defined by DSS/POCL and will not be part of Release 1c.
4.1.5.4.1 Transaction Information Processing	These sections describe the interface with TIP. No interface with TIP is supported within Release 1c. Support for the IGL ABED interface will be continued in Release 1c for BPS transactions.
4.1.5.1.7 Mobile Configurations	These sections refer to the use of mobile configurations. The peripherals attached to these systems are currently being specified. Mobile configurations are not supported at Release 1c.
4.1.6.2.1.1.1 & 4.1.6.2.1.1.2 Receipt of Batches of Cards into Post Office	Where receipt of cards at the Post Office have not been entered into the system (due to the Post Office being out of commission) then the Help desk cannot activate the card in order to access payment details for payment authorisation. Customers will have to contact DSS office for payment via Green Girocheque
4.1.6.12.2.1	Mobile Office configurations will not be supported at Release 1c.

FUJ00119593

4.10 SECURITY

With the exception of the items listed in the tables below (section 4.6.2 to 4.6.9 below), the Security functionality for Release 1c will be as required in SFS Version 2.0. The section headings from the SFS have been used to identify the Release 1c content paragraphs which have been excluded. Within the SFS extensive use is made of references to the Access Control Policy. Version 1.0 of the Access Control Policy (ACP) has been approved. Approval of this version of the ACP is caveated by the need to resolve a number of issues associated with particular sections of the document. For clarification, the outstanding issues relate to sections 3, 4, 5, 6 and 8 of the ACP..

4.10.1 INTRODUCTION

For the sake of clarity, the following is a list of the components included in the Release 1c BPS and OBCS end-to-end systems.

- 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 and OBCS 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;

FUJ00119593

- 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.

It is believed that the Contracting Authorities have some concerns that it may be possible for some penetration of the security features to take place during the lifetime of Release 1b. Whilst such an event is unlikely to pose any threat to the system during Release 1b, concern exists that this may undermine the integrity of the later releases where the security facilities would otherwise have prevented such events occurring. In recognition of the fact that the Release 1b security functionality falls short of the full set of security components defined in SFS Version 2.0 for the Steady State system, Pathway intend that the following steps be taken in moving the system from Release 1b to Release 1c where the security is increased:

- the Release 1b Oracle tables containing the Control Notice data, the central Customer Reference File and the Customer 'Nominated Office' File should be transferred to a new Oracle database at the Live Data Centres;
- the Release 1b correspondence server layer of the TMS (located at Feltham) should be archived;
- The Release 1b hardware platforms located in each outlet will be replaced by completely new Release 1c hardware delivered from the Pathway distribution centre and configured with Release 1c software;
- the central and local message stores will be re-populated with OBCS Control Notice data when Order Books are next presented at the counter in any particular office;

Migration of the IGL system to the Release 1c environment is to be dealt with in a separate migration document.

FUJ00119593

4.10.2 SECURITY COMPONENTS

The security components identified in Section 4 of the SFS will be provided at Release 1c.

4.10.3 IDENTIFICATION AND AUTHENTICATION

The identification and authentication components identified in Section 5 of the SFS which will not be provided at Release 1c are identified below.

Security Functional Specification	Description
5.1.1.2	• Mitigation: • The administration and control of user accounts on both Dynix and NT platforms is restricted to a single Security Manager role. • This exclusion only applies in those domains where professional, vetted staff operate the Pathway computer systems. Vetting is to Northern Ireland Civil Service standards, and CFM staff are currently undergoing M.o.D. vetting. • CFM operational documentation will be modified to state that it is forbidden for users to change their User Id. • Management procedures will be put in place to ensure that relevant members of staff are aware of the SFS requirement, and that disciplinary action is taken against any offender. • Any staff member guilty of deliberate contravention will be subject to severe disciplinary action. • All operational activity takes place in a physically secure environment. Physical security components of the Data Centres and support sites in Bootle, Wigan and Belfast will comply with agreed standards. • Pathway will create a 'Code of Practice' to embody the additional processes proposed for Release 1c. All affected members of staff will be required to sign an appropriate undertaking to abide by the Code of Practice and copies will be retained by the Pathway Security Manager. Please see associated mitigations in SFS Reference 6.1.2.1.
5.1.2.2	No restriction on the number of Logon attempts will be imposed at Release 1c, for OPS.
5.1.2.3	Failed logon attempts will not require to be reset for Release 1c, for OPS
5.1.2.5	Date and Time of User's last successful logon will not be displayed at Release 1c, for all NT domains
5.1.4	The use of tokens will not be introduced at Release 1c.

