



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

**Document Title:** Post Office Payment Service

**Document Reference:** ARC/SOL/CSP/3268

**Document Type:** Customer Solution Proposal

**Release:** Release Specific

**Abstract:** The purpose of this document is to describe the provision of a service to meet the requirements of Post Office to perform payment using cards and banking transactions at the SSK and counter.

**Document Status:** APPROVED

**Author & Dept:** Chris.Bailey GRO

**External Distribution:** Phil Evans, Post Office Limited

**Security Risk Assessment Confirmed** Yes

**Approval Authorities:**

Name	Role	Signature	Date
Torstein Godeseth	Chief Architect		
David Randall	Programme Manager		

**F00004291522**  
OASIS



## 0 Document Control

### 0.1 Table of Contents

<b>0</b>	<b>DOCUMENT CONTROL .....</b>	<b>2</b>
0.1	Table of Contents .....	2
0.2	Figures .....	4
0.3	Tables .....	4
0.4	Document History .....	5
0.5	Review Details .....	5
0.6	Associated Documents (Internal & External) .....	6
0.7	Abbreviations .....	7
0.8	Glossary .....	7
0.9	Changes Expected .....	8
0.10	Accuracy .....	8
<b>1</b>	<b>PURPOSE .....</b>	<b>9</b>
1.1	Introduction .....	9
<b>2</b>	<b>SCOPE .....</b>	<b>9</b>
2.1	Timescales and Phasing .....	10
2.2	Requirements out of Scope .....	10
2.3	External Dependencies .....	10
2.3.1	On Post Office .....	10
2.3.2	On ComputaCentre .....	11
2.4	Design Assumptions .....	11
2.4.1	Additional EMIS files received from Global Pay .....	12
2.4.2	Transaction determined before card read .....	12
2.5	Requirements .....	12
2.6	Use Cases .....	12
2.7	Non Functional Requirements .....	12
2.8	External Interface Specifications .....	12
2.8.1	Application Interface Specification (AIS) .....	12
2.8.2	Technical Interface Specification (TIS) .....	13
2.8.3	Operating Level Agreement (OLA) .....	13
2.9	Architectural Requirements .....	13
<b>3</b>	<b>SOLUTION ARCHITECTURE .....</b>	<b>13</b>
3.1	High Level Diagram .....	13
3.2	PCI Isolation .....	16
3.3	Design Outline .....	16
3.3.1	Network routing .....	19
3.3.2	Component Overview .....	19
3.3.3	Key Usage .....	20
3.3.4	Request and Authorisation Data .....	21
3.3.5	Reference Data .....	21
3.4	Reconciliation processes .....	21
3.4.1	General .....	21



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

3.4.2	Banking.....	22
3.5	Recovery.....	22
3.6	Removal of PCI data from systems .....	23
4	USER INTERFACE .....	23
4.1	Counter Dialogue.....	23
4.2	SSK Dialogue .....	23
4.3	Transaction flow on the PIN Pad.....	23
4.3.1	Note on Notation .....	24
4.3.2	Client system.....	24
4.3.3	C3E and AXIS .....	25
4.3.4	PSS .....	26
5	INFORMATION MANAGEMENT.....	27
6	NETWORK INFRASTRUCTURE .....	27
6.1	C3E to Ingenico Data Centre .....	27
6.2	Ingenico Data Centre to PSS .....	27
6.3	Near Real-Time Cancellations to Ingenico Data Centre .....	27
6.4	Documentation.....	28
6.5	Network Capacity.....	28
7	COMPLIANCE WITH LAW AND INDUSTRY STANDARDS .....	28
7.1	Data Protection and Obfuscation (DPA/PCI) .....	28
7.2	PCI compliance .....	28
7.3	On-going Compliance .....	28
8	SECURITY.....	29
8.1	Transaction security and replay protection.....	29
8.2	Key protection.....	29
8.2.1	Key Change.....	29
8.3	Device Security .....	30
9	RESILIENCE AND AVAILABILITY STRATEGY.....	30
9.1	Capacity .....	30
9.2	Availability.....	30
9.3	Recovery.....	31
10	PERFORMANCE AND SCALABILITY STRATEGY .....	31
10.1	Payment .....	31
10.2	Banking .....	31
10.3	Network.....	31
11	EXTERNAL DOCUMENTS .....	32
12	TESTING STRATEGY.....	32
13	ACCEPTANCE STRATEGY .....	32



<b>14</b>	<b>SERVICE INTRODUCTION AND MIGRATION STRATEGY .....</b>	<b>33</b>
14.1	Horizon Data Centre changes .....	33
14.2	EMIS files .....	34
<b>15</b>	<b>APPENDIX A OUTSTANDING DESIGN ISSUES .....</b>	<b>35</b>
15.1	A.1 Issues (on POL/3rd Parties) .....	36
15.2	A.2 Issues on FJS .....	36
15.3	A.3 Issues Resolved .....	36

## 0.2 Figures

Figure 1 - Block Diagram.....	15
Figure 2 - Payment Interaction Diagram .....	17
Figure 3 - Banking Interaction Diagram.....	18
Figure 4 - Component overview .....	20
Figure 5 –Future PCI data centre (logical) .....	33

## 0.3 Tables

Table 1 – External Documents .....	32
Table 2 – Outstanding Issues on Post Office Ltd/Other Suppliers.....	36
Table 3 – Outstanding Issues on Fujitsu Services .....	36
Table 4 – Issues Resolved .....	36





Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

## 0.4 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	20/10/2016	Initial draft	
0.2	21/10/2016	Minor alterations and corrections	
0.3	27/10/2016	Further additions	
0.4	n/a	Internal version	
0.5	18/11/2016	Further details added. Version shared with Post Office for info only	
0.6	25/11/2016	Draft for review internally and for impacting of build/test/deliver CP	
0.7	28/11/2016	Amended Review details.	
0.8	30/11/2016	Updates from POL review comments.	
0.9	08/12/2016	Added detail to support impacting	
0.10	16/12/2016	Revised in light of more detailed design	
0.11	11/1/2017	Revision in light of comments from Impacting process	
0.12	n/a	Internal version	
0.13	n/a	Internal version	
0.14	08/02/17	Clarification of scope of changes to PCI scope in light of information from last PCI audit and comments received.	
0.15	13/2/17	Add further clarification from comments received in Change Boards. Specifically add comment about BAL, PCI and APADC.	
1.0	15-02-2017	Version for approval.	CT2241

## 0.5 Review Details

Review Comments to :		Paul.Braisher; GRO; & PostOfficeAccountDocumentManagement; GRO
Mandatory Review		
Role	Name	
Security Architect	Dave Haywood; Darren Gaile	
Network Architect	Steve Freke	
CISO	Stephen Godfrey	
SSC Manager	Steve Parker; sscdm; GRO	
Service Architect	Phil Boardman	
POA BAS Lead	Steve Bansal	
Business Architecture & Requirements	Steve Evans	
Architect	Jon Hulme	



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

SV&I Manager	Ray Wodhams
Testing Manager	Mark Ascott
Architect – Counter and BAL	Andy Thomas
Infrastructure Implementation	Katy White
HDCR Principal CSA	Tim Jones
HDCR Infrastructure Solution Owner	Gareth Jenkins
<b>Optional Review</b>	
<b>Role</b>	<b>Name</b>
System Management Group	John Bradley (for SMG)
Quality & Compliance	Bill Membery
Security & Risk Team	CSPOA.Security GRO
Chief Architect	Torstein Godeseth
Application Lead SDM, Risk and Service Introduction	Yannis Symvoulidis
Application Development Manager	Graham Allen
Lead Hosting Architect	Patrick Kelly
Crypto, Agent & Web Svcs Developer	Stuart Honey
Release, Integration & InfRel	Vijesh Pandya
Programme Manager	Cameron Houston
Chief Architect	Torstein Godeseth
Operational Change/Release Management	Alan Flack
Business Continuity	Almizan Khan
Network Operations Manager	Roger Stearn; Chris Harrison
Systems Mgt & Global Cloud	Catherine Obeng
Infrastructure Operations Manager	Andrew Hemingway
Solution Design / Development	Pavan Vejendla
Atos Lead Project Architect	Peter Stanley (Atos)

(\*) = Reviewers that returned comments

## 0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
REQ/GEN/PRO/0735			HNG-X Generic Release Acceptance Process	Dimensions
SVM/SDM/PRO/0875			End to End Application Support Strategy	Dimensions
DES/INF/HLD/1969	4.0	22/10/14	Post Office Managed Switch HLD	Dimensions
ARC/NET/DPR/1467	2.0	08/11/12	Post Office Managed Switch(POMS) Design Proposal	Dimensions
DES/NET/TIS/xxxx	Tbs		Ingenico Axis service to HBS Payment Service TIS	Tbs



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Reference	Version	Date	Title	Source
REQ/APP/AIS/3265			Ingenico Axis service to HBS Payment Service AIS	Dimensions
REQ/CUS/BRS/3267			Requirements Catalogue - Payment Service	Dimensions
ARC/SOL/CSP/3173			Implementation of POCA on SSK (Fujitsu Components)	Dimensions
ARC/SOL/CSP/3291			Payment Service Counter Integration	Dimensions

*Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.*

## 0.7 Abbreviations

Abbreviation	Definition
ACE	Application Control Engine on a Cisco router. Provides load balancing etc.
ARC	Asylum seekers Registration Card
APOP	Automated Payments Out Pay – this is essentially a database containing vouchers.
BAL	Branch Access Layer platform (runs the OSR)
BRDB	Branch DataBase
CISO	Chief Information Security Officer
DRS	Data Reconciliation Service – system that reconciles transactions and payments
HBS	Horizon Business Server
MID	Merchant Identifier – number assigned by the acquirer to represent the merchant performing a payment. In Post Office, this relates to an individual branch.
OSR	Online Service Router
POA	Post Office Account (inside Fujitsu)
PODG	Post Office Data Gateway
POL	Post Office Limited
POMS	Post Office Managed Switch
PSS	POCa Support Service
RDT	Reference Data Test – used to identify test rigs
RTS	Retail Transaction Service – component within HBS that handles transactions for SSK
SSK	Self-Service Kiosk
TID	Terminal Identifier

## 0.8 Glossary

Term	Definition
ATOS/Atos	Post Office Limited's SISD supplier
BRA01	Term used to identify the Fujitsu premises at Lovelace Road, Bracknell, RG12 8SN.



