CONFIDENTIAL

SCHEDULE B4.3

EXISTING CENTRAL AND TELECOMMUNICATIONS INFRASTRUCTURE

Version History

Version No.	Date	Comments
1.0	31/08/06	Agreed version as at date of signature of CCN 1200
1.1	26/09/06	Minor corrections by PO
1.2	11/10/06	Further minor corrections by FS
1.3	19/01/07	Further minor amendments.
2.0	25/01/07	Baseline copy of 1.3
2.1	13/05/09	Applying changes as per CCN1258
6.0	06/07/09	Moving all schedules to V6.0 as agreed with Fujitsu
7.0	26/04/10	Moving all Schedules to v7.0 as agreed with Fujitsu
8.0	21/02/12	Moving all Schedules to v8.0 in accordance with CCN1294d
9.0	13/01/14	Moving all Schedules to v9.0 in accordance with CCN1349
10.0	10/09/15	CCD reference updates and moving all Schedules to v10.0 in accordance with CCN1506
11.0	31/03/16	Applying changes as per CCN1427 and moving all Schedules to Version 11.0 as per CCN1604
12.0	03/07/17	Moving all schedules to V12.0
13.0		Updating as per CCN1616b and CCN1617a and moving all Schedules to v13.0

SCHEDULE B4.3

EXISTING CENTRAL AND TELECOMMUNICATIONS INFRASTRUCTURE

1. INTRODUCTION

1.1 This Schedule B4.3 provides an overview of the Horizon Service Infrastructure and the Horizon Infrastructure Services that Fujitsu Services shall provide to Post Office in order to deliver the Horizon Applications and thereby provide the HNG-X Services from the Amendment Date until Trigger Point T5 (Data Centre Ready for HNG-X).

1.2 This Schedule B4.3 shall cease to have effect at Trigger Point T5 (Data Centre Ready for HNG-X).

1.3 The Horizon Service Infrastructure comprises the:

1.3.1 Horizon Branch Infrastructure, the provisions relating to which are set out in Schedule B3.4;

1.3.2 Horizon Central Infrastructure; and

1.3.3 Horizon Telecommunications Infrastructure.

1.4 The Horizon Infrastructure Services provide the functions and capabilities of the Horizon Service Infrastructure (used to deliver the Horizon Applications) and comprise the OPS and the TMS.

1.5 The provisions of this Schedule B4.3 shall not apply in respect of the Horizon PostShop Infrastructure which does not comprise Horizon Branch Infrastructure, Horizon Central Infrastructure or Horizon Telecommunications Infrastructure as defined (accordingly it does not form part of the Horizon Service Infrastructure). The PostShop Infrastructure is detailed in CS/SER/027 PostShop Service description.

2. HORIZON CENTRAL INFRASTRUCTURE

2.1 Subject to paragraph 3.4, Fujitsu Services shall provide all equipment at the Data Centres necessary to provide the Services. This equipment, including the telecommunications equipment, shall have sufficient capacity to meet the business volumes as set out in the CCD entitled “Horizon Capacity Management and Business Volumes” (PA/PER/033).

2.2 The CCD entitled "Core System Release Asset Register" (CS/REP/045) **[This is no longer a CCD]** contains an inventory of the hardware and software to be used to provide the host and network facilities of the Horizon Service Infrastructure and located in the Data Centres as at 24 September 1999.

2.3 From the Amendment Date until Trigger Point HNG-X Project Workstream X3 (HNG-X Pilot and Acceptance), Fujitsu Services shall maintain hardware and software in relation to the Horizon Service Infrastructure providing, as a whole, equivalent capability to those listed in the CCD entitled "Core System Release Asset Register" (CS/REP/045). Such hardware and software shall constitute the "Horizon Initial Central Infrastructure".

2.4 Fujitsu Services shall in addition maintain all increases in the capacity of the Horizon Services Infrastructure which have been made at the request of Post Office.

2.5 Fujitsu Services shall specifically retain all hardware and software provided to a particular Post Office specification, save that Fujitsu Services may substitute identical replacements for such hardware and software.

2.6 Fujitsu Services may replace, upgrade, remove or decommission hardware and software from time to time comprised in the Horizon Service Infrastructure provided that it continues at all times to comply with its obligations in paragraphs 2.3, 2.4 and 2.5 (unless agreed otherwise under the Change Control Procedure).

