Document Title	Security Acceptance Test	
Document Type	Acceptance Specification	
Abstract	This document describes the Acceptance Test for Security	
Status	Issued	
Author	D J JONES/J C C DICKS	
Approval By	APPROVED	
Distribution	Pathway	Management Team Test & Integration Manager Pathway Library
	POCL/DSS	Gareth Lewis
	PDA	Mary Reade

Recommended for Approval	ICL Pathway Test Manager	Authority(ies) Test Manager
Signature		
Name **Date**	D J JONES	
Approved	For and behalf of ICL Pathway	For and behalf of Authority(ies)
Signature		
Name **Date**		

0. DOCUMENT CONTROL

0.1 DOCUMENT HISTORY

Version	Date	Reason
1.0	7/7/97	Release 1e Version for approval
1.1	30/3/97	New Release 2 Version for review
1.2	30/07/98	Incorporating comments from Horizon Quality Review and changes to some of the High Level Test Plans.
1.3	14/08/98	Changes to incorporate final comments from Horizon
1.4	20/08/98	New Release 2 Version for approval by Horizon
2.0	16/10/98	Issued (for baselining)

0.2 ASSOCIATED DOCUMENTS

	Reference	Version	Date	Title	Source
(1)					
(2)	Acceptance Standard	0.1	13/09/96	Standard for Raising and Progressing Acceptance Incidents.	Pathway
(3)	Acceptance Standard	0.1	17/09/96	Standard for documenting Acceptance Specification	Pathway
(4)	Authorities' Agreement	8.0	14/11/97	Acceptance Procedures Schedule (A)A07	DSS/POCL
(5)	POCL Agreement	8.0	13/11/97	Acceptance Procedures Schedule (P)A11	POCL
(6)	DSS Agreement	8.0	14/11/97	Acceptance Procedures Schedule (D)A11	DSS
(7)	Authorities' Agreement	8.1	9/3/98	Requirements Schedule (A)B04	DSS/POCL
(8)	Authorities' Agreement	8.1	9/3/98	Solutions Schedule (A)B05	Pathway
(9)	DSS Agreement	8.1	9/3/98	Requirements Schedule (D)A15	DSS
(10)	DSS Agreement	8.1	9/3/98	Solutions Schedule (D)A16	Pathway

(11)	POCL Agreement	8.0	13/11/97	Requirements Schedule (P)A15	POCL
(12)	POCL Agreement	8.1	9/3/98	Solutions Schedule (P)A16	Pathway
(13)	CR/FSP/004	5.1	23/7/98	Service Architecture Design Document	Pathway
(14)	PA/STR/009	2.0	24/2/98	Release Contents Definition for Pathway New Release 2	Pathway
(15)	RS/FSP/001	3.2	5/8/98	Security Functional Specification	Pathway
(16)	RS/POL/003	2.0	24/2/98	Access Control Policy	Pathway
(17)	VI/STR/008	2.0	28/1/98	Release 2 Security Test Strategy	Pathway
(18)	VI/PLA/005	4.0	20/8/98	Pathway Corporate Services (MIS) Domain - Security HLTP	Pathway
(19)	VI/PLA/006	4.0	20/8/98	De La Rue Domain - Security HLTP	Pathway
(20)	VI/PLA/007	3.0	20/8/98	Systems Management Domain - Security HLTP	Pathway
(21)	VI/PLA/008	2.0	29/1/98	DSS Service Environment Domain - Security HLTP	Pathway
(22)	VI/PLA/009	3.0	6/3/98	Central Services Domain- Security HLTP	Pathway
(23)	VI/PLA/010	4.0	20/8/98	POCL & POCL Clients Domain - Security HLTP	Pathway
(24)	VI/PLA/011	2.0	20/08/98	Post Office Platform Domain - Security HLTP	Pathway
(25)	VI/PLA/012	4.0	20/8/98	PAS/CMS Service Domain - Security HLTP	Pathway
(26)	VI/TSC/105	3.0	31/07/98	Technical Integrity Test Plan	Pathway
(27)	RS/POL/002	3.3	23/2/98	Pathway Security Policy	Pathway
(28)	RS/PR0/028	0.1	27/4/98	ICL Pathway Security Management Procedures	Pathway
(29)	RS/PRP/002	1.0	21/12/95	BPS - Security Proposal	Pathway