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

Term	Definition
C3	This is a software component produced by Ingenico which, subject to commercials being agreed, will be modified to support POCA (Banking).
C3E	C3 Embedded. A version of C3 that runs inside the pin pad.
CDE	Cardholder Data Environment (i.e. parts of a system where cardholder data is processed)
EMIS	Electronic MIS file: a file of data from the acquirer (GlobalPay) showing the result of the payment requests in the payment file.
PCI	Payments Card Industry (PCI sets rules for handling cardholder data)
Quantum	Prepaid gas card and system for topping it up
Talexus	Prepaid token for electricity meters and system for adding credit to such tokens.

## 0.9 Changes Expected

Changes
Changes due to review. This document is expected to be changed iteratively as the project develops. Change is therefore expected until the first baseline.

## 0.10 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.



# 1 Purpose

The purpose of this document is to describe the provision of a service to meet the requirements of Post Office to perform payment using cards and banking transactions at the SSK and counter. The introduction of this will be phased, starting with the support for credit/debit card payments at the SSK, followed by support for credit/debit cards, banking and ARC at the counter. A third phase may, in future, introduce POCA and possibly other banking transactions on the SSK. A fourth phase would see the introduction of a separate data centre for the systems holding PCI data. This could be a logically or physically separate data centre.

The intention of the overall project is to reduce the scope of PCI within the Post Office Horizon solution by:

- replacing bespoke components with validated COTS solution where available,
- the enhancement of such products while retaining their status as COTS,
- enabling the future rehousing of the remaining bespoke components within a PCI data centre.

While none of these things remove the PCI scope completely, they seek to reduce it to the minimum possible.

The journey to the reduced PCI scope within the Post Office Horizon solution will be, by necessity, phased. This is the first step of that journey, and covers the first two phases.

## 1.1 Introduction

Post Office currently support a number of financial transactions with plastic cards which fall within the regulatory domain of PCI. The systems involved pre-date PCI and while secure and never implicated in any breach or disclosure, were not constructed on the same philosophical footprint as PCI has developed. The consequence of this is that as PCI bring in ever more stringent regulation, it is becoming increasingly difficult to not only maintain compliance but to evidence it.

Post Office also wish to provide POCA transactions on the SSK. A number of approaches had been explored and one of these was to expand the current payment interface to support this. This payment interface is provided by YesPay, but they were unable/unwilling to provide the required support. An alternative where the YesPay solution is replaced by an Ingenico solution and that solution expanded to provide the necessary banking interfaces is described in this solution.

The adoption of such a solution for the SSK allows the use of point-to-point encryption (P2PE) immediately for payment and allows it to be introduced for banking and POCA immediately on the counter, once other changes are made (see [ARC/SOL/CSP/3291]).

## 2 Scope

This document covers the overall solution design. It does not describe the design of the Ingenico solution, stopping at the requirements of it.

The document also describes the responsibilities of the parties and covers the creation, maintenance and updating of the various items of reference data that control the solution.

The current implementation of payment on the SSK uses a third-party solution which handles the whole transaction and this solution will be no different. This makes payment much more like banking from the perspective of handling failure and recovery from it.

Part of the latest PCI standards is chain of custody, and therefore this is covered in the scope of this document, including key management and hardware replacement by engineering.



Accreditation and compliance to PCI standards are a specific requirement, so the elements that will affect this are in scope. The document therefore covers software maintenance and reference data and the control of change. Unlike the current solution where Post Office initiate and commission all changes, it is anticipated that there will be updates issued to ensure continued compliance, with timescales dictated by external bodies.

The parts of the Banking solution in the Horizon Data Centre are not being changed, and thus the version of the standards to which they comply will not be changed by this. While the changes here are intended to remove PCI data from systems where it is no longer required, it is unlikely that this will actually remove those systems from the scope of PCI audits. This results from a decision in a recent PCI audit which determined anything connected to a system carrying PCI data was within scope.

Outlines of the interfaces and parameters to the technical aspects of these are documented in appropriate AIS and TIS documents. Where relevant some of the details will be discussed here to give context, but the AIS and TIS will be the definitive source. The interfaces will be identified here and the corresponding documents cross-referenced.

Changes to the counter are covered by a separate document [ARC/SOL/CSP/3291].

Changes to the SSK and RTS are covered, insofar as they pertain to Fujitsu changes, are documented in [ARC/SOL/CSP/3173].

## 2.1 Timescales and Phasing

*Once a CT for implementation of the solution described in this document is approved, timescales can be confirmed.*

## 2.2 Requirements out of Scope

None identified.

## 2.3 External Dependencies

### 2.3.1 On Post Office

#### 2.3.1.1 PCI Compliance

PCI compliance is adjudged by Post Office and External QSAs. Post Office are responsible for PCI compliance. Post Office are responsible for satisfying themselves that this solution meets their PCI obligations and that it is acceptable to their internal and external QSAs.

If there are changes to PCI requirements, it is incumbent on Post Office to raise the necessary changes under change control procedures. Any such changes will be scheduled into the program and will impact on it in both time and cost.

#### 2.3.1.2 Network

Dependency on Post Office to arrange with Verizon for required networking in their domain, viz. network between HNGA and Ingenico.

#### 2.3.1.3 Deployment Plan

The changes delivered by this CT is part of the overall solution. Deployment of the overall solution is dependent on the replacement of the devices currently in the estate with devices which have been recycled through the Ingenico secure facility and loaded with the appropriate version of firmware. Post





Office own the relationship with the parties involved in this and thus have the responsibility to ensure this is planned and coordinated with these parties.

The deployment plan needs to ensure the integrity of the Chain of Custody is maintained and evidenced (see next two items).

#### **2.3.1.4 Pin Pad Lifecycle**

Post Office must ensure that such updates as are necessary are made to plans and processes relating to the management of pin pads from acceptance through to disposal, to reflect the new solution being deployed. This needs to ensure the integrity of the Chain of Custody of the devices is maintained.

#### **2.3.1.5 Inventory**

Post Office have responsibilities under PCI in relation to maintaining an inventory of pin pads. The processes for maintaining this will need to be updated in light of the changes made for this solution. The inventory itself will need to be updated and maintained to reflect the deployment of the recycled devices. The inventory will form a part of the evidence of the integrity of the Chain of Custody of the devices.

#### **2.3.1.6 End of Life Processes**

Post Office have a responsibility to ensure the disposal of all devices, including Pin Pads and keyboards, is managed. For Pin Pads, this needs to be consistent with the *Pin Pad Lifecycle*, see above.

#### **2.3.1.7 PCI, SRED, Magnetic Card Readers**

The current keyboards on the counter have magnetic card readers. This will impact on the PCI compliance of the solution. There is a dependency on Post Office to agree measures to bring about compliance.

#### **2.3.1.8 SSK**

There is a dependency on NCR to provide access to a working kiosk to Fujitsu (Ingenico) sufficiently close to the go-live version for accreditation activities to be progressed.

#### **2.3.1.9 Staff Training**

The user interface on the counter for banking transactions will be changed by the introduction of these changes. It is the responsibility of Post Office will to introduce this change to their counter staff with appropriate notice, briefings or training as they deem necessary.

### **2.3.2 On ComputaCentre**

ComputaCenter to provide SV&I and LST with a CC TYPE C BUILD that incorporates the Payment Service HNG-A Counter Application changes. ComputaCenter also has a dependency to supply LST with a CC TYPE D BUILD that incorporates all required Payment Service HNG-A Counter Application peak fixes. Without these dependencies being satisfied, SV&I functional testing will not be possible nor will LST sign-off of the Payment Service HNG-A Counter Application such that the EUC can then progress deployment into ATOS/POL UAT, then Post Office Model Office, then Live.

## **2.4 Design Assumptions**

The Ingenico iPP350 pin pad currently deployed on the SSK will support banking transactions, as does the same device on the counters. It does not currently support a certified P2PE scheme. This will require the device to be reloaded with firmware at Ingenico, in order to achieve the required provenance of the firmware and keys.





The following design assumptions have been made:

#### 2.4.1 Additional EMIS files received from Global Pay

GlobalPay send a number of EMIS files to the Horizon Data Centre each day to allow Horizon to reconcile payments made by credit and debit card across the Post Office estate.

It is assumed that Global Pay will send data for any given MID within the same EMIS file for all debit and credit card payments carried out during the migration, whether it is performed via Horizon or Ingenico.

However, it cannot be assumed that the MID and TID will be carried forward from the one service provision to the other. It is also unlikely that migrated and un-migrated counters data can be delivered together in the same EMIS file. Therefore it is assumed that the number of EMIS files to be received is increased during migration and will change again once migration is complete. The same applies for EPA file from AMEX.

#### 2.4.2 Transaction determined before card read

Moving the application which reads the PAN from the counter means that the transaction is started before the card is read. This requires that the clerk or customer decides what transaction they wish to do before starting it. This seems not unreasonable, since the customer has presumably arrived at the counter with this purpose already in mind, however, it may cause an error where the customer has inadvertently chosen the wrong card to use. The customer can still insert the card before the start of the transaction, it simply means the clerk will be required to select the transaction type and amount before the pin pad is asked to start the transaction. It is possible that the transaction may go online before the system detects that it is not permitted, but this will be handled in a similar fashion to other online declines, e.g. where there are insufficient funds.