FUJ00119593

5.2.1.2	Mitigation • SFS already updated to read "All account information associated with Guest will be disabled, or where possible, removed entirely." • Configuration scripts already modified to flag the Guest account as disabled. • The CFM Security Manager will perform weekly independent checks to verify the status of the account on the NT Domain Controller(s). A check list, and record of this procedure, shall be maintained, and made available for inspection.
5.4.1.4	Authentication of Help Desk to Post Office counter staff. A manual process is to be agreed between Pathway and PDA.
5.5	Authentication of DSS/BA staff making telephone calls *No software based solution will be provided, however agreed manual procedures will be put in place*
5.6	Authentication of POCL staff making telephone calls *No software based solution will be provided, however agreed manual procedures will be put in place*

4.10.4 LOGICAL ACCESS CONTROL

The following logical access controls identified in SFS section 6 are not provided in Release 1c.

Security Functional Specification	Description
6.1.1	The facilities described in the Access Control Policy document are not fully implemented at Release 1c (see section 4.10 above)

FUJ00119593

Security Functional Specification	Description

6.1.2.1 and 6.4.1	Mitigation
	
	• In the absence of COSManager, ICL Pathway will apply the principle of least privilege within the constraints of the Dynix operating system.
	
	• This exclusion only applies in the CFM Belfast Data Centre; no interactive Dynix or NT accounts exist in Bootle or Wigan. Only monitoring accounts exist in Bootle & Wigan. There are two types of engineering activity undertaken: 'part swap' and 'machine rebuild'. Part swap requires no access as diagnostics are run by CFM. Machine rebuild occurs before Dynix is available. When Dynix becomes available, CFM staff in Belfast manage the loading of configuration / authentication files
	
	• All CFM staff providing operational support to the Pathway system are dedicated to the project i.e. they are not involved in work on any other CFM business.
	
	• The CFM Security Manager will allocate roles in accordance with the ACP, utilising the user account facilities available in Dynix where appropriate.
	
	• It is not possible to login directly as <root>. Dynix is configured to only allow <root> access at the console (which is in Wigan). Belfast users must login with their unique User Id and *su* to <root>. The *su* to <root> is logged, BMC Patrol will monitor the *sulog* and cause a Tivoli event to be notified if it detects the use of su.
	
	• Roles requiring access to the Dynix operating system will be divided into those with a legitimate <root> access requirement, and those with no <root> access requirements at all. In this way, <root> access will be restricted to the absolute minimum number of users necessary to maintain efficient operation of the system. For Release 1c that means two senior support staff plus the Security Manager.
	
	• Operational procedures will be introduced in addition to existing physical and personnel controls; these include but are not limited to:
	
	  • Two man working if <root> access is required during the operational day;
	
	  • <Root> access outside of the operational day is event driven and is only available to two members of staff on a rota basis;
	
	  • A paper audit log of all such access and reasons..
	
	• The Unix utility '*BOMverify*' will be scheduled to run at each shift change to highlight any changes in file characteristics. Output will be reviewed by the CFM Security Manager and exceptions escalated to the Pathway Security Manager for investigation. The BOMverify program compares the Bill of Materials (BOM) of the specified products to the actual status of each file listed in the BOM as it currently exists on the system. The information listed in the BOM includes: the mode (read, write, etc.), owner, group, size and checksum, and hard and symbolic link data. BOMverify will be run with the '-l' option. When this is specified, no attempts are made to correct inconsistent files. Inconsistencies are reported with the expected and

FUJ00119593

Security Functional Specification	Description
	actual file status. • The NT Admin privilege will be controlled in the same way as <root> (i.e. restricted to the absolute minimum number of users necessary to maintain efficient operation of the system). • The Pathway Security Manager will perform periodic physical audits to ensure the continued application of these mitigations. • The CFM Security Manager will be responsible for the allocation of roles in accordance with the ACP, utilising the NT privilege facilities where appropriate. • Passwords associated with <root> and Admin will be administered by the CFM Security Manager, whose responsibilities include changing the passwords regularly in step with the staff rota. • As part of the CFM Security Manager's weekly independent review of NT defaults, the presence of comprehensive event logs for the preceding seven days will be verified. • The secure 'bridge' area in Belfast is monitored by CCTV and video, as is the machine room. At Bootle and Wigan CCTV is proposed only for the machine room with monitoring in the 'bridge' area. Subject to budgetary approval, it is also proposed to 'cross monitor' the two bridge rooms between sites The card access system which provides an audit trail of entry and exit is mandated for all Pathway Data Centre sites. Existing procedures instruct staff not to allow tailgating. Associated NT functionality not available; PinICL 3774. User assigned extra privilege if PDC is down. PinICL 4890., 5396. Selected roles can create and delete folders in TMS domain. PinICL 5071. Various roles can shut down system. PinICL 5316. NT directory structure not secure on all platforms. PinICL 5317. NT administrator role permissions are not restricted. PinICL 5294. Server manager can stop event logging. PinICL 4906. Security Manager can change system time. PinICL 4970. NFS log in returns error on PWYSEC and domain.
6.1.4	Two Person controls will not be implemented at Release 1c.
6.1.5	Discretionary Access controls will not be implemented at Release 1c.