(30)		6.0	6/97	Benefit Payment Card: Card Technical Specification	DSS
(31)	RS/SPE/003	2.0	8/4/98	Extended Verification Process Requirement	Pathway
(32)	RS/SPE/001	4.0	12/12/97	Fraud Risk Management Service Design Specification	Pathway
(33)	RS/SPE/002	0.9	1/7/97	Forwarding, Disposal of Impounded Cards, PUNs and Temporary Tokens	Pathway
(34)	SU/STD/001	0.1	20/7//94	DSS Business Data Standards (Referenced)	DSS
(35)	CAP/IFS/002	6.04	10/10/97	CAPS to PAS/CMS Data Interface Definitions & Validation Rules (R3) (Release 2)	DSS
(36)	RS/PRO/030	0.2	4/8/98	Evidential Information - Production, Certification & Retention (PACE)	Pathway
(37)	CR/FSP/006	2.2	8/9/97	Audit Trail Functional Specification	Pathway
(38)	CR/FSP/008	7.0	20/4/98	Post Office Not Available for Benefit Encashment	Pathway
(39)	BP/PRO/003	2.0	27/9/96	Post Office Site Failure Contingency Procedures	POCL
(40)	PA/PLA/003	0.6	17/4/97	Disaster Recovery Plan (in course of update)	Pathway
(41)	BP/PLA/013	1.0	22/2/97	Contingency Map	Pathway
(42)	BS/DOC/001	01	30/11/95	BPS Security Statement	DSS/POCL
(43)	RS/REQ/0001	2.0	12/12/96	ICL Pathway Security Objectives	Pathway
(44)	TD/DES/031	1.3	03/4/98	Release 2 Resilience and Recovery Strategy	Pathway
(45)	RS/PRO/031	0.1	17/8/98	Security Awareness Training	Pathway
(46)	RS/PRO/032	0.1	17/8/98	Security Event Management Process	Pathway
(47)	RS/PRO/013	1.0	25/6/98	Horizon Security Passes Procedure	Pathway
(48)	RS/PRO/002	1.0	28/7/98	Security Vetting Process	Pathway
(49)	IA/PLA/001	0.1	28/4/98	Audit Plan	Pathway

(50)	IM/ACS/001	2.0	23/6/98	Training Acceptance Test Specification	Pathway
(51)	t b a			Security HLTP	Girobank
(52)	t.b.a			Security HLTP	ICL Outsourcing
(53)	t.b.a			Security HLTP	ICL Outsourcing

0.3 ABBREVIATIONS

BT	Business Thread
DSS	Department of Social Security
HLTP	High Level Test Plan
PDA	Programme Delivery Authority
POCL	Post Office Counters Ltd

0.4 CHANGES IN THIS VERSION

This Version is issued for approval by Horizon.

TABLE OF CONTENT

1. PURPOSE & SCOPE

This document describes the Acceptance Test for Security in accordance with the Acceptance Procedures that are set out in the Schedules referred to in section 0.2 and also in the Pathway document "Standard for Documenting Acceptance Specifications". This Test will determine that Security meets all the Acceptance Criteria that are agreed in the Acceptance Specification and that are within the scope of the "Pathway Release Contents Specification" document for New Release 2, if applicable.