### 2.5 Requirements

Requirements have been derived from Ref 4.

*A requirements catalogue needs to be produced and agreed in detail with POL. The final version of the requirements catalogue will be used as the basis for the implementation CT.*

### 2.6 Use Cases

This document introduces a new service for use by clients. Use cases document the interaction with a user and thus are not strictly relevant to a service of this type.

As clients are migrated to use this service, their user interactions will change, so consideration will need to be given to the counter and SSK operator prompt screens, as well as the pin pad prompt tables. In the case of the SSK, this will be the result of new functionality enabled by this service. In the case of the counter, the interaction with the clerk will change because the service has some differences in the way it works from the existing counter application which is tightly integrated with the pin pad.

For SSK, see [ARC/SOL/CSP/3173]. For other, future, clients, see the relevant client documents.

### 2.7 Non Functional Requirements

Any non-functional requirements are included in the spreadsheet at Appendix B.

### 2.8 External Interface Specifications

#### 2.8.1 Application Interface Specification (AIS)



An AIS will be produced describing the interface between the Ingenico AXIS component and a new service running in HBS; this new service will be responsible for relaying messages between the Ingenico AXIS component and the existing POCA Agent running in the Horizon Data Centre. This AIS has been allocated reference number REQ/APP/AIS/3265.

The specification for invoking the C3E component running on the SSK and the counter will be based on the current specification, available from Ingenico. The updates will cover the changes needed to support the POCA and other banking transactions.

## 2.8.2 Technical Interface Specification (TIS)

A new TIS is required to cover the connection between the SSK and the Ingenico Data Centre (to cover traffic between C3E and AXIS)

A new TIS is required to cover the connection between the Ingenico Data Centre and the Horizon Data Centre. This will cover traffic between AXIS and the new service running in HBS.

A new TIS is required to cover the connection between the Cancellation NRT service and the Ingenico Data Centre. This will cover the traffic from Horizon to Axis generated when a transaction has failed after approval by the pin pad or where a timeout has occurred.

## 2.8.3 Operating Level Agreement (OLA)

A draft OLA will be produced to provide a shape for the day to day running of the service.

## 2.9 Architectural Requirements

The solution will be designed to make minimal changes to the existing Banking infrastructure within the datacentre, subject to achieving the primary business requirements. Thus some change is unavoidable to reduce the PCI scope, e.g. around guaranteed reversals.

In the branch, the solution will use the pin pad to perform all relevant transactions and the pin pad will handle all of the PCI related data. The pin pad will exchange data with its data centre components in a form which protects any PCI data according to a certified scheme provided by Ingenico and will provide to the counter and SSK only permissible data for their use.

The design will minimise the number of interfaces between the Fujitsu and Ingenico domains and will seek to avoid or minimise data that has to be synchronised between the environments. Where this cannot be avoided, the design will seek to ensure that the mechanism employed allow any differences between the data held by the two domains to be handled gracefully and consistently. The period where such differences can persist will be designed to be minimal.

## 3 Solution Architecture

The solution will be delivered in a number of phases based on the requirements of Post Office. The first major phase (which in itself, will be phased) will deliver payment to the SSK. The second phase will be to deliver the remaining solution to support all banking and payment and certain other card based transactions, as detailed below (specifically ARC) at the counter. A third phase will include further pin pad based developments to cover Talexus and Quantum, if required.

It should be noted that much of the functionality currently implemented directly in the counter will now be transferred to an application running inside the pin pad. This removes much of the logic from the counter, thereby allowing the removal of the counter application from the CDE.

### 3.1 High Level Diagram



The diagram below shows the interactions necessary to support the Banking and Payment solution proposed. The interfaces between these components are the main focus of this diagram.

The Blue interfaces are existing interfaces which will remain unchanged, with the exception of IF09, which will be cease to be used with time.

The Yellow interfaces are ones which require change. Both the SSK and the counter use pin pad API's and these interfaces will change. The current proposal from Ingenico is to base the solution on the embedded version of their C3E product (C3E). This resides in the pin pad. A small driver resides in the client system which is connected over TCP/IP – on the diagram below, this is shown as C3Net, but is displaced to the Ingenico domain, however, it does reside in the client platform and IF02 is an internal connection.

The Green interfaces are new interfaces between HBS and the financial systems for the purposes of instigating recovery. Both RTS and PSS will have a role in recovery as detailed later. This interface is for use by the recovery process that will run within HBS.

The red interfaces are new interfaces, or new flows over existing interfaces.

The domains are coloured according to responsibility.

This diagram covers Payment and Banking for the SSK<sup>1</sup> and the counter.

Note that neither the Counter nor the SSK developments necessary to consume this service form a part of this design; these are covered in ARC/SOL/CSP/3291 and ARC/SOL/CSP/3173, respectively.

<sup>1</sup> Although only POCA is planned for the SSK; this will be controlled through ref data on the pin pad.



Post Office Payment Service

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

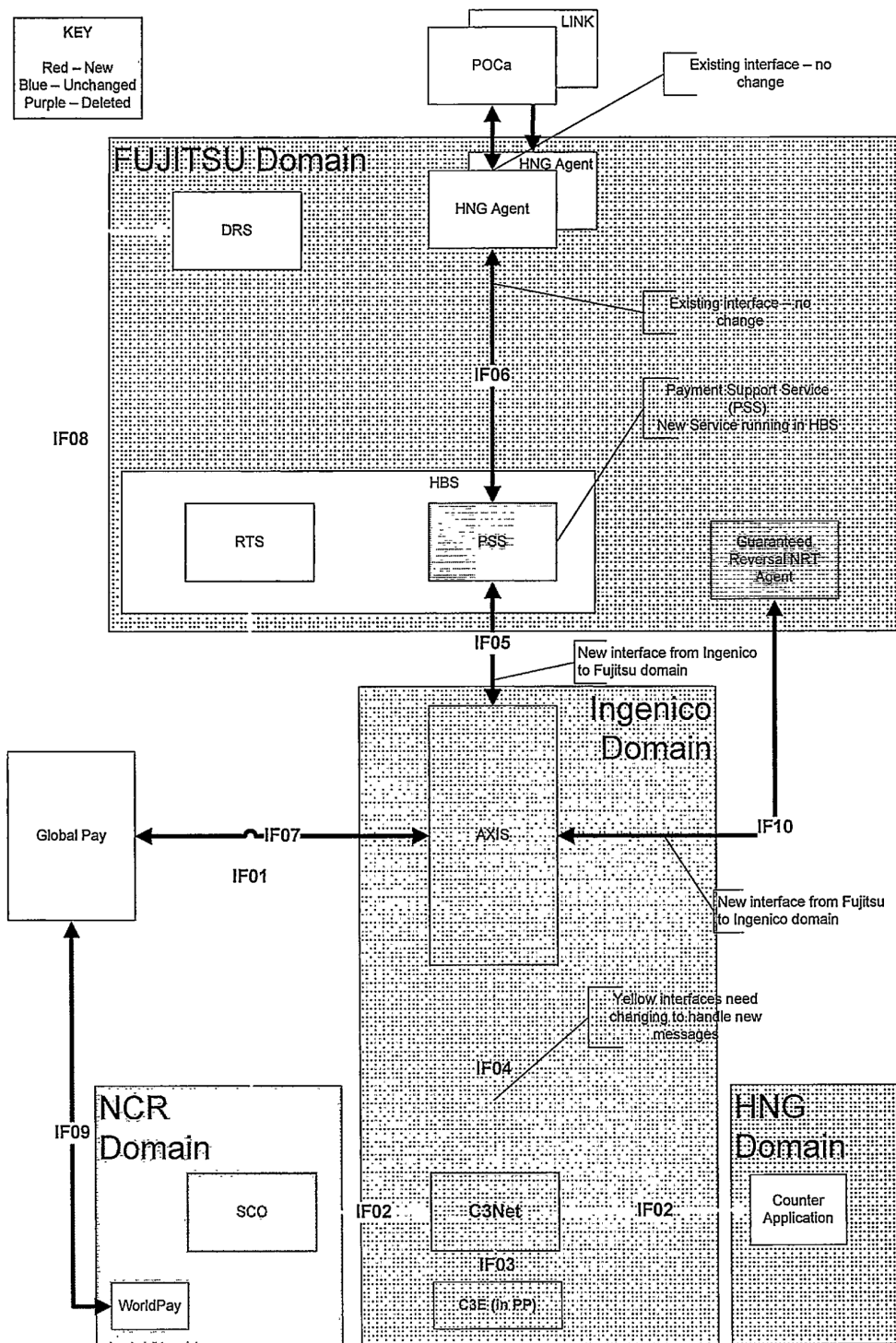


Figure 1 - Block Diagram





### 3.2 PCI Isolation

The pin pad is central to banking and payment transactions. The solution has to comply with a number of regulations handed down by PCI, EMV and the banks and schemes themselves.

The main intention of the solution is to isolate all of the PCI relevant parts of the solution from HBS, to avoid HBS and the rest of the Horizon Data Centre coming into the PCI scope<sup>2</sup>. Point-to-Point Encryption (P2PE) will be deployed to ensure the SSK and counter PCI scope are minimised. The use of P2PE requires keys to be present in the device to encrypt the cardholder data prior to it being transmitted from the device, which are injected in a Visa approved Ingenico Key loading facility. The corresponding decryption will be performed in an Ingenico data centre. In the case of payment transactions, these will then be forwarded to an appropriate MA or PSP.

POCA and other banking transactions will be forwarded to the Horizon Data Centre, where they will be received by a new service PSS which interfaces to the Agent layer. Here they will be handled with POCA and other banking traffic from the counters. PSS, which will be a separate HBS service, based on a BAL/OSR, will be stood up to handle this traffic. This will prevent PCI traffic that has come from the Ingenico data centre mixing with traffic through the remainder of the Horizon estate as far as PSS.