FUJ00119593

4.10.4.1 PAS / CMS HELP DESK

Technical controls for the PAS/CMS Helpdesk in Bootle are at 2 levels:

1. Access to Windows NT on the individual workstation.
2. Access to the Oracle application on the Sequent

NT	
Current	Exclusions
The following access controls will apply: ➢ Users assigned unique ID ➢ Authenticate using passwords ➢ Enforced password change on first logon ➢ Maximum Password age : 30 days ➢ Minimum Password age : 1 day ➢ Minimum password length : 6 characters ➢ Not allowed to use previous 12 passwords ➢ Account lock out after 3 consecutive incorrect password attempts ➢ After lock out, account enabled by administrator intervention	➢ List of excluded passwords ➢ System displaying date and time of previous successful logon ➢ Administrators are able to change account policies
The following events will be audited: ➢ Logon and Logoff ➢ User and Group management ➢ Security Policy Changes ➢ Restart, Shutdown, and System	➢ NT 3.51 does not audit incorrect logon attempts
Application	
Current	Exclusions
The following access controls will apply: ➢ Users assigned unique ID ➢ Authenticate using passwords	➢ Enforced password change on first logon (PinICL - 5729) ➢ System displaying date and time of previous successful logon (5727) ➢ Maximum Password age : 30 days (5728)

FUJ00119593

	➢ Minimum Password age : 1 day (5728) ➢ Minimum password length : 6 characters (4118) ➢ More than two consecutive characters in password (4118) ➢ Password same as user ID (5719) ➢ Account lock out after 3 consecutive incorrect password attempts (4072) ➢ After lock out, account enabled by administrator intervention (4072)
The following events will be audited: ➢ Logon and logoff ➢ Failed logon attempts ➢ Application start up and shutdown ➢ System start up and shut down	

4.10.5 AUDIT AND ALARMS

With the following exceptions Audit and alarm facilities identified in SFS section 7 are provided at Release 1c.

Security Functional Specification	Description
7.2.1.1, 7.4.1.4	Provisions at R1c The following audit events will be provided at R1c. 1. DSS Service Environment 1.1 VME CAPS and OBCS Access to the VME system, from PAS/CMS host, is required to view files transferred at the contractual boundary. This has been agreed with the DSS and appropriate security controls are already in place: System access to the VME host is controlled by ACL's. Apart from file transfer verification, Pathway has no access to this machine 2. DSS Service Infrastructure 2.1 PAS/CMS Host Security related auditable events on the PAS/CMS host system are given in the table

FUJ00119593

Security Functional Specification	Description
	below. Action or Event — Audit Data Successful System Log-on — Script system log Failed System Log-on (Loginlog) — Dynix system log System Log-off — Script system log System Exceptions — BMC Patrol (limited) Oracle Exceptions are logged on) — BMC Patrol (users who File Transfer Success/Exceptions — FTF alert Successful Oracle Log-on — Oracle audit table System Start-up — Script system log System Shutdown — System log Change of User Rights — System log Write Access to Files in script system log. BOMVerify. — Access to files recorded User Account Management — Script system log 2.2 PAS/CMS Help Desk User access to the PAS/CMS Oracle database is held as an audit trail within one or more of its tables. 2.3 Horizon Help Desk As 3.2. 3. TMS 3.1 OBCS Host The script command will support system level auditing, as for PAS/CMS. Security related auditable events on the OBCS host system are given in the table below. Action or Event — Audit Data Successful System Log-on — Script system log* Failed System Log-on — Script system log* System Log-off — Script system log* File Transfer Success/Exceptions — Control files

FUJ00119593

Security Functional Specification	Description
	System Start-up — Script system log*
	System Shutdown — Script system log*
	Change of User Rights — Script system log*
	Write Access to Files — Access to files recorded in script system log. Write access to files not available
	User Account Management — Script system log*
	* The script system log contains the output from the UNIX script utility (enabled to capture keyboard activities and screen images).
	3.2 Agents
	Windows NT system and application level events will be forwarded, by a TME Agent, to a central Tivoli system. Security related auditable events on agent systems and other NT systems, are given in the table below.
	Action or Event — Audit Data
	Successful System Log-on — NT Event log
	Failed System Log-on — NT Event log
	System Log-off — NT Event log
	Application Exceptions — NT Event log
	Successful System Start-up — NT Event log
	Failed System Start-up/Shutdown — NT Event log
	Successful User Account Management — NT Event log
	Failed User Account Management — NT Event log
	Successful Change of Security Policy — NT Event log
	Failed Change of security Policy — NT Event log
	Write Access to Files — Write access to files not available
	HP Open View will detect any system inactivity on the network and forward such events to a central Tivoli system.
	Audits of failed start-up and shutdowns are dependent on the operability of the operating system. Again, HP Open View will report any system inactivity.
	3.3 Correspondence Servers
	As 3.2
	4. De La Rue Card Management
	As 3.2
	5.Post Office Counters
	All security related activities are managed by Riposte software and recorded within the