2.7 Fujitsu Services' SMS software shall monitor installed PIN Pads and detect PIN Pad failures.

3. HORIZON TELECOMMUNICATIONS INFRASTRUCTURE

3.1 Communications Access Methods

3.1.1 The Horizon Telecommunications Infrastructure shall use one or more of the following communications access methods between the Horizon Branch Infrastructure and the Data Centres:

3.1.1.1 Integrated Services Digital Network (ISDN);

3.1.1.2 Integrated Satellite Business Network (ISBN), generally referred to as Hughes VSAT, , which shall be replaced by BT Enterprise VSAT on a Branch by Branch basis on commencement of Associated Change Workstream A3 (Branch Network Changes) and shall be fully withdrawn on completion of Associated Change Workstream A3 (Branch Network Changes);

3.1.1.3 Public Switch Telephone Network (PSTN) as part of the data recovery service;

3.1.1.4 Asymmetric Digital Subscriber Line (ADSL);

3.1.1.5 frame relay, which shall be replaced by the VSAT on commencement of Associated Change Workstream A3 (Branch Network Changes);

3.1.1.6 Branch Network Resilience (BNR), which shall be withdrawn on a Branch by Branch basis on commencement of Associated Change Workstream A7 (Branch Router Rollout) and shall be fully withdrawn on completion of Associated Change Workstream A7 (Branch Router Rollout);

3.1.1.7 IP Stream, which, if it becomes available, shall be introduced on a Branch by Branch basis on commencement of Associated Change Workstream A7 (Branch Router Rollout); or

3.1.1.8 General Packet Radio Service (GPRS) / Enhanced Data GSM Environment (EDGE) which shall be introduced on a Branch by Branch basis on commencement of Associated Change Workstream A7 (Branch Router Rollout).

3.1.2 There may be restrictions on the size of the Branch that can be supported on some technologies. Any such restrictions will be set out in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033).

3.1.3 The backup network is designed to cater for failures of the primary network at individual Branches and not for a total failure of the primary network at all Branches. Any capacity limits for the backup network will be set out in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033).

3.2 The Horizon Telecommunications Infrastructure shall include capability to enable connection between the Data Centres and Post Office systems or Client systems. The style of connection and operation may support real time transaction dialogues and/or bulk file transfer as required by the relevant Horizon Application specified in Schedule B4.2.

3.3 Fujitsu Services shall be responsible for provision of, security of, and management of the communications link between the Data Centres and Santander (which for the purposes of this Schedule shall include the physical routers, encryption devices, file transfer management servers and associated cabling), subject to Post Office complying with (and ensuring that any third party Post Office uses for siting or storage of such equipment complies with) the following:

3.3.1 provision of a suitable physical operating environment for Fujitsu Services' equipment used for or in connection with the communications link including the following:

3.3.1.1 ensuring the physical security of all equipment which is located on Post Office and/or any such third party's premises to protect against unauthorised access; and

3.3.1.2 provision of environmental conditions as reasonably required by Fujitsu Services.

3.3.2 permitting Fujitsu Services to gain access (at reasonable times and on reasonable notice) to all locations where such equipment is held or is to be installed, in order to enable Fujitsu Services to effect or procure the installation, maintenance, repair, renewal and support of such equipment.

3.4 Post Office shall be responsible for procuring the provision of, security of, and management of the communications links between the Data Centres and CAPO and LINK respectively (which for the purposes of this schedule shall include the physical routers, encryption devices, file transfer management servers and associated cabling) in accordance with and subject to paragraph 3.5, subject to Fujitsu Services complying with (and ensuring that any third party Fujitsu Services uses for siting or storage of such equipment complies with) the following:

3.4.1 provision of a suitable physical operating environment for CAPO and LINK equipment used for or in connection with the communications links including the following:

3.4.1.1 ensuring the physical security of all equipment which is located on Fujitsu Services and/or any such third party's premises to protect against unauthorised access; and

3.4.1.2 provision of environmental conditions as reasonably required by CAPO and/or LINK;

3.4.2 permitting CAPO and/or LINK (including their respective contractors) to gain access (at reasonable times and on reasonable notice, and subject to paragraph 3.5) to all locations where such equipment is held or is to be installed, in order to enable Post Office to effect or procure the installation, maintenance, repair, renewal and support of such equipment; and

3.4.3 any reasonable request for co-operation and/or information made by Post Office from time to time, where the provision of such co-operation or information is necessary to enable Post Office to perform the Post Office Communications Links Services.

3.5 Post Office shall, in relation to paragraph 3.4, be responsible for ensuring that:

3.5.1 the Post Office Communications Links Services are carried out promptly, efficiently, diligently and professionally, and with all reasonable skill and care;

3.5.2 it obtains an undertaking from each LINK and CAPO that its respective employees, servants, agents or sub-contractors engaged to perform the Post Office Communications Links Services:

3.5.2.1 keep confidential, and do not disclose to anyone else, any Confidential Information of Fujitsu Services disclosed by or obtained from Fujitsu Services in the course of performing the Post Office Communications Links Services;

3.5.2.2 use such Confidential Information only to the extent reasonably required to perform the Post Office Communications Links Services; and

3.5.2.3 return such Confidential Information held in tangible form to Post Office, and irretrievably delete or destroy all such information held in electronic form, on termination or expiry of that party's obligations in respect of the Post Office Communications Links Services, other than as required by law;

3.5.3 it or any third party engaged by it to perform the Post Office Communications Links Services complies with any reasonable instructions and/or requirements (including without limit any reasonable instructions and/or requirements relating to Data Centre security) given to it by Fujitsu Services from time to time; and

3.5.4 the communication links between the Data Centres and CAPO and LINK (respectively) shall have sufficient capacity to meet Post Office's business volume requirements from time to time.