The next phase will be to remove the direct traffic from the counters by migrating to the C3E solution, and once this phase is complete, the agents and attendant hardware and software can be isolated from the rest of the Horizon solution, thereby enabling the rest of the solution to be removed from the PCI scope. However, this will require changes to the Horizon Data Centre infrastructure beyond the scope of this design.

It should be noted that this does not take account of any flows of PCI data brought into the system as a result of its capture by APADC scripts. These scripts are not under the control of Fujitsu Services, but they can capture PCI data and then cause it to be stored in the BRDB, passing through the BAL. The data will then be processed into host files and transmitted to the client of the APADC products.

### 3.3 Design Outline

The card transaction will be initiated by the counter or SSK invoking the C3E application within the pin pad. The invocation will include a number of parameters, including the type of the transaction (deposit, debit card payment, debit/credit payment etc.) and the amount.

C3E will display messages to the customer on the pin pad and manage the transaction to the point of requiring communication with the data centre. C3E will produce progress updates back to the SSK or counter, which can be used to update the main display, e.g. to inform the clerk so they can provide assistance.

The two diagrams below show a logical view of the transactions.

The first shows a payment transaction and the components involved. The transaction is similar both on SSK and Counter. The primary difference is that the counter performs the menu displays and user interaction prior to the initiation of the payment transaction, whereas the SSK interacts with HBS/RTS to arrive at this point. Similar, the last steps of recording the transaction in the Basket, while logically similar are clearly implemented differently.

The same considerations apply to the second diagram which shows a banking transaction. While there are a number of different banking transactions supported, they are logically identical at the level considered here, and thus the diagram applies equally for all types. The specific differences in transactions are handled within C3E and are not exposed to the SSK or counter.

For payment transactions on the counter only, some interaction may be required for cardholder signature or referrals. This is omitted from this diagram.

<sup>2</sup> Currently it is in scope for other reasons, but this is the first step to removing it.



## Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

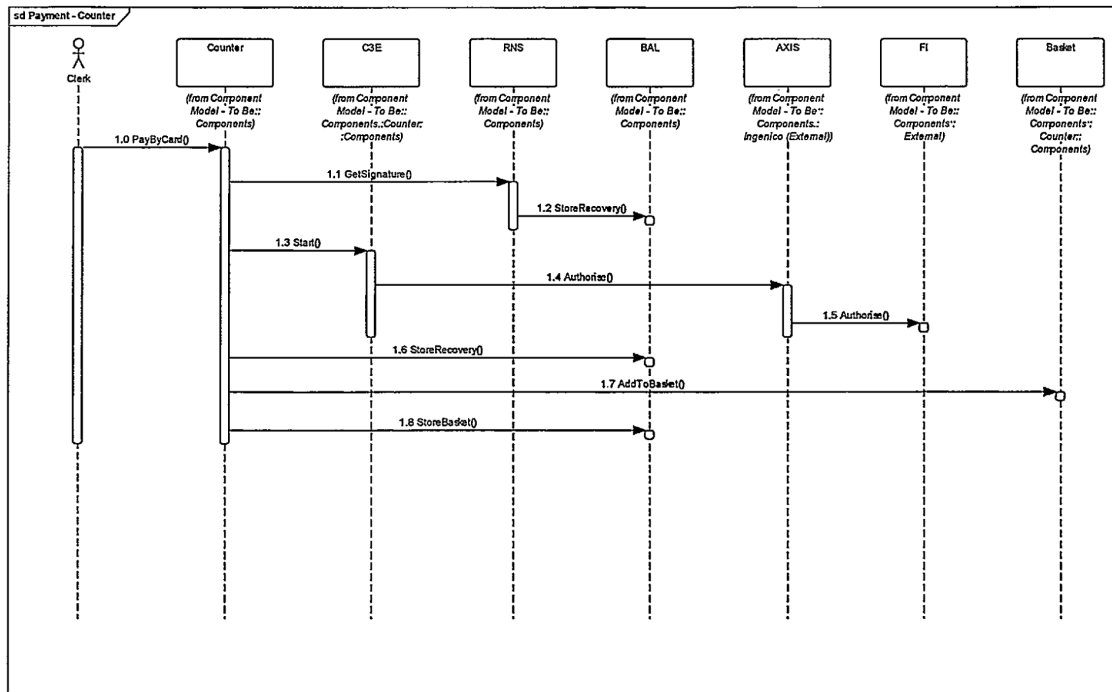


Figure 2 - Payment Interaction Diagram

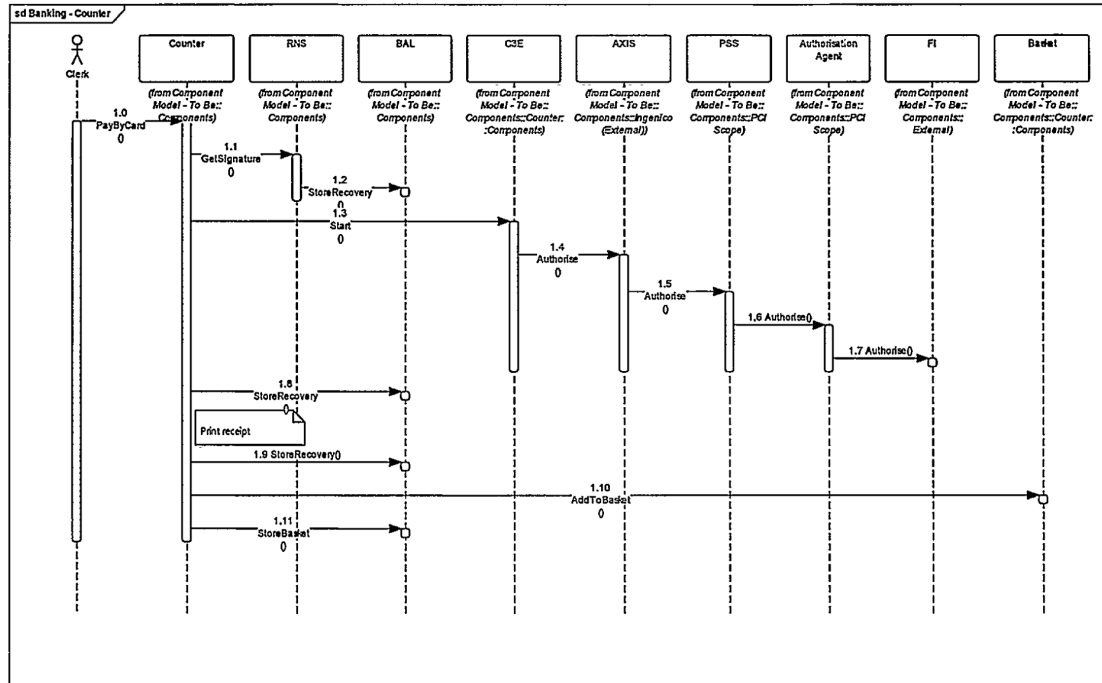


Post Office Payment Service

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



The diagram below shows the interactions for an SSK or counter performing a banking transaction (for SSK, this is likely to be limited to POCA). This is discussed in more detail later.



**Figure 3 - Banking Interaction Diagram**

The counter or SSK makes the request to the C3E application, which interacts with the customer and the card and will then make an online request. This is *tunnelled* through the SSK or counter. However, any PCI data contained in this is encrypted, so the PCI isolation is unaffected by this data passing through. The response received from the data centre is returned to the pin pad and the transaction concluded by the device. The response is passed back from the device; in the case of the SSK, it will then use this to complete the original AddLineItem or AddTenderItem request and resubmit it to RTS. RTS will return a basket entry reflecting the final outcome as recorded. RTS will also cause the recovery data to be updated and trigger any recovery actions required at that point. In the case of the SSK, the basket entry will be added to the basket. For the counter, similar actions will take place, with the counter adding the transactions directly to its basket. Where necessary, the counter will send appropriate messages to the BAL to update the recovery data held in the data centre.

The recovery process will monitor the outstanding recovery items and take appropriate action in respect of aged data according to a schedule to be agreed. It is likely that payment transactions could be timed out if not settled within a specified period (60 minutes).

Where the data a transaction is detected to have failed, i.e. the result is not received from C3E or the result now differs from that delivered by C3E, the cancellation of the transaction will occur via the data centre. This allows a single mechanism to be implemented which can manage failures detected in both the branch and centrally. It also avoids depending on C3E and the pin pad which and enables the implementation of a guaranteed, reliable mechanism.

**DN: Note: this is different from the existing system and in the case of a counter crash and recovery may result in a customer seeing a charge followed by a later refund. In the worst case, these may appear on different statements, and thus could lead to customer queries.**





In the case of banking, the same process will be followed, with the transaction cancellation going to Ingenico and being promptly returned to the Fujitsu PCI data centre. This allows a single mechanism to be used for all reversals without that mechanism having to understand transaction domain data.

If an attempt is then made to add an item to the basket which has been cancelled through timeout, then it will be rejected as failed (with an appropriate basket entry and ultimately receipts). It could then be retrieved, or the whole basket could fail, as appropriate.

The basket entry will contain no PCI data. The entry will be sent to the Branch Database as in the current solution and will be harvested from there to the TES. The TES will continue generate the REC files and therefore will continue to contain PCI data.

### 3.3.1 Network routing

The SSK is connected to the Horizon data centre to allow connection to HBS/RTS. It is also connected to the POMS LAN to allow connection through to YesPay, and in future to support connection to the Ingenico data centre.

With the implementation of the Post Office Towers model, responsibility for networking has passed from Fujitsu. The network routes are therefore covered by an external dependency. For HNGx, the traffic will be forced to the data centre by the existing VPN solution. Therefore, assuming there are still HNGx counters, the routes will also need take this into account.