FUJ00119593

Security Functional Specification	Description
	TMS Journal as defined by the table below. Action or Event — Audit Data Successful System Log-on — TMS Journal Failed System Log-on — As in R1c RCD System Log-off — TMS Journal Application Exceptions — Local NT Event log Successful Start of Session — TMS Journal Successful End of Session — TMS Journal Failed System Start-up/Shutdown — NT Event log Successful User Account Management — TMS Journal Successful Change of User Rights — TMS Journal 6. Systems Management Solaris Event servers (front end to the Tivoli central system) will not be accessible to users either locally or remotely other than for maintenance by system administrators. Therefore there are no security issues for these systems. NT servers, holding events and notices in Oracle databases, will follow 3.2 for remote access. Local access will not be available other than for maintenance by system administrators. 7. MIS No system level auditing is planned for Release 1c or later. Access and changes to sensitive data in CCS and Contract Administration, namely SLA and Invoicing, is recorded. Authentication of users logging into the Oracle system is not recorded but details of each user viewing or modifying information is audited in tables. 8. Associated NT functionality not available; PinICL 5261, 5318. Not all NT events audited (system shutdown). PinICL 4655, 3726. Specific nature of user account change not defined in audit log.
7.3.3	No audit logs are maintained within the OBCS Host System of actions on the Oracle database since all OBCS processes are 'batch' and no data modification takes place within the processes. The execution of all OBCS processes are logged in the Oracle Process Audit Table.
7.4.1.1	All security related activities are managed by Riposte software and recorded within the TMS Journal. (see above).
7.5.1.1	Mitigation: DYNIX • The UNIX utility '*BOMverify*' will be scheduled to run at each shift change to highlight any changes in audit file characteristics. Output will be reviewed by the CFM

FUJ00119593

Security Functional Specification	Description
	Security Manager and exceptions escalated to the Pathway Security Manager for investigation. • The Dynix utility <script> is to be enabled for all interactive Dynix operational users. This utility captures all keyboard activity and screen images. <Script> output will be piped to a secured directory, modifiable only by <root>. It is not possible to login directly as <root>. Users must login with their unique User Id and *su* to <root>. The *su* to <root> is logged, BMC Patrol will monitor the *sulog* and cause a Tivoli event to be notified if it detects the use of *su* NT • NT will generate messages in the NT Security log according to Audit Policy settings. • The three event logs on all central NT servers (System, Application & Security) are polled at 20 second intervals by a Tivoli NT Event Adapter. All events that have been written to the event logs in the preceding 20 seconds are 'harvested' and written to a Tivoli Event Server (TES) in the Wigan Data Centre. • The TES is archived daily and archives are (currently) maintained for 18 months. • The TES is managed by dedicated CFM Systems Management Centre staff who can only change the status of an event (e.g. from OPEN to ACKNOWLEDGE). They cannot amend fields within the event nor can they delete events. GENERAL The Pathway Security Manager will perform periodic physical audits to ensure the continued application of these mitigations. Details of these audits will be made available to PDA/FSG, and PDA/FSG will be able to conduct independent audits. • All CFM staff providing operational support to the Pathway system are dedicated to the project i.e. they are not involved in work on any other CFM business. • The CFM Security Manager will allocate roles in accordance with the ACP, utilising the user account facilities available in Dynix where appropriate. • Roles requiring access to the Dynix operating system will be divided into those with a legitimate <root> access requirement, and those with no <root> access requirements at all. In this way, <root> access will be restricted to the absolute minimum number of users necessary to maintain efficient operation of the system. For Release 1c that means two senior support staff plus the Security Manager. • Operational procedures will be introduced in addition to existing physical and personnel controls; these include but are not limited to: • Two man working if <root> access is required during the operational day; • <Root> access outside of the operational day is event driven and is only available to

FUJ00119593

Security Functional Specification	Description
	two members of staff on a rota basis; • A paper audit log of all such access. • The NT Admin privilege will be controlled in the same way as <root> (i.e. restricted to the absolute minimum number of users necessary to maintain efficient operation of the system). • The Security Manager will be responsible for the allocation of roles in accordance with the ACP, utilising the NT privilege facilities where appropriate. • Passwords associated with <root> and Admin will be administered by the CFM Security Manager, whose responsibilities include changing the passwords regularly in step with the staff rota.
7.6.1.6	Mitigation • The Pathway Security Manager is responsible for the issue, control, verification and modification of cryptographic key material, as described in the document 'Pathway Key Process Management for Release 1c'. • A key change is a combination of a physical process performed by the key custodian and an automated Tivoli process to introduce the three elements necessary to satisfy comprehensive integrity checks. • In addition to the general controls described below, an independent audit of key changes is maintained by the Pathway Security Manager. • The UNIX utility '*BOMverify*' will be run at each shift change to highlight any changes in file characteristics. Output will be reviewed by the CFM Security Manager and exceptions escalated to the Pathway Security Manager for investigation. • The Dynix utility <script> is to be enabled for all interactive Dynix operational users. This utility captures all keyboard activity and screen images. <Script> output will be piped to a secured directory, modifiable only by <root>. It is not possible to login directly as <root>. Users must login with their unique User Id and *su* to <root>. The *su* to <root> is logged BMC Patrol will monitor the *sulog* and cause a Tivoli event to be notified if it detects the use of *su*. GENERAL • The Pathway Security Manager will perform periodic physical security audits to ensure the continued application of these mitigations. • All CFM staff providing operational support to the Pathway system are dedicated to the project i.e. they are not involved in work on any other CFM business.