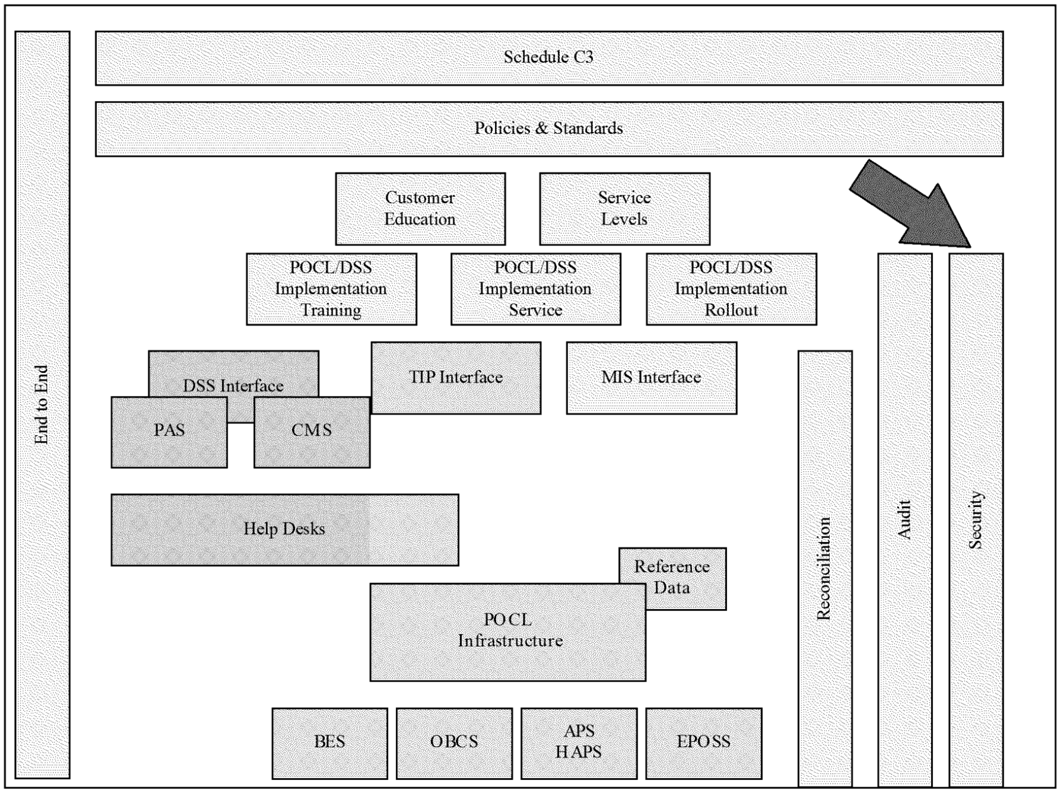

Figure1-1: This Acceptance Test in relation to others

2. ACCEPTANCE INCIDENTS

The standard and method for originating, progressing and resolving Acceptance Incidents shall be as described in the associated Document "Standard for Raising and Progressing Acceptance Incidents".

3. ACCEPTANCE PERIOD

The Acceptance Period for the Acceptance Tests which comprise the Operational Trial is as determined by schedule B07 of the AUTHORITIES' Agreement.

The Pathway programme plan details the schedule for the Security Acceptance Test.

4. DELIVERABLES & SERVICE

This section details the Deliverables and Services that are the subject of this Acceptance Test and as defined by the related Agreements.

Deliverable or Service.	**Contract Reference**	**Method**
Non-functional requirements	Requirements Schedule (A)B04 Requirements Schedule (D)A15 Requirements Schedule (P)A15	Acceptance Trial Acceptance Review

Table of Deliverables and Services.

5. ACCEPTANCE CRITERIA

This section lists the identifier of each Acceptance Criterion that will be demonstrated by the Acceptance Test. It also lists the Acceptance Test Conditions that are used to determine whether (or not) the Acceptance Criterion has been met together with the applicable test Phase, Technical Test, or Live Trial.

Acceptance Criteria are split into three sets of tables according to the nature of the acceptance method, one set for those tested by Acceptance Trial, a second for those tested by Acceptance Review and a third which lists those criteria which are for Acceptance at a later release. The Release on which Acceptance is to be conducted is defined by reference to the Release Contents Description included in the Associated Documents section of the Acceptance Specification. Exceptionally, it may be necessary for one particular Acceptance Criterion to be tested by a combination of trial and review in which case there are entries for Trial and Review.

5.1 ACCEPTANCE CRITERIA AND TEST CONDITIONS

Conformance of the Security Acceptance Criteria will be demonstrated through Acceptance Trials and/or Acceptance Reviews.

Tests conducted by Acceptance Trials comprise practical tests using prepared test scripts. If applicable the Test Condition(s) appropriate to a criterion are specified in section 5.1.1 together with a description of the test. Detailed composition of the test in terms of sequences of Test Conditions is contained in Section 10. In the tables in section 5.1.1 the rows labelled Function Run entry will be populated immediately prior to the running of the Acceptance Trials in a working version of the Acceptance Test Specification. These will provide invigilators with references to the checklists used to monitor the progress of the testing. The order of running of Test Conditions will not necessarily correspond to the order presented in HLTPs because of the “physicalisation” of the testing. The Function Run entry will allow the invigilator to read across from the criterion to the checklist.

Tests conducted by Acceptance Review comprise typically document reviews, site visits or presentations. If applicable the Test Condition(s) are described in section 5.1.2.

5.1.1 Description of tests conducted by Acceptance Trial

The table below shows which acceptance criteria will be met by Acceptance Trial.

All of the tests in this section will be performed during the Technical Test phase.

Requirement ID	828
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
HLTP / Business Thread Scenario	(18) through (25) ; (51); (52); (53) Requirement entry 828/1 is used to reference all the relevant Acceptance Trial provisions of (15) and (16).
Scenario Description	Test Scripts as shown in Section 10.1
Function Run Entry	Non-functional tests

Nothing contained herein shall be deemed or construed as affecting existing contractual obligations or creating new contractual obligations between ICL Pathway and the DSS and/or POCL.