The Network routes between Ingenico Axis and Fujitsu PSS and between Fujitsu Reversal NRT Agent and Ingenico Axis are internal to the solution and thus will be a Fujitsu responsibility.

A VPN will need to be established to connect from the core network to the Ingenico data centre. A further two VPNs will need to be established which will allow connection between the Ingenico data centre and IRE11/19. The first of these is the POL responsibility, the latter two are Fujitsu's.

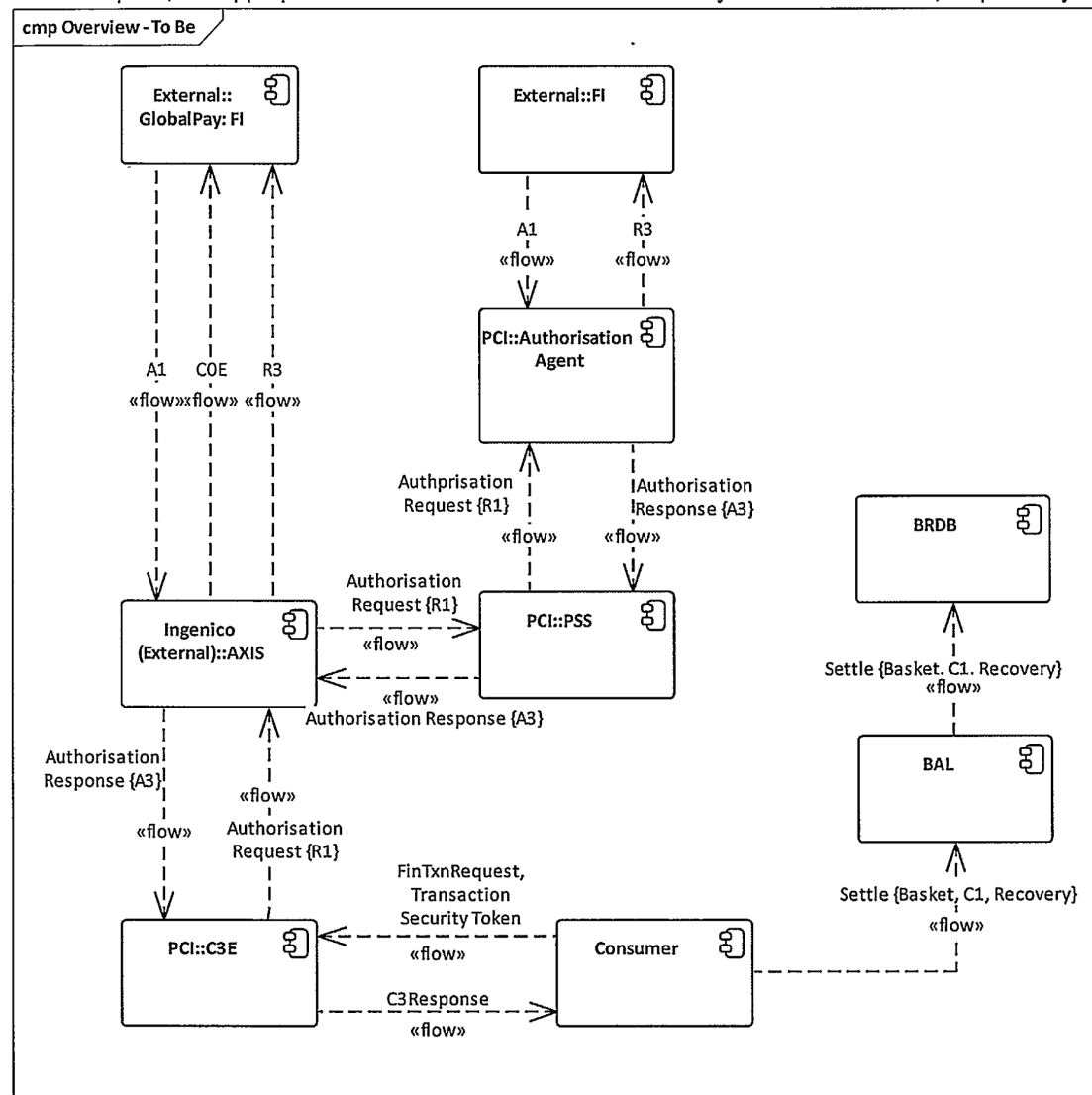
### 3.3.2 Component Overview

The following diagram shows the major architectural components of the solution. For both SSK and Counter, when a new transaction is required, then the reference number to be assigned will be created by RTS or the counter, respectively, and a signature obtained from a new service RNS, in the BAL. C3E will then be initiated to interface with the application within the PIN Pad. This will handle all aspects of the transaction, obtaining online authorisation and obtaining the funds.

In the case of banking transactions, the authorisation will be routed to the Fujitsu data centre to a new service, PSS, which will interface to the existing banking agents. This service will verify the signature obtained from RNS.



Once complete, the appropriate basket entries will be constructed by RTS or the counter, respectively.



**Figure 4 - Component overview**

At each stage as the transaction passes through the Horizon domain recovery data will be updated to reflect the currently known disposition of the transaction – see Figure 2 - Payment Interaction Diagram and Figure 3 - Banking Interaction Diagram, and the descriptions there.

### 3.3.3 Key Usage

The pin pad will contain 3 keys. All of these are generated and managed by Ingenico.

The P2PE solution has a key which is injected by Ingenico before delivery of the device to the field. This key is used to encrypt the cardholder data. The corresponding decryption key is held in the HSM in the Ingenico data centre to decrypt the cardholder data prior to its being sent to the MA, or across the Horizon Data Centre in the case of Banking, including POCA.



The PEK (aka the Banking key) is the key used to encrypt the online pin used (only) in POCA transactions. The corresponding decryption key is held in the Horizon Data Centre HSMs where the pin is re-encrypted under a key shared with the POCA host.

The TK is a transport key used to permit changes to the PEK without having to withdraw the device physically.

A fourth key may be required as the transport key for replacement P2PE keys. This will be documented once the detailed design and commercials have been agreed.

An administrative interface will be required to allow the replacement keys to be loaded if a key change is required to either the PEK or the P2PE keys. The replacement keys will be distributed and loaded in a similar manner to reference data.

As a part of the migration process, the devices currently installed on the counter and SSK will be replaced. Apart from a small buffer stock introduced to start the process, the devices will be recovered from branches, returned to the Ingenico secure facility and wiped completely. All of the devices will be loaded from a clean state with a new version of firmware and set of keys. This includes the Ingenico P2PE firmware signing key and all of the keys mentioned above.

Once in the field, the keys will be managed through the use of the Ingenico TMS application. This allows remote application of reference data, firmware upgrades and key replacement (with the probable exception of the P2PE firmware signing key).

### 3.3.4 Request and Authorisation Data

The cardholder data is encrypted according to an approved PCI scheme. The Ingenico data centre has knowledge of the key in the pin pad and so can decrypt the cardholder data.

For Banking transactions, this data is sent to the Horizon data centre, where it passes through a new service provided by PSS. This will check the signature against the data provided. If it is invalid, a decline response will be returned, otherwise, it will pass the request to the relevant banking authorisation agent. This part of the journey sees security checks performed on the pin block and its transformation from the internal domain encryption to the domain shared with the appropriate Financial Institution (LINK, POCA, or Santander). This is the same process as for the existing Horizon counter transactions. Once authorised (or otherwise) by the FI, the response will return by the same route to the C3E software.

### 3.3.5 Reference Data

The Ingenico product set includes an administration tool - TMS<sup>3</sup>. This will load reference data into the device, as well as firmware and keys. To do this the device must remain unused for a period. The administrative interface allows the client system to signal that this is a period when the system will be quiescent. This will cause the software to contact TMS and if there are outstanding updates, they can be downloaded. There is an option to indicate whether slow actions may be performed, such as firmware updates, to allow reference data updates in the day without having the penalty of the device being unavailable for an extended period.

## 3.4 Reconciliation processes

### 3.4.1 General

The data fed to the DRS will remain much the same as the current solution, as used for YesPay payment transactions. That is to say the amount of data available in these will be much reduced.

<sup>3</sup> Terminal Management System



GlobalPay and AMEX will be asked to deliver EMIA/EPA files with masked PANs. Where this is not possible, the EMIS file will be received into the PCI data centre, where the PAN will be masked before the data is passed over to the Horizon data centre.

Within the Horizon data centre, the EMIS/EPA files will be processed and loaded into the DRS and feed POLSAP as per the current solution.

### 3.4.2 Banking

Banking reconciliation will continue to be performed using the DRS. The feed to DRS will be reduced to the same content as for payment, and in particular PANs and any other sensitive data will no longer be delivered. This will remove all PCI data from DRS without impact on reconciliation.

TES is currently involved in collecting and processing the parts of banking transactions. Since it produces the REC files output to POCA and Santander, unless the PANs can be removed from these files, TES will continue to need the PAN in a form it can process to produce these files.

TES also receives the LREC file from LINK, which contains PANs. TES will therefore reside within the PCI data centre.

The reconciliation processes themselves do not need access to the PAN, and although there are reconciliation verification steps that check for consistency of the PAN on various records, these can be performed quite successfully with masked PAN. On this basis, it is intended that the DRS can stay outside the PCI scope. The data feed from TES to DRS will therefore contain no PCI data.

The feed from baskets on the counters and SSKs will no longer contain any PCI data, and the feed from DRS to TES will contain very little more than the amount, transaction type and the TransactionIdentifier.

## 3.5 Recovery

As noted above, recovery is an important topic, since failures may leave a difference between the bank or financial institution's view of the outcome of the transaction and the actual outcome. In any case where a transaction has been declined, there is no possibility of a difference of opinion, so action is only necessary where authorisation has been given and where the system fails before successfully completing the real-world effects of that transaction and recording the outcome. However, in all cases, it is necessary to record the final outcome of any transaction that has started to ensure both a complete audit trail and to ensure that reconciliation can be reliably performed.