FUJ00119593

Security Functional Specification	Description

	• The CFM Security Manager will allocate roles in accordance with the ACP, utilising the user account facilities available in Dynix where appropriate.
	• Roles requiring access to the Dynix operating system will be divided into those with a legitimate <root> access requirement, and those with no <root> access requirements at all. In this way, <root> access will be restricted to the absolute minimum number of users necessary to maintain efficient operation of the system. For Release 1c that means two senior support staff plus the Security Manager.
	• Operational procedures will be introduced in addition to existing physical and personnel controls; these include but are not limited to:
	  • Two man working if <root> access is required during the operational day;
	  • <Root> access outside of the operational day is event driven and is only available to two members of staff on a rota basis;
	A paper audit log of all such access.

7.7	Audit facilities for Windows NT systems at Release 1c will be provided through use of the Tivoli Systems Management software.

4.10.6 ADDITIONAL NT FUNCTIONALITY NOT AVAILABLE

PinICL 3888, 4425, 4517, 5223. List of excluded passwords.

PinICL 5229. NT 3.51 (as used at Help Desk) does not default to force change of password on first log on. Mitigation; manual process to ensure that administrator sets initial password to auto expire.

4.10.7 CRYPTOGRAPHIC FUNCTIONALITY

All cryptographic functionality identified in SFS section 8 is provided with the following exclusions:

Security Functional Specification	Description
8.3	TIP Links will not be supported at Release 1c.
8.3.1	POCL TIP Link protection *Protection in later releases is deferred as described in the SFS*

FUJ00119593

Security Functional Specification	Description
8.4	APS Links will not be supported at Release 1c.
8.6.2	Post Office ISDN/PSTN/GSM Links, Roll-out: The first real CHAP key and the Post Office's private key for use in signing automated payments are transferred from KMS as part of the personalisation process *KMS will not be available, a simple algorithm will be used to determine the initial CHAP key, and the AP signing key is not needed as AP signing is not provided in Release 1c.*
8.6.3	Post Office ISDN/PSTN/GSM Links, Key management: CHAP keys will be replaced at regular intervals. *The CHAP key will not be replaced during the life of Release 1c.*

4.10.8 MESSAGE PROTECTION

Message protection identified in SFS section 9 is provided in Release 1c with the following exclusions:

Security Functional Specification	Description
9.1, 9.2	Key management: Working public keys are distributed by KMS *The life of public keys is long enough not to need to change during Release 1c and before the next release*
9.4	Automated Payments are signed in the Post Office and the signature will be verified just prior to delivery of the AP data across the agreed delivery interface *Signing AP transactions is not in Release 1c due to implementation and KMS (Key Management System) issues*

4.10.9 FILESTORE ENCRYPTION IN POST OFFICES

Filestore encryption identified in SFS section 10 is provided in Release 1c.

4.10.10 ADMINISTRATION OF SECURITY

Management and operational controls identified in SFS section 11 are provided in Release 1c.

FUJ00119593

4.10.11 ACCESS CONTROL ISSUES

The following table identifies the remaining issues raised by the PDA in the area of Access Control for which there is no agreed resolution at Release 1c..

Access Control Issues	Comment
1. Access differentiation is required at lower than the button impulse. (e.g. allow a supervisor to create a supervisor but disallow the creation of a manager.	Resolved by agreement with PDA Security Management over restriction of 'Create User' facilities to only the most senior level of user.
1. Once created, the full name and teller ID must not be accessible for modification by users.	Teller ID is an optional field which is not used within the application.
1. There is a requirement to restrict password re-usage by user (preference is password disallow attribute to be set to 3).	This facility is supported only for the most recent password (i.e. the user may not enter a new password which is the same as the one previously used). Full implementation of password histories is not currently supported by NT4 Application Programming Interfaces (APIs). Manual Procedure Required at Release 1c.
4. There is a requirement for the password and user ID formats to be restricted to a maximum size.	Maximum sizes are not supported by NT4, Manual Procedure Required at Release 1c.
1. There is a requirement for logon procedures to comply with best practice as exemplified within BS 7799 / DITSS e.g. Computer misuse warnings; unsuccessful logon attempt warnings.	Computer misuse warnings will be delivered as part of Release 1c. Unsuccessful logon attempt warnings cannot be delivered currently since NT4.0 does not support the APIs necessary to determine the status of the previous logon attempt.
6. User groups which are not appropriate to within outlet use should not be accessible of viewable from the outlet.	Only groups which are appropriate to an outlet are displayed. In the event that an authorised user assigns multiple roles which include a 'visitor' role (e.g. Auditor), the characteristics of the 'visitor' role take precedence.