Requirement ID	830
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
HLTP / Business Thread Scenario	(26) ; (44) Requirement entry 830/1 is used to reference all related Acceptance Trial provisions. These are described in sub-referenced documents: Pathway Release 2 Resilience and Recovery Strategy, (TD/DES/031), Issue 1.0; Pathway Network Infrastructure Resilience Validation (TD/DES/0029), Issue 1.0. Note that Requirement entry 830/1 is also included in the list of criteria to be met by Acceptance Review.
Scenario Description	Test Scripts are as shown in the Technical Integrity Test Plan (26).
Function Run Entry	Non-functional tests

5.1.2 Description of tests conducted by Acceptance Review

The table below shows which Acceptance criteria are to be met by Acceptance Review. Acceptance Tests will use the versions of any relevant documents (as referenced from section 0.2) contained in the approved version of the Acceptance Specification.

Requirement ID	698
Criterion Number	1
Derivation	Requirement
Criterion Description	The contractor shall minimise and control liabilities to itself and the AUTHORITIES
Test Condition	Appropriate policy and standards are in place.
Method	Document Inspection
References	(27); (28); (15) ; (16)
Phase	Operational Trial

Requirement ID	698
Criterion Number	2 (a) and (c to o)
Derivation	Requirement

Criterion Description	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;
	(b) (see next page)
	(c) security education and training;
	(d) reporting security incidents;
	(e) physical security control;
	(f) virus control;
	(g) business continuity;
	(h) control of Software;
	(i) safeguarding DSS and POCL records;
	(j) information classification;
	(k) compliance with data protection and other legislation;
	(l) information exchange control;
	(m) CONTRACTOR's sub-contractors and suppliers;
	(n) compliance with security policy;
	(o) the management of fraud and risk during Service operation.

Test Condition	An organised security infrastructure is in place.
Method	Document Inspection ; Site Visits
References	Review of (27): (a) (27) is approved by the Authorities (b) (see next page) (c) Section 5.3 ; and (45) (d) Section 3.8 ; and (46) ; (47) (e) Section 6.3 (f) Section 7.4 (g) Section 8; and (28) Section 9. See also 830/1 (h) Section 7.6; and (28) Section 8 (i) Section 6.2 . See also 828/1 (j) Section 6.1; and (28) Section 3.2. see also 830/1 (k) Section 9.2; and (28) Section 10.1.3. See also 830/1 (l) Section 7.5. See also 828/1 (m) Section 7.7; and (48) (n) Section 9.1; and (49) (o) Section 4. See also 897/1

Phase	Operational Trial

Requirement ID	698
Criterion Number	2 (b)
Derivation	Requirement
Criterion Description	Allocation of security responsibilities;.
Test Condition	An organised security infrastructure is in place.
Method	Demonstration or Presentation
References	(27) Section 3
Phase	Operational Trial

Requirement ID	698
Criterion Number	3
Derivation	Requirement
Criterion Description	The CONTRACTOR shall be compliant with BS7799.
Test Condition	Pathway complies with BS7799
Method	Document inspection
References	(27) Section 9.3 ; See also 828/1
Phase	Operational Trial

Requirement ID	722
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
Test Condition	Card Authentication Methods are as described.
Method	Document Inspection
References	((8) S722 Pathway Response Pathway confirms that the card authentication method will be positive rather than negative, resistant to forgery or other unauthorised manipulation and will include an agreed mechanism for identifying the attempted use of counterfeit or invalid cards and temporary tokens. Please see also the document entitled “The Pathway Benefit Payment Service - Security Proposal”, dated 21/12/95 [(29)]. Pathway Comment None); (29) Section 3 as updated by (30) and (13) 3.1.1.4 See also 828/1 and 830/1
Phase	Operational Trial

Requirement ID	723
Criterion Number	1
Derivation	Requirement
Criterion Description	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 person other than an Authorised Person.
Test Condition	1. Cardholder Verification Methods are as specified.
Method	Document Inspection
References	1. ((8) S723 2. Reference No 723 3. 4. Pathway Response 5. Pathway confirms that cardholder verification methods will be resistant to impersonation and will include an agreed mechanism for identifying the attempted use of a card or temporary token by unauthorised persons. Please see also the document entitled "The Pathway Benefit Payment Service - Security Proposal", dated 21/12/95[(29)]. 6. 7. Pathway Comment 8. None); 9. 10. (29) Section 5.3, 6 as updated by (13) 4.1.1.5; (31) 11. See also 828/1 and 830/1 12.
Phase	Operational Trial

Requirement ID	747
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
Test Condition	The following are secure, auditable and allow the production of audit trails: (a) Card and Temporary Token production and storage (b) Card delivery (c) Card and Temporary Token impounding / destruction / forwarding at the post office; Card destruction at the FRM centre
Method	(m) (a) Site visits (n) (b) Document inspection; Live Trial Report review (o) (c) Document inspection (p)
References	(a) to be scheduled (b) (13) 4.1.1.2, 4.1.1.3 [Note: Change Proposal pending] (c) (13) 4.1.1.6, 4.1.1.7; (33);(32) ; PPD ; (50)
Phase	Operational Trial