Within the retail payment part, the Ingenico solution will submit the payment record at a batch submission point sometime after the successful completion of a transaction. If circumstances in the client require that payment not be taken, a cancellation will be initiated. In the absence of such a cancellation, the transaction will be submitted and payment to Post Office (or from Post Office in the case of refunds) will be made by the FI. The cancellation process will deal with the case where payment has already been requested, by raising a refund. The effect of this is that the payment solution now needs to handle recovery in the same way as banking, since as stated above, if no further action is taken after an authorisation request is sent, then the account concerned will be debited.

For banking transactions, the same logic applies. The difference is that the funds have already moved at the point the authorisation response was received. The reconciliation with the FI occurs only after the basket entry is settled in the current solution, and this will continue to be the case. The real-world effect in the Post Office can only occur once the corresponding basket entry has been secured, and this is managed by the existing recovery process in the client system. In the case of failure, when the recovery process completes, any outstanding TransactionIdentifiers that have been assigned to transactions can be identified; these correspond to transactions which were initiated, but which did not reach a stage where the result was secured; as such, they need to be cancelled, as the real world actions would not have been triggered. This then re-aligns the banking world view with the real world events in the branch. The facilities to manage this are provided here, but details of the actual use of this will be found in the corresponding client design: see ARC/SOL/CSP/3173 and ARC/SOL/CSP/3291.





Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

The recovery and therefore possible cancellation of a transaction, within Horizon, will only have limited access to data, and in particular not much more than the TransactionIdentifier, amount and transaction type.

The cancellation of a banking transaction will be initiated from the Horizon system based on the TransactionIdentifier only. This will be in the form of a synchronous call or message to PSS. The response will indicate either failure, such as *no such transaction*, or success, which indicates that PSS is now responsible for completing the action. In normal circumstances, once this call has completed, it may be assumed that the system will be put into a defined state as a result of the call.

Where the failure is detected within the counter or RTS, the cancellation will be sent to Ingenico for both payment and banking. For banking the effect of this is that the Ingenico system will send the cancellation to PSS. This provides a single unified solution for payment and banking, and for cancellations triggered from within Ingenico and from Horizon.

### 3.6 Removal of PCI data from systems

The result of the above is to remove flow of PCI data from all systems with the exception of:

1. TES
2. Authorisation Agent
3. Guaranteed Reversal Agent
4. PSS
5. REC/LREC agent(s)
6. Audit Server

And in particular, Horizon except banking and payment components listed above, will be clear of PCI data, plus DRS will be clear of PCI data.

This will only be true once all counters have migrated to the new solution and any remaining PCI data has drained out or been archived from the solution. No special steps are being implemented to expedite this. The audit records will continue to contain encrypted PCI data for at least 7 years, as required.

In the latest PCI audit, a decision was made by the QSA that the connections for Systems Management and Monitoring expanded the scope of PCI within the data centre. The decision identified a large number of systems that became connected to parts of the solution carrying PCI data and thus came into scope of the PCI audit. Further work will be required to reduce this scope. This is not part of this change.

## 4 User Interface

The user interface for this solution is provided by the SSK or Counter. This is documented in ARC/SOL/CSP/3173 and ARC/SOL/CSP/3291, respectively.

The user interface for the counter solution will change radically from the currently implemented interface.

### 4.1 Counter Dialogue

See ARC/SOL/CSP/3291.

### 4.2 SSK Dialogue

See ARC/SOL/CSP/3173.

### 4.3 Transaction flow on the PIN Pad



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

The client system will start the transaction on the PIN Pad by calling C3E. It is expected that C3E will retain control of the transaction until completion, or until certain key events requiring the clerk's intervention. Clerk intervention is required for referrals and for signature checking.

After the initial call to C3E, a number of callbacks will occur providing progress information, and in some cases requiring input. The example given in the documentation is for signature:

Client	Flow	C3E	Comments
Open socket			
EFT_BEGIN	→		Start a transaction
	←	EFT_BEGIN_CONFIRM	Acknowledge
	←	POS_DISPLAY	Display message on POS
POS_DISPLAY_CONFIRM	→		Acknowledge
	←	PRINT_REQUEST	Print a signature slip
PRINT_REQUEST_CONFIRM	→		
	←	POS_DISPLAY	Display message on POS
POS_DISPLAY_CONFIRM	→		Acknowledge
GET_KEY	→		Return response to C3E
	←	GET_STRING_REQUEST	Request input
GET_STRING_RESPONSE	→		Return input with response to C3E
	←	POS_DISPLAY	Display message on POS
POS_DISPLAY_CONFIRM	→		Acknowledge
	←	EFT_END	End of transaction
		Close socket	

The interface defined by C3E is due to change to accommodate the introduction of banking. The following sections detail the flow of data across the system to drive the banking transaction and the reconciliation process. This then highlights the information to be gathered at each stage and what needs to be passed to the next.

### 4.3.1 Note on Notation

The following sections use a notation to indicate the data passed from one system to another. This is based on the function notation. By way of example

**F:(X,Y)→(Z)**

Which means the function F is called, taking the values of X and Y and returning in response the value of Z. The actual form of the interface may not be seen as functional in the classical sense, but, since these are synchronous exchanges of information, this notation is adequate to explain the data exchanged at a high-level.

### 4.3.2 Client system

The client system is used directly (SSK) or indirectly (counter) by the customer to determine the transaction to be performed and the amount involved (which will be zero for some transactions, by definition). As a blackbox definition of the rest of the solution, the client interfaces to it with the following minimum logical definition

**DoBankTransaction: (TransactionType, Amount) → (Approved, Amount, (Description, Balance)\*)**

Where the system takes a Transaction Type and an Amount and returns an approval, the amount approved and zero or more balances with accompanying descriptions.



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

To aid identification of transactions and allow tracking and recovery of them, a transaction identifier will be obtained. In addition, a signature will be appended to the transaction, which will be across the transaction type, amount, receipt date and time<sup>4</sup>, and transaction identifier. This is intended to show the client was logged in at the time.

The transaction identifier and the signature will be obtained from the HBS, thus a call to this must be made first, by the client system. HBS will check the credentials of the user to ensure they are permitted to perform the transaction, and then issue the response accordingly.

**RNS.GetAuthorisation:**

(TransactionType, TransactionIdentifier, Amount, ReceiptDate, ReceiptTime, User)

-&gt;

(Signature)

The call to initiate the banking transaction must then be:

**C3E.DoBankTransaction:**

(TransactionType, Amount, ReceiptDate, ReceiptTime, TransactionIdentifier, User, Signature)

-&gt;

(Approved, AmountAuthorised, ReceiptDate, ReceiptTime, C1Detail, (Description, Balance)\*)

C1detail is a data structure containing data from the final stages of the transaction in C3E. This will be stored to the BRDB and sent to TES. No PCI sensitive data shall be returned in this structure.

### 4.3.3 C3E and AXIS

C3E will ask for the card, and perform the EMV phases of the transaction. This will lead to an online authorisation request being sent from C3E to AXIS, and thence to PSS. The internal requirements between C3E and AXIS are a matter for Ingenico, but will require all of the data required to drive the call to PSS. The interface described here will be definitively specified in REQ/APP/AIS/3265, and is included here for explanation only.

The call to PSS will be:

**PSS.AuthoriseBankTransaction:**

(MsgTime, MsgType, MsgVer, AgtTmOut, Application, AppVer, BranchId, CounterId, TransactionType, Amount, ReceiptDate, ReceiptTime, TransactionIdentifier, User, Signature, CurrencyCode, EntryMode, ClearPAN, HashedPAN, PIN1, PIN2, Track2, ICCData)

-&gt;

(AuthorisationResponseCode, AuthorisationCode, AmountAuthorised, ICCData, (Description, Balance)\*)

<sup>4</sup> If these are sourced from the client. If they are sourced within C3 and returned to the client, then they will not be known at the correct stage and will not be covered by the signature. Preference is for them to be sourced from the client, or RTS. If the latter, then the RTS.GetAuthorisation signature will change to show them on the output not the input.





A further call will exist to handle cancellation of transactions previously performed. This will only be accepted before the transaction has been confirmed through the client, e.g. by the basket being settled.

#### PSS.CancelTransaction:

(MsgTime, MsgType, MsgVer, Application, AppVer, BranchId, CounterId, ReceiptDate, ReceiptTime, TransactionIdentifier, User)

->

(error)

The interface will normally return a zero error status indicating that responsibility for the reversal has passed to PSS. Errors may be returned, for a variety of reasons, e.g. the transaction identified cannot be found.

### 4.3.4 PSS

PSS has an existing interface to the Agent that mirrors that used by the BAL. This is defined thus:

#### Agent.AuthoriseBankTransaction:

(MsgTime, MsgType, MsgVer, AgtTmOut, Application, AppVer, BranchId, CounterId, TransactionType, Amount, ReceiptDate, ReceiptTime, TransactionIdentifier, User, Signature, CurrencyCode, EntryMode, ClearPAN, HashedPAN, PIN1, PIN2, Track2, ICCData, Add1, Add4, Postcode, IssSchId, AgentHash, ClientId, RoutingGateway)

->

(MessageTime, MessageType, MessageVersion, ApplicationType, ApplicationVersion, TransactionIdentifier, BankTransactionId, AmountAuthorised, CurrencyCode, ResponseCode, AuthCode, (BalanceType, BalanceValue)\*, Fee, IssuerResponse, ReceiptText, SettlementDate, EncryptedCardData, ICCData( IssuerScripts, IssuerAuthenticationData), AgentDiagnostic, AgentError, AgentSLAInfo)

The implication of this is that the following fields have to be determined by PSS itself, since they will be unavailable on the interface from AXIS.