FUJ00119593

4.11 FRAUD RISK MANAGEMENT AND BPS MIS

The requirements and contractual obligations have been taken from the following source documents:

1. Benefit Payment System MIS Catalogue, Issued Version 4 dated 11 December 1996
2. Fraud Risk Management Service Design, next version following Version 2.0 dated 14 Th. November 1996 (yet to be issued)
3. Schedule B01, Requirement 895, Version inclusive of drop-down amendments.
4. Extended Verification Process Requirement, Draft Version 0.5 dated 11 October 1996

At *Release 1c*, some of the required reports will be passed to the CA clerically rather than electronically. This will include details of real or suspected fraudulent transactions, sufficient (as agreed with CA) to support case investigation.

Functionality at *Release 1c* is documented in "Fraud Risk Management and BPS MIS *Release 1* Contents" ref. RS/SPE/0004, again to be updated following issue of new version of FRMSD [2] above.

The following sections identify known limitations regarding the implementation of Fraud Risk Management.

FUJ00119593

4.11.1 FRAUD RISK MANAGEMENT AND BPS MIS - RELEASE 2

All the following requirements have all been deferred to Release 2. This deferral assumes that the DSS will have established a central Fraud Case system which is capable of communicating electronically with Pathway's Data Warehouse. If this interface is agreed by dates to be defined by Pathway, then Pathway can develop and implement the required FRMS database on the Data Warehouse for release 2.

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
[2] 3.4	2.5.2	Total number and value of fraudulent Permanent and Casual agent transactions by region and as a percentage of all fraudulent agent transactions.	needs FRMS database
[2] 3.4	2.5.2	Total number and value of fraudulent transactions by loss category by region.	needs FRMS database
[2] 3.4	2.5.2	Total number and value of fraudulent transactions by region.	needs FRMS database
[2] 3.4	2.5.2	Total number and value of all fraudulent transactions.	needs FRMS database
[2] 3.4	2.5.2	Average value of fraudulent transactions.	needs FRMS database
[2] 3.4	2.5.2	Total number and value of fraudulent transactions by benefit type.	needs FRMS database
[2] 3.4	2.5.2	Average value of fraudulent transactions by benefit type.	needs FRMS database
[2] 3.4	2.5.2	Total number and value of fraudulent transactions by customer type (Beneficiary, Appointee, Casual Agent, Permanent Agent).	needs FRMS database
[2] 3.4	2.5.2	Total number and value of fraud losses by type of loss category	Not defined at this stage, but expected to include Card: lost, stolen, counterfeit. Needs FRMS database
[2] 3.4	2.5.2	Total number and value of foreign transactions by loss category.	needs FRMS database
[2] 3.4	2.5.2	List of PUNs reported not received but card collected.	New Help Desk Functionality Required

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
[2] 3.4	2.5.2	At the end of each quarter a report incorporating the above quarterly reports in an aggregated format will be provided. The report will also detail any identified trends that fall outside of the above reports. These will be compared against previous reports in order to monitor long term fraud control.	Use of Business Objects
[2] 3.4	2.5.2	At the end of each ICL Pathway financial year a full report incorporating the above in an aggregated format will be provided. ICL Pathway FRMS will also report on the identified trends occurring during the year. These will be compared against previous years in order to monitor long term fraud control.	Use of Business Objects
[2] 3.5	2.5.2	Post Offices where the number of individual frauds are > than X.	needs FRMS database
[2] 3.5	2.5.2	Post Offices where levels of fraud loss is > X.	needs FRMS database
[2] 3.5	2.5.2	Post Offices where there is a higher than X incidence of fraudulent foreign and / or agent encashments.	This will most likely be expressed as a percentage of total office transactions. Needs FRMS database
[2] 3.5	2.5.2	Post Offices where fraud losses > than X occur involving a particular type of Identification Document (where recorded) or extended verification procedures.	needs FRMS database
[2] 3.5	2.5.2	Post Offices where more than X fraudulent transactions are made by Casual Agents.	needs FRMS database
[2] 3.5	2.5.2	Post Offices where more than X percentage of all transactions are fraudulent	needs FRMS database
[2] 3.5	2.5.2	Customers who have been issued with a second reminder PUN.	Function issuing 2nd PUN reminders to be enhanced to produce a summary list of customers. Awaiting CMS CP to be raised & impacted.
[2] 3.5	3.1.2.10.2	Customers who have infringed	Additional functionality to CMS