Requirement ID	747
Criterion Number	2
Derivation	Requirement
Criterion Description	The CONTRACTOR shall use all reasonable endeavours to assist with the investigation of the repudiation claim, including, but not limited to, timely provision of relevant data and documents from the CONTRACTOR's systems or services in a format suitable for detailed analysis by the AUTHORITIES.
Test Condition	Processes provide for data to be so retained
Method	Document Inspection
References	(32)
Phase	Operational Trial

Requirement ID	828
Criterion Number	2
Derivation	Requirement
Criterion Description	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.
Test Condition	The agreed Test Reports from CAPS DIT and E2E contain no non conforming entries relating to PAS/CMS to CAPS transfers.
Method	Document inspection. New Release 2 KPR has no non-conforming entries relating to PAS/CMS to CAPS transfers.
References	(34), (35) ; E2E Test Report
Phase	Operational Trial

Requirement ID	829
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
Test Condition	Such information is evidentially admissible and certifiable.
Method	Document Inspection
References	(27) Section 9.2; CFM data centre logs and Powerhelp Call Management System logs; (36) ; (28). See also 828/1 & 830/1
Phase	Operational Trial

Requirement ID	829
Criterion Number	2
Derivation	Requirement
Criterion Description	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.
Test Condition	Processes provide for information to be so retained at the direction of the Authorities
Method	Document Inspection
References	(32); (37); (36)
Phase	Operational Trial

Requirement ID	830
Criterion Number	1 through 8
Derivation	Requirement
Criterion Description	(1) 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. (2) The CONTRACTOR shall ensure that the contingency plans for each Service are compatible with an overall service continuity framework. (3) 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. (4) Ownership of all contingency actions shall be identified in the contingency plans. (5) The contingency plans shall include activation procedures and time periods within which the contingency measures shall be activated. (6) The contingency plans shall include a testing strategy with two distinct parts: (a) Initial testing before commencement of Roll Out of Services; (b) Regular testing. (7) The contingency plan shall include without limitation the following: (a) Prevention measures. (b) Preparedness measures. (c) Contingency measures. (d) Recovery of normal Service. (e) Contact lists. (8) 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.
Test Condition	Appropriate agreed contingency plans are in place and are subject to review Suitable Contingency plans are in place. Note that Requirement entry 830/1 is also included in the

CONTRACT CONTROLLED

Nothing contained herein shall be deemed or construed as affecting existing contractual obligations or creating new contractual obligations between ICL Pathway and the DSS and/or POCL.

	criteria to be met by Acceptance Trial to cover operational facilities for Resilience, Recovery and Error Handling.
Method	Document inspection ; Demonstration; Test Report Review
References	(41); (38); (39); (13) Section 4.1.6; (40)
Phase	Operational Trial

Requirement ID	830
Criterion Number	9
Derivation	Requirement
Criterion Description	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.
Test Condition	None
Method	
References	
Phase	

Requirement ID	872
Criterion Number	1
Derivation	Requirement (DSS only)
Criterion Description	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)
Test Condition	Processes for handling such information are in accordance with the applicable standard
Method	Document inspection
References	(13) 3.1.1.8.4, 3.1.2.11, 3.1.3.4
Phase	Operational Trial

Requirement ID	897
Criterion Number	1
Derivation	Requirement
Criterion Description	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.
Test Condition	The security policies are consistent with the objectives and policies of the BPS Security Statement
Method	Document Inspection
References	(27); (42)
Phase	Operational Trial

Requirement ID	897
Criterion Number	2
Derivation	Requirement
Criterion Description	The CONTRACTOR shall provide an appropriate countermeasure to each threat identified in the BPS Security Statement.
Test Condition	An appropriate countermeasure is provided to each threat.
Method	Document inspection
References	(42); (29) as updated by (43) and (15); (27)
Phase	Operational Trial

5.2 CRITERIA FOR LATER ACCEPTANCE

n/a

5.3 CRITERIA SUMMARY

Req ID	Criterion	Trial	Review	Later Acceptance
698	1		✓	
698	2		✓	
698	3		✓	
722	1		✓	
723	1		✓	
747	1		✓	
747	2		✓	
828	1	✓		
828	2		✓	
829	1		✓	
829	2		✓	
830	1	✓	✓	
830	2		✓	
830	3		✓	
830	4		✓	
830	5		✓	
830	6		✓	
830	7		✓	
830	8		✓	
830	9		✓	
872	1		✓	
897	1		✓	
897	2		✓	

6. ACCEPTANCE INCIDENT SEVERITY

This section identifies the guidelines to be applied during the analysis of Acceptance Incidents, in order to establish the severity of such Acceptance Incidents.