3.6 Post Office shall fully indemnify Fujitsu Services in respect of any personal injury or loss of or damage to Property incurred by Fujitsu Services, its contractors or their respective employees and authorised agents to the extent that such personal injury or loss of or damage to Property is caused by a Default of Post Office, its employees, agents or contractors in connection with the performance of the Post Office Communications Links Services.

4. OFFICE PLATFORM SERVICE

4.1 Purpose

This paragraph 4 details the functions and capabilities provided by the OPS that shall be supplied by Fujitsu Services. The OPS is provided using the Equipment installed in Branches which enable the Horizon Applications to operate in accordance with the functionality described in Schedule B4.2.

4.2 Overview

4.2.1 Fujitsu Services shall, in each Branch, install the Equipment used to provide OPS, and provide OPS, subject to the limits specified in Annex A to Schedule D1.

4.2.2 Two categories of Counter Position configurations shall be provided:

4.2.2.1 a range of standard configurations (as specified in the CCD entitled "Counter Hardware Design Specification" (BP/DES/003)) which shall be suitable for the majority of Branches; and

4.2.2.2 a mobile configuration, as defined in the CCD entitled "Introduction of the Mobile Configuration" (CR/SPE/025), which shall be installed in Branches to the maximum number described in Annex A to Schedule D1.

4.3 General Service Description

4.3.1 Demonstrations and marketing

Fujitsu Services shall provide OPS Equipment which shall be required to demonstrate and market office platform services to Clients and prospective

Clients. The Equipment that is required shall be set out in marketing plans as agreed jointly between Post Office and Fujitsu Services from time to time.

4.3.2 Appearance of the Equipment within OPS

4.3.2.1 With the exception of PIN Pads, the standards for equipment livery to be used within OPS are defined in the CCD entitled "Counter Hardware Design Specification" (BP/DES/003). The standards for equipment livery for PIN Pads are defined in the CCD "PIN Pad Product Specification" (NB/PDN/010).

4.3.2.2 The procedures required to maintain the appearance of the Equipment shall be minimal and capable of being undertaken by the local Branch Users. It shall be comparable to the cleaning required of any desk-based office computer system.

4.3.3 Health, Safety and Legal obligations

All Equipment used to provide OPS shall comply with the health, safety and legal requirements laid down in Schedule A4.

4.3.4 Equipment Environmental Considerations

All Equipment used to provide OPS shall comply with the Equipment environmental considerations laid down in Schedule A4.

4.3.5 Continued Support of Operating Systems, Middleware and Horizon Applications Software

Fujitsu Services shall fully support the Software in the Horizon Service Infrastructure during the life of the elements of Horizon Service Infrastructure on which such Software is utilised in providing Services.

4.3.6 Capabilities of OPS

4.3.6.1 Fujitsu Services shall provide Horizon Service Infrastructure appropriate for each Branch.

4.3.6.2 Fujitsu Services shall install and support Horizon Service Infrastructure provided as mobile counter configurations, in accordance with the limits set out in Annex A of Schedule D1, where requested by Post Office.

4.3.6.3 In each Branch, at each Counter Position PC, OPS shall comprise Equipment as specified in the CCD entitled "Counter Hardware Design Specification" (BP/DES/003). The capabilities of this equipment shall comply with the manufacturers specification.

4.3.6.4 Fujitsu Services shall ensure that all automated Counter Positions shall have the capability to support the use of PIN Pads (PPR010).

4.3.7 Ability to Provide Authorisation to Post Office Products

Infrastructure Services and Horizon Service Infrastructure shall support authorisations for Post Office products through access to computer systems which are external to Post Office Services or are within Post Office Services.

4.4 Availability

4.4.1 User access to OPS

4.4.1.1 Users may only log-on to the OPS in their Branch in accordance with their defined role. Any access to data or services outside of that Branch is controlled exclusively by the relevant counter application.

4.4.1.2 Access to OPS and Post Office Services offered via OPS to Users working in the Branches shall be controlled by a mechanism conforming to the CCD entitled “HNGX-UI Style Guide” (DES/APP/STD/0001) (formerly “Horizon Office Platform Service Style Guide” (SD/STD/001)), offering multiple access levels and providing specific identification of each User. An exception to this is the Mails Application which does not conform to the “HNGX-UI Style Guide” (DES/APPS/STD/0001) (formerly “Horizon Office Platform Service Style Guide” (SD/STD/001)).

4.4.1.3 Authentication of all Users logging on to the OPS in the Branch shall be undertaken by the elements of Horizon Service Infrastructure on which OPS is based. Full access control and password management facilities shall be provided. Users shall only access those Horizon Applications for which