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
	2.5.2	Change of Nominated Post Office rules.	required. Only relevant to those cases where Restricted Post Office Indicator is set.
[2] 3	2.5.2	Allow transaction data identified as representing real or suspected fraud to be copied from the Data Warehouse to the FRMS Database. This will enable flags to be applied to monitor the progress of investigation.	needs FRMS database
[2] 3	2.5.2	Allow flags to be altered that are attached to transactions which have been investigated for actual or suspected fraud. This will allocate the transaction and value to one of a number of loss categories, and will allow full accounting, fraud analysis and assist in the determination of liability.	needs FRMS database
[2] 3	2.5.2	Ensure that flagged data relating to actual and suspected fraud is retained within the FRM Database for a period of time beyond that used for normal transactions to enable a full and detailed ICL Pathway fraud history to be compiled and used to determine future fraud prevention measures and as evidence.	needs FRMS database
[2] 3	2.5.2	Analyse the database using rules to identify potential fraud incidents; these rules require definition and agreement by ICL Pathway and the Contracting Authorities. Be sufficiently flexible to automatically produce reports according to parameters set, and allow ICL Pathway FRMS to amend these overnight. This only applies to the FRMS Database, those reports being produced from other parts of the system will require a longer notice period. Be accessed by dedicated PC workstations. Be fully auditable, password	All non-functional requirements to be addressed and met on the introduction of the FRMS database at release 2

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
		protected and able to produce activity logs for each operator including terminal ID, log on/off times and files/records accessed. This system will be automatic requiring no manual input by ICL Pathway FRMS management	
[2] 3.2	2.5.2	In order to carry out effective Fraud Risk Management the system will be able to access and retrieve all information associated with fraudulent or suspect transactions. If all the information required in the data capture list is not available within the data warehouse, the FRM system will be able to retrieve it from other Pathway databases such as PAS and CMS.	needs FRMS database
[2] 3.2	2.5.2	The placing of fraud flags on particular transactions will instigate automatic retrieval of associated items of information, which may or may not be held within the data warehouse. ICL Pathway FRMS will only be able to place these flags once the repudiated transaction becomes known to the FRMS. Therefore a mechanism for passing this information from the Contracting Authorities to ICL Pathway FRMS is required. ICL Pathway FRMS will inform the Contracting Authorities of suspect events through an exception reporting process as ICL Pathway becomes aware of such occurrences. Once a fraud has been confirmed and a final category flag relating to that event has been posted, the event will be linked to any appropriate previous reports. This will allow a full fraud and transaction history to be built up within the FRMS Database and hard copy reports to be produced The ICL Pathway FRMS Database	needs FRMS database

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
		will also allow information to be recalled by using any of the individual pieces of data as the search field.	
[2] 4.6	2.5.2	All PCs will be subject to access controls and located in a physically controlled environment with a full audit trail enabling ICL Pathway FRMS management to trace what information was accessed and by whom. A separate Data Protection entry in the FRMS Database may also be required and the production of full operator activity sheets will allow management to investigate any alleged breaches of the Act. It will be possible to show who requested a report, when the request was made, when the information was made available and when it was finally accessed and, where appropriate, printed.	All non-functional requirements to be addressed and met on the introduction of the FRMS database at release 2 Needs FRMS database
[2] 3.2	2.5.2	The system will also have access control to indicate and prevent an ICL Pathway FRMS operator of the FRMS Database accessing data relating to an account deemed to be sensitive by the Contracting Authorities i.e. a National Sensitivity Indicator is set, unless authorised to do so.	Definition required, introduce with FRMS database at release 2
[3] 1	2.5.2.2	Monthly reports of individual instances of non encashment of a means tested benefit for a period of (four weeks)	Need changes to reference data sourced through CAPS such that Payment Description carry 2 new signals + new CMS report
[3] 2	2.5.2.2	Monthly reports of individual instances of non encashment of a non means tested benefit, specified according to benefit type (e.g. incapacity benefit), for a period of (six weeks)	Need changes to reference data sourced through CAPS such that Payment Description carry 2 new signals + new CMS report
[3] 3	2.5.2.2	Monthly reports of individual instances of change of nominated	Cardholder record needs to change to add last to POs + date

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
		post office, not reversed within (six weeks), where there is both encashment of any means tested or specified non-means tested benefit, whose date of first availability is after the change of nominated post office, and where there is no notification of change of address received within (six weeks).	change + last change of address date, + new CMS report
[3] 5	2.5.2.2	Monthly reports of individual instances of any encashment made after a payment stop has been received by Pathway	New CMS report from exception file - assume these are also reported back through CAPS
[3] 9	2.5.2.2	Daily reports of transactions at a non-live post office i.e. one reported to Pathway as temporarily out of commission	CMS functionality required to record office temporarily out of commission then to reinstate - these records to be made available to MIS
[1] 1		Number of Cards Issued	Report is being produced at release 1c by everything except DSS Issuing Office. Assume reference data mapping of Post Office to DSS Issuing Office to BA region is resolved at release 2.
[1] 3 & 5		Number of Calls Received Average Length of Calls	For calls received from BA Staff, the release 1c function only reports by BA Office. Assume reference data mapping of Post Office to DSS Issuing Office to BA region is resolved at release 2.
[1] 12		Ongoing number of cards activated	The release 1c function does not report by DSS Issuing Office. Assume reference data mapping of Post Office to DSS Issuing Office to BA region is resolved at release 2.
[1] 11	See next issue of SADD	Number of Temporary Tokens issued	Awaiting introduction of temporary token functionality
[1] 14	See next issue of SADD	Random Selection of encashment records	Awaiting production and impact of CP on PMS
[4] 11		The usage of EVP by Benefit type	EVP functionality within BES to