6.1 HIGH SEVERITY INCIDENTS

Failure to meet an Acceptance Criterion which would have a substantive impact on the service received by the Customer, e.g. failure to pay benefits to the right person, at the right place, at the right time.

Failure to meet an Acceptance Criterion which would have a major impact on the ability of the AUTHORITY or AUTHORITIES to perform their business, or where there was a major impact on the resources of the AUTHORITY or AUTHORITIES necessary to overcome that impact on their business, e.g. failure to support accurate POCL accounting.

Failure to meet an Acceptance Criterion which would impact the security of the service where there is no acceptable procedural workaround.

Consistent failure to meet Minimum Acceptable Thresholds for Service Levels, e.g. where particular transactions do not meet the minimum Acceptable Threshold under normal loading.

6.2 MEDIUM SEVERITY INCIDENTS

Failure to meet an Acceptance Criterion which is visible to the Customer and is likely to give rise to an adverse public perception of the service, but does not substantively impact the service received by the Customer, e.g. incorrect spelling on a receipt.

Failure to meet an Acceptance Criterion which would have a medium impact on the ability of the AUTHORITY or AUTHORITIES to perform their business, or where there was a medium impact on the resources of the AUTHORITY or AUTHORITIES necessary to overcome that impact on their business, e.g. non-production of a weekly report, resulting in its manual transcription, which causes additional resource or effort at every outlet of the average duration of one hour per week per outlet.

Occasional failure to meet Minimum Acceptable Thresholds for Service Levels, e.g. at peak loading, some transactions fail to meet Minimum Acceptable Thresholds, but on average all transactions within the service do achieve Minimum Acceptable Thresholds.

6.3 LOW SEVERITY INCIDENTS

Failure to meet an Acceptance Criterion that is neither visible to nor has substantive impact on the service received by the Customer e.g. presentational, style and other cosmetic faults that are only visible to the user.

Failure to meet an Acceptance Criterion which would have a minor impact on the ability of the AUTHORITY or AUTHORITIES to perform their business, or where there was a minor impact on the resources of the AUTHORITY or AUTHORITIES

necessary to overcome that impact on their business, e.g. non-production of a weekly report, resulting in its manual transcription, which causes additional resource or effort at ten or fewer outlets of the average duration of one hour per week per outlet.
Failure to meet an Acceptance Criterion which would impact the security of the service but where the workaround is as secure as the original solution (i.e. the only impact on risk is in ensuring that the workaround is performed, but where procedures have been agreed and are in place).

7. TEST DATA

Test data including any operator entered scripts that are required to run the Acceptance Test are defined below.

Business TestThread:

None

High Level Test Plan(s):

Pathway Corporate Services (MIS) Domain - Security HLTP

De La Rue Domain - Security HLTP

Systems Management Domain - Security HLTP

DSS Service Environment Domain - Security HLTP

Central Services Domain- Security HLTP

POCL & POCL Clients Domain - Security HLTP

Post Office Platform Domain - Security HLTP

PAS/CMS Service Domain - Security HLTP

Technical Integrity Test Plan

THIRD PARTY TEST DETAILS

Girobank - Security HLTP

ICL Outsourcing(Systems management) - Security HLTP

ICL Outsourcing(Support Services) - Security HLTP

Organisations:

Solutions Engineering, The Solution Centre, ICL
ICL Outsourcing -
Girobank

8. AUTHORITY RESPONSIBILITIES

This section describes the AUTHORITY's or AUTHORITIES' Responsibilities in relation to this Acceptance Test. Particular Acceptance Tests may also require additional participation and responsibility by the AUTHORITY or AUTHORITIES.

8.1 APPOINT TEST MANAGER

The AUTHORITY or AUTHORITIES shall nominate a Test Manager and other representatives to review the tests prior to commencement of the test.

8.2 ACCEPTANCE INCIDENT REPORTS

The nominated representatives and Test Manager shall be diligent in raising complete, accurate and timely Acceptance Incident Reports as set out within this Acceptance Test specification.

8.3 ACCEPTANCE INCIDENT ANALYSIS REPORTS

The Test Manager shall be diligent in returning signed Acceptance Incident Analysis Reports with their decision (e.g. Accept, Reject, Discuss) normally within five working days, or when urgency is requested by Pathway, within two working days of receipt from Pathway. A copy of all correspondence will be faxed to reduce delay.

8.4 ATTENDANCE AT TRIALS AND REVIEWS

The nominated representatives shall at their discretion attend Acceptance Test Trials and Reviews including repeat Tests at reasonable times and reasonable locations and with reasonable advance notice by Pathway.