Field	How determined
Add1	Lookup on BranchId
Add4	Lookup on BranchId
Postcode	Lookup on BranchId
AgentHash	Function of BranchId
IssSchId	Lookup on BIN
ClientId	Lookup on BIN
RoutingGateway	Lookup on BIN

The cancellation message will need to be populated with all of the details from the original authorisation request message. This detail cannot be known in RTS because of PCI constraints, and for some classes of automatic recovery that may be required, where the only detail available is the TransactionIdentifier. These details can be recovered by using the T1, T2 message pair in the same way as counter recovery does in the current system.

#### Agent.CancelTransaction:



Post Office Payment Service



FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)

(MsgTime, MsgType, MsgVer, Application, AppVer, BranchId, CounterId, User, AgtHash, ClientId, RtngGwy, LclDte, LclTme, TransactionIdentifier, STAN, ConfAmt, CntSLA, CurrCd, EtyMde, IssSchld, ReqAmt, RespCd, TranType, TxnRsltCd, AuthCd, FeeAmt, SettDte, Qty, ExpDte, PAN, T2, EfctDte, IssNum, ICCData)

-&gt;

(error)

A success response is only taken as an indication that the cancellation is the responsibility of the guaranteed reversal agent

## 5 Information Management

Ingenico have an e-portal solution which will provide management information about both transactions and the pin pads. The pin pad information comprises the location inventory which is a requirement of PCI, and also drives the whitelist of devices accepted within the solution. This will enable the tracking of devices and it is envisaged this will be used as part of the future engineering management of the devices.

The transaction reporting will provide an adjunct and possibly a replacement in the longer term for the reports from DRS and TES. This is still to be investigated and further proposals will be developed under change control.

## 6 Network Infrastructure

This will be covered in more detail in network design documents and the appropriate AIS and TIS documents.

The basic outline of the network is provided in **Error! Reference source not found..** This is no change on the existing network, topology, but new links will be required. It is anticipated that these will be supported by a VPN across the Internet.

### 6.1 C3E to Ingenico Data Centre

The C3E solution has a small driver within the host system. This will establish a connection with the Ingenico data centre. The route for this will be via the POMS vlan to the datacentre and from there through the established VPN to Ingenico. Responses will be by the reverse route.

The network will be managed by Verizon and therefore the routing of traffic on the POMS vlan will be for them. However, for HNGx, the presence of the Utimarco VPN solution requires the data to be presented at the VPN servers and thus will need to be routed from there. The SSK does not use the Utimarco solution and thus the same consideration apply as for HNGA. Apart from these considerations, this routing is a matter for Verizon, or Post Office.

### 6.2 Ingenico Data Centre to PSS

Banking transactions will be routed to the PSS service across a second VPN. The PSS service will handle the interface to the banking agents and thence the FIs as documented elsewhere. The response will be transmitted in reverse across the same route.

### 6.3 Near Real-Time Cancellations to Ingenico Data Centre

Cancellation requests generated outside of the pin pad are sent from the solution to Ingenico, for both banking and payment transactions, when required. These use a near real-time mechanism. This will require travel across a VPN and this traffic could be either be routed over its own VPN or the VPN at 6.2 above.



## 6.4 Documentation

The network components will be documented within the TIS [DES/NET/TIS/xxxx].

## 6.5 Network Capacity

Capacity model will be developed to determine the network load in each leg. This will be shown here when developed. This will be based on existing traffic for payment and banking.

# 7 Compliance with Law and Industry Standards

## 7.1 Data Protection and Obfuscation (DPA/PCI)

It is intended that no personal data emanating from the card will be recorded within Horizon. The Payment Service components will be in line with normal industry practice and therefore should naturally conform to the data protection regulations. Since the GDPR will come into force after this solution is implemented, its impact upon the solution will have to be assessed and any amendments made as required. As a general principle it should comply from the start, despite the regulation not being in force, but until it is in force, interpretation of the regulation may not be settled.

As the introduction of this will provide no route for personal data into Horizon, there should be no need to consider any addition obfuscation of data. Any data provided out of the solution to Horizon will already be conformant, e.g. any PANs will be obfuscated prior to passing them to Horizon.

## 7.2 PCI compliance

PCI compliance will be a fundamental requirement of the solution. The solution implemented will be conformant and certified to meet the requirements of PCI P2PE, PCI SRED and PCI DSS (or PCI DSS-PA) as appropriate. This section will be updated once detailed design and commercials have been agreed.

It is a Post Office responsibility to verify with their QSA that the solution will meet their needs, to establish the scope of the overall solution that stays in PCI scope, and that this is acceptable for their purposes.

## 7.3 On-going Compliance

The parts of the solution concerned with card payment will be composed primarily of a COTS product and thus will remain compliant as the COTS parts of the solution are updated, provided any changes requiring action or permission from Post Office are progressed within the dates required.

The remaining parts of the solution are bespoke. As these will be constructed to Post Office specification, including the re-use of existing components of the current banking solution, these will be compliant on the day of release. Further changes will be under change control initiated by Post Office.



## 8 Security

There are a number of sensitive items managed by this solution and their security is paramount. These are discussed here, but the design is covered elsewhere. Network related security details are recorded in the TIS [DES/NET/TIS/xxxx], and design details may be found via that document.

### 8.1 Transaction security and replay protection

Each request from a counter or SSK to perform a banking or retail payment transaction will require the issue of a unique identifier for tracking recovery. This identifier will be issued from the datacentre, and can only be issued to a device which has logged on. As part of logon, the device is checked to ensure it is known.

Where a banking transaction is being performed, the authorisation request has to bear a valid identifier for the device requesting the authorisation. This same identifier is used to associate the captured online pin with the transaction, thus ensuring that the encrypted pin block can only be used on this request, and hence only used once.

The existing banking agents will be used to perform later parts of the authorisation and their current replay protection mechanisms will prevent the same transaction being submitted more than once.

### 8.2 Key protection

This does not cover the keys used in the network components of the solution. For details of these see [DES/NET/TIS/xxxx].

Two active keys will be in use by the application components of the solution. The PAN and other sensitive transactional data will be protected using Point-to-Point Encryption (P2PE) according to an approved scheme. This will ensure the data is encrypted from the pin pad to the Ingenico data centre using a key held in the pin pad and known only inside HSMs in the Ingenico data centre. The key is thus only known within tamper evident devices compliant with the P2PE standard.

Encryption giving equivalent protection will be used to transfer the data to the banking servers.

The online pin entered by the user is encrypted within the pin pad using a key held there and known to the HSMs in the Fujitsu data centre. This is exactly as for the current banking solution. This is compliant to the relevant security standards, including X9.24, ISO11568 and LIS security standards.

Any attempt to tamper with the pin pad in an attempt to recover the keys will destroy the keys with it and render it useless. Such a device has to be returned to Ingenico.

#### 8.2.1 Key Change

Should the Pin Encryption key need to be changed, there is a secure mechanism in place to ensure that this can be done. The new key is encrypted under a unique key known to the device. Only the correct device can load the key. Each key has an identifier which is sent with the transaction, part of which is used to indicate a common series number for the whole estate. The datacentre will only accept keys that are from the one or more current live series. On start-up of the counter or SSK, the loaded key is checked to ensure that it will be accepted. Where a key has to be retired as an emergency, e.g. because of a suspected compromise, this mechanism will prevent the device from being used until a new key has been loaded.

A similar mechanism will be in place for the change of the P2PE key.

The keys used to encrypt the updated keys while in transit cannot be changed without returning the device to Ingenico.





## 8.3 Device Security

On each start-up of the SSK or counter, the attached pin pad is assessed to determine whether it is the correct device, whether it has the correct keys loaded and whether the firmware is up to date. If any of these checks fail, the device cannot be used for transactions until this has been rectified (see below). This is the current behaviour.

With the implementation of P2PE, these checks may not be deemed as necessary for device security, since any connected device must contain the correct key, or it will fail every transaction. However, such a device would still be used by customers to enter pins, which could then be captured by an invalid device, and thus action needs to be taken to verify the device nonetheless.

DN: ideally, the device should be tested at intervals to ensure that it not only reports a valid key identity, but that it actually contains a valid key. The most obvious time to verify this is from the results of every transaction performed, with a response indicating an invalid key was used causing the device to become untrusted and thus unusable.

When a new device is installed, the engineer must run an installation process which uses the trust established in the engineer's logon to associate the device to the counter or SSK. The device will not be usable for transactions if the firmware or keys checks fail. The installation process will force an immediate refresh of keys or firmware if required.

DN: A pre-requisite to load a new key is that there is an aged, but otherwise valid key in the device, as well as the correct transport key. Keys cannot be loaded by a bogus device, since it will not have the correct transport key to decrypt the key and the process will fail. This would leave the device disabled.

DN: the current process does not allow the PPID part of the key identity to be changed by the remote key loading process. The factory key loading process insists on it.

This is based on the design of the existing device protections and processes, but it is assumed the new firmware will offer equivalent protection and processes.

Each time the client system connects to the C3E software in the pin pad, checks are made for firmware, reference data and key updates. If they are found, then these are downloaded prior to the device becoming available. There are options on the connect command to suppress the downloading non-critical items, which will be set for connections established during the working day. Overnight the client will disconnect and re-establish a connection with the options to suppress unset so that updates can take place when they are least likely to disrupt normal business.

The only processes that will interact with a device which has not been installed, are the regular security checks on the device, which will of course leave it disabled, and the installation process run by the engineer, previously described.

## 9 Resilience and Availability Strategy

### 9.1 Capacity

The three components that are additional to the current solution are the network link to the Ingenico data centre, the link back for banking and the Ingenico data Centre itself.

The links can be sized for the volume of traffic carried by the current networks. The leg from the branch estate to the Fujitsu core network will carry no more data (subject to minor variation in message size and content) than for banking and payment transactions today.