FUJ00119593

[Source Doc.] Section	SADD Ref.	Requirement Description	Comment
			be reviewed at release 2
[4] 11		Number of the same question failed as a percentage of all same question e.g. Day of Birth, failed, as a percentage of all Day of Birth questions.	EVP functionality within BES to be reviewed at release 2
[4] 11		Breakdown by percentage of successful to failed EVP transactions by Post Office and or Benefit Type.	EVP functionality within BES to be reviewed at release 2

FUJ00119593

4.12 SCHEDULE B03

Release 1c includes limited functionality to measure SLAs and to calculate Liquidated Damages. Schedule B03 assumes that the target component times will be established during Operational Trial, and that Actual System Component Times will be recorded by the system. The exact mechanism had not been agreed at the time that the original Release1 Contents Definition was authorised: it remained the subject of discussions and CCNs which may have had a material impact on measurement methods. Consequently, the way in which Release 1c measures the SLAs may not correspond with what was ultimately agreed for Schedule B03 and its replacement Schedules. Any such differences will be addressed in Release 2.

4.13 BOUNDARY SERVICE PERFORMANCE LEVELS

The mechanisms for monitoring and reporting internal boundary service performance levels for TMS/CMS/PAS will not be available in Release 1c.

FUJ00119593

ANNEX 1 :- CONTRACTUAL FUNCTIONAL BASELINE

Title	Reference Number	Version	Status
Security Functional Specification	RS/FSP/0001	2.0	Approved
Service Architecture Design Document	CR/FSP/0004	2.0	Approved
Fraud Risk Management Service Design Specification	RS/POL/0002	2.0	Approved
CAPS Access Service High Level Design	SU/DES/0001	5.0	Approved
CAPS to PAS/CMS Data Interchange Definition	PTA/PR/0008	06	Approved
BPS MIS Requirements Catalogue	BS/REQ/001	3.0	Approved
OBCS Business Process Rules	BP/PRD/0002	2.0	Approved
DSS Client Interface Specification - OBCS	OBCSINT	01	Approved
OBCS Interface High Level Design	SU/DES/003	2.0	Approved

FUJ00119593

ANNEX 2 :- RELEASE 1C TECHNICAL AND PHYSICAL ENVIRONMENT - ISSUE 4 (4/9/97)

SADD v 2.0 Reference	Release 1C Position
2.3.2.1	Apart from the use of Bootle to hold a single correspondence server, the Wigan site only is used at Release 1C. The Wigan site has comms connections through to the CAPS ACC at Livingstone and the ESNCS system at Washington
2.3.2.2	4 Correspondence Servers in a single group (3 at Wigan and 1 at Bootle) are deployed at Release 1C
3.1.1.8.2 3.1.2.11.1	Bootle is the only Help Desk location.
3.1.3.9.2.1.2	Online CAPS operation is not provided at Release 1C
3.2.1	Single site only at Release 1C (Wigan) with 2 hardware mirrors of the databases held on Symmetrix disks
3.2.3.1	Access to a single ACC (Livingstone) is provided at Release 1c start. During the lifetime of Release 1c a separate plan exists to introduce new CAPS functionality (multi service / Single ACC then multi service / multi ACC) Transfers in the direction from CAPS to Pathway are integrity protected using a Red-Pike encrypted checksum.
3.2.3.2	Single campus (Wigan) at Release 1C
3.2.3.3	At Release 1c, connection is made to the De La Rue site in Tewkesbury only for card and PUN production.

FUJ00119593

SADD v 2.0 Reference	Release 1C Position
3.2.3.4	No connection to Royal Mail is provided at Release 1c
4.1.3.3.5.1	The target 'time service' is not provided. At Release 1c, for Pathway's own operational purposes, counters and correspondence servers are time synchronised using native Riposte facilities. Central systems (including the correspondence servers) have their time set and synchronised manually.
4.1.5.1	Mobile configurations are not provided at Release 1c.
4.1.5.1.2	Support for weigh scales is not required at Release 1c
4.1.5.2.2.2	TMS will support approximately 5000 counter positions at Release 1c. The release is expected to be installed at approximately 500 counter positions and thus there is no constraint in practical terms.
4.1.5.1.6	Standard OPS configuration only
4.1.5.1.7 4.1.5.2.3.1	Mobile configuration not supported at Release 1C
4.1.5.3.1	No connection to Huthwaite or Farnborough at Release 1c. As a temporary expedient until the POCL TIP system becomes available, 'ABED' reports will be generated and transferred to Chesterfield via a modem connection.
4.1.5.2.3.3	No connections to TIP, Farnborough or POCL clients at Release 1C.
4.1.5.3.2.1.5	No Key Management Service at Release 1c. All keys are generated locally by Pathway and installed at build time.