8.5 MANAGEMENT AND CO-ORDINATION

The Test Manager shall be the single point of communication and co-ordination with Pathway's nominated Test Manager for all matters concerning this Acceptance Test from its initial planning through to Acceptance.

8.6 PROGRESS REVIEWS

Unless otherwise waived by both parties, Pathway's Test Manager and the AUTHORITY's or AUTHORITIES' Test Manager shall meet each week to review the progress and actions of both parties until Acceptance of the Acceptance Test is achieved. The time and location of review meetings will be scheduled with at least two week's advance notice by Pathway.

9. CONTRACTOR RESPONSIBILITIES

The Contractor shall nominate a Test Manager for each Test who shall be the single point of communication and co-ordination with the AUTHORITY's or AUTHORITIES' Test Manager for all matters concerning this Acceptance Test from its initial planning through to Acceptance.

Upon receipt of a signed Acceptance Incident Analysis Report from the AUTHORITY or AUTHORITIES, where correction is required to be re-tested within the same phase of Acceptance Test, the Contractor will return the amended component(s), on average, within 4 days. This will include re-testing necessary as per the agreed test strategies.

10. ACCEPTANCE TRIAL TEST CONDITIONS

10.1 SECURITY NON-FUNCTIONAL TESTS (REQ 828/1)

The following represent the eight Security Domains and extracts from the corresponding Solution Centre(TSC) HLTPs.
The Generic group represents tests from one domain but which are common to several of the Domains.

DOMAIN	Subdomain	User Identification	Authentication	Access Control	Audit	Alarms	Encryption / Integrity
GENERIC	Dynix (Sequent)	PAS01_1	PAS01_1	PAS01_2	PAS01_3	PAS01_3	
	Oracle RDBMS	PAS02_1	PAS02_1	PAS02_2	PAS02_3	PAS02_3	
	NT Server & Workstation	CSD01_1	CSD01_1	CSD01_2	CSD01_3	CSD01_3	
PATHWAY CORPORATE SERVICES	Dynix (Sequent)			PCS01_2			
	ORACLE RDBMS (Sequent) MIS Data Warehouse/SLAM DB Database - DW			PCS02_2			
	MIS NT Clients Slam Cache DB Help Desk FTF Gateway (Local & Remote) Pathway Clients	PCS03_1 PCS19_1 PCS20_1	PCS03_1 PCS19_1 PCS20_1	PCS03_2 PCS19_2 PCS20_2	PCS03_3 PCS19_3 PCS20_3	PCS03_3 PCS19_3 PCS20_3	
	MIS NT Clients	PCS04_1	PCS04_1	PCS04_2	PCS04_3	PCS04_3	

SQL*Forms Interface CON						
MIS NT Clients SQL*Forms Interface CCS	PCS13_1	PCS13_1	PCS13_2	PCS13_3	PCS13_3	
MIS NT Clients SQL*Forms Interface Reference Data	PCS14_1	PCS14_1	PCS14_2	PCS14_3	PCS14_3	
MIS NT Clients SQL*Forms Interface Fraud Risk Management	PCS15_1	PCS15_1	PCS15_2	PCS15_3	PCS15_3	
MIS NT Clients - FTMS Help Desk FTF Gateway (Local & Remote)			PCS05_2	PCS05_3	PCS05_3	
MIS SLAM cache DB Oracle Express Administrator			PCS06_2			
MIS Client PC Windows (SQL*Net Interface with Oracle) Pathway Clients	PCS07_1	PCS07_1	PCS07_2	PCS07_3	PCS07_3	
Oracle Express Server (OLAP) MIS Data Warehouse / SLAM			PCS08_2	PCS08_3	PCS08_3	
MIS Client PC Oracle Express (OLAP) Pathway Clients	PCS09_1	PCS09_1	PCS09_2	PCS09_3	PCS09_3	
MIS Client PC Business Objects FRM Pathway Clients	PCS10_1	PCS10_1	PCS10_2	PCS10_3	PCS10_3	

	ORACLE RDBMS (Sequent) MIS Data Warehouse/SLAM DB Database - FCDB	PCS11_1	PCS11_1	PCS11_2	PCS11_3	PCS11_3	
	ORACLE RDBMS (Sequent) MIS Data Warehouse/SLAM DB Database - SA	PCS12_1	PCS12_1	PCS12_2	PCS12_3	PCS12_3	
	MIS Client PC Business Objects BO_REP Pathway Clients	PCS10_1	PCS10_1	PCS16_2	PCS10_3	PCS10_3	
	MIS Client PC Business Objects BPSMIS Pathway Clients	PCS10_1	PCS10_1	PCS17_2	PCS10_3	PCS10_3	
	MIS Client PC Business Objects BUSDEV Pathway Clients	PCS10_1	PCS10_1	PCS18_2	PCS10_3	PCS10_3	