The network links and the Ingenico data centre will be sized as required for the workload.

### 9.2 Availability



The availability will be commensurate with the current Horizon availability. The additional components are intended to have higher availability than Horizon's currently contracted availability.

### 9.3 Recovery

For the detailed design of this, see elsewhere.

Recovery will be mediated by the issue of a serial number from the data centre to any terminal performing a banking or payment transaction. The status of this transaction will be updated whenever a change of status is available. If the transaction is not completed within a reasonable time, it may then be cancelled and if required reversed. Reversal is only required where there is a financial effect to the transaction (i.e. the amount is non-zero) and the decision the FI may have taken was an approval and the transaction has been declined.

Recovery will attempt to record the transaction with the correct status and this may depend on the environment in which the transaction is being performed. In the case of the SSK, a POCA transaction can only become effectively completed at the completion of the whole session, and thus unless the basket completes, the transaction will be deemed to have failed and will be reversed if necessary.

## 10 Performance and Scalability Strategy

The solution is based on the existing banking solution, but the new parts must be capable of achieving the same performance.

### 10.1 Payment

The Ingenico solution is designed to handle the additional capacity and more. The network traffic generated through the existing network will be replaced by equivalent traffic and thus the capacity of this should be adequate. The remaining parts of the workload generated by the new solution is commensurate with that already handled, and in many cases will be identical.

### 10.2 Banking

The changes to banking at a high-level amount to the diversion of the acquiring messages via Ingenico. The performance and capacity of the solution is therefore as required, with the exception of PS which is new. This will be based on the same sizing as the BAL, which already handles this traffic and has adequate capacity.

### 10.3 Network

The network connections to and from Ingenico will be sized according to current traffic predictions. Some additional latency may be introduced as a result of the diversion to Paris and the cryptographic operations involved in the P2PE scheme. It is not anticipated that these will be significant, as they are already present in the Payment solution offered by Ingenico.



## 11 External Documents

The following external documents will be updated by Fujitsu.

Reference	Version	Date	Title	Comments

Table 1 – External Documents

## 12 Testing Strategy

The solution will be constructed in 2 main phases. The first of these will deliver the components to support card payment on the SSK. The second will deliver Banking, card payment and ARC on the HNGx and HNGA counters.

Accreditation of the solution with GlobalPay will be performed by Ingenico, with support from Fujitsu. Banking and ARC accreditations will be the responsibility of Post Office and normally handled by ATOS. These activities will be supported by Fujitsu and Ingenico as required.

## 13 Acceptance Strategy

No deviation from standard acceptance is expected.

Accreditation of the card payment solution is in scope of acceptance.

Accreditation activities associated with Banking and ARC, while supported by Fujitsu, are outside the scope of acceptance.





## 14 Service Introduction and Migration Strategy

### 14.1 Horizon Data Centre changes

Whilst the end goal is to introduce a 'PCI data centre' which will be separated from the 'remainder' this will be achieved through a number of phases, not all of which are covered by this design. Logically the 'PCI data centre' will contain the Ingenico components and a number of Fujitsu platforms as illustrated in the diagram below.

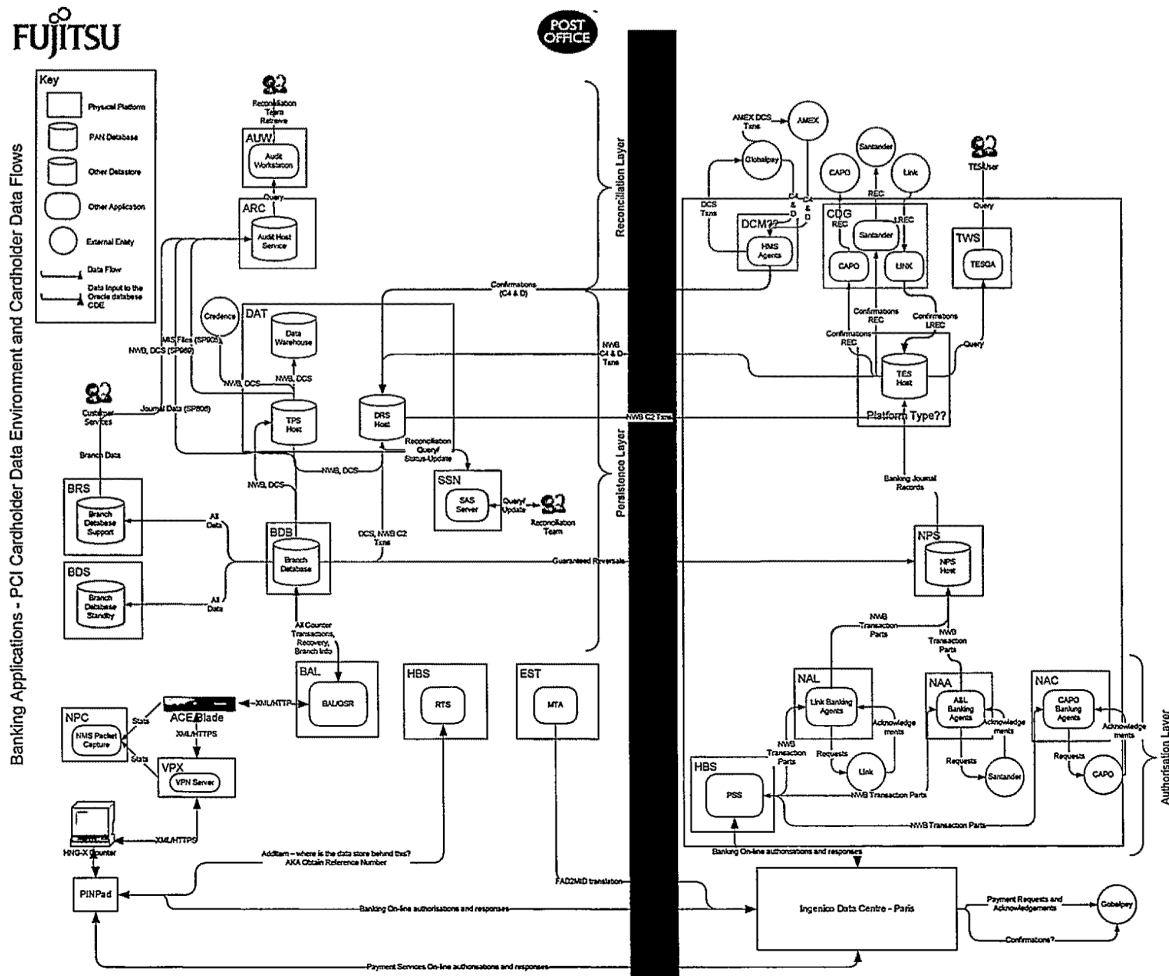


Figure 5 –Future PCI data centre (logical)

In the diagram above elements to the right of the red line are in the future 'PCI data centre' and those to the left are not.



In the first implementation of the Payments Service steps will be taken to sanitise the interfaces across the red line removing flow of PCI data through platforms such as BAL, BRDB and DRS, although they will remain connected to the PCI CDE.

Further phases will be required to increase the separation of the 'PCI data centre'.

It should be noted that this does not take account of any flows of PCI data brought into the system as a result of its capture by APADC scripts. These scripts are not under the control of Fujitsu Services, but they can capture PCI data and then cause it to be stored in the BRDB, passing through the BAL. The data will then be processed into host files and transmitted to the client of the APADC products.

## 14.2 EMIS files

The Payment transaction performed through the Payment service will be reported through EMIS files from GlobalPay as normal, in the same way as for YesPay. This may require an additional processing cycle to process these. However migration is straightforward in that the number of transactions in the one will increase and the number in the other will decline. The end stage is that the YesPay file will be empty and will stop being sent.

All the new devices on SSK will be allocated new MIDs and TIDs. This will require some consideration of the process, but from a migration viewpoint, the whole estate will exist in both places, but with only one in use at any time.

For counters, the MID and TID will be retained.

Since the SSK is an unattended device, it may not be possible to allocate the same MID to it as the counter; this is something which is up to Global Pay to decide. The rules on the allocation of MIDs to EMIS files are also down to Global Pay, so the number of EMIS files which will be required is not yet known.

For Amex transactions, the equivalent is the EPA file, and Amex will determine the rules on the allocation of MIDs to these. The number of files required to be handled will be determined by the application of these rules by these bodies and will need to be determined as a part of the more detailed design of the solution.

Since the banking transactions will go through the same process in the data centre, the change will be a shift in the numbers of transaction arriving by the different routes. There will be a corresponding difference in the data provided on the transaction messages.



Post Office Payment Service


FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)




## 15 Appendix A Outstanding Design Issues

*[This appendix lists any outstanding design issues. A suggested form of words and method is given below]*

There are also a number of issues identified in this document.

A number of areas of in the document require clarification. These are marked in yellow or  highlight in this working draft (as indicated):

1. Yellow highlight indicates further investigation required within Fujitsu Services or significant bits of text to be produced
2.  indicates a clarification of requirements is needed from Post Office Limited.

Wherever possible a working assumption is recorded.

*There may also be a number of minor comments that require resolving, made in a distinctive style like this.*



Post Office Payment Service

FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE)



## 15.1 A.1 Issues (on POL/3rd Parties)

### ISSUES ON POL

Section	Issue	Action	On	Priority
	What do receipts look like in the various Use cases?			

Table 2 – Outstanding Issues on Post Office Ltd/Other Suppliers

## 15.2 A.2 Issues on FJS

### ISSUES ON FJS

Section	Issue	Action	On	Date

Table 3 – Outstanding Issues on Fujitsu Services

## 15.3 A.3 Issues Resolved

### ISSUES RESOLVED

Section	Issue	Action	On	Date

Table 4 – Issues Resolved

o