DE LA RUE	Campus Access Node NT	DLR01_1	DLR01_1	DLR01_2	DLR01_3	DLR01_3	DLR01_4
	DLRCT Access Node NT	DLR02_1	DLR02_1	DLR02_2	DLR02_3	DLR02_3	DLR02_4
	TDLR Access Node NT	DLR03_1	DLR03_1	DLR03_2	DLR03_3	DLR03_3	

SYSTEMS MANAGEMENT							
	Cisco Routers and Lan Switches	SMS09_1	SMS09_1	SMS09_2	SMS09_3		

	Auto Configuration Database Server			SMS20_2	SMS20_3		
	Auto Configuration Server - Database Client	SMS20b_1	SMS20b_1	SMS20b_2	SMS20b_3		
	Roll Out Database Server			SMS21_2	SMS21_3		
	Roll Out Database Client	SMS21b_1	SMS21b_1	SMS21b_2	SMS21b_3		
	Boot Server			SMS22_2	SMS22_3		
	CM Signing Server	SMS23_1	SMS23_1	SMS23_2	SMS23_3		SMS23_4
	Migration Agent Server	SMS25_1	SMS25_1	SMS25_2	SMS25_3		
	Miecco Laptop	SMS25b_1	SMS25b_1	SMS25b_2	SMS25b_3		
	SecurID Server	SMS26_1	SMS26_1	SMS26_1	SMS26_3		

DSS SERVICE ENVIRONMENT	Access to VME	DSE01_1	DSE01_1	DSE01_2	DSE01_3	DSE01_3	
	VME Filestore partition			DSE01_2	DSE01_3	DSE01_3	
	OBCS data						DSE03_3
	CAPS data						DSE04_3
	On-line data						DSE05_3

CENTRAL SERVICES	NT Domain Login	CSD01_1	CSD01_1	CSD01_2	CSD01_3		
	PDC						
	NT Domain Login	CSD02_1	CSD02_1	CSD02_2	CSD02_3		
	BDC						
	Correspondence Server Login	CSD03_1	CSD03_1	CSD03_2	CSD03_3		CSD03_4

	Agent & Signing Server Login	CSD04_1	CSD04_1	CSD04_2	CSD04_3		CSD04_4
	Archive Server Login	CSD05_1	CSD05_1	CSD05_2	CSD05_3		CSD05_4
	Vector (Crypto) Server Login	CSD06_1	CSD06_1	CSD06_2	CSD06_3		CSD06_4
	Network Time Management Server Login			CSD07_2			
	POLO Recovery PRAW Workstation Login	CSD08_1	CSD08_1	CSD08_2	CSD08_3		CSD08_4
POCL AND POCL CLIENTS	HAPS Campus Access Node (NT 4.0)	POCL01_1	POCL01_1	POCL01_2	POCL01_3	POCL01_3	POCL01_4
	HAPS Remote Access Node (NT 4.0)	POCL02_1	POCL02_1	POCL02_2	POCL02_3	POCL02_3	
	TIP Campus Access Node (NT 4.0)	POCL03_1	POCL03_1	POCL03_2	POCL03_3	POCL03_3	POCL03_4
	TIP Remote Access Node (NT 4.0)	POCL04_1	POCL04_1	POCL04_2	POCL04_3	POCL04_3	POCL04_4
OFFICE PLATFORM	Single-Counter Desktop	OPS01_1	OPS01_1	OPS01_2	OPS01_3	OPS01_3	OPS01_4
	Multi-Counter Desktop	OPS05_1	OPS05_1	OPS05_2	OPS05_3	OPS05_3	OPS05_4
	Riposte Message Store	OPS06_1	OPS06_1		OPS06_3		
	Communications - ISDN	OPS07_1	OPS07_1	OPS07_2	OPS07_3		
	ISDN Crypto	OPS10_1	OPS10_1		OPS10_3		
	ISDN Routers - External Interface - CLI	OPS09_1	OPS09_1	OPS09_2	OPS09_3		
	ISDN routers and Post Offices -	OPS10_1	OPS10_1		OPS10_3		

	External Interface - bidirectional CHAP Authentication						

PAS/CMS SERVICE	Hosts Central Server OS: Dynix	PAS01_01	PAS01_01	PAS01_02	PAS01_03		
	Hosts Central Server Database: Oracle	PAS02_1	PAS02_1	PAS02_2	PAS02_3		
	SQL Forms (Help Desk & SASD)	PAS03_1	PAS03_1	PAS03_2	PAS03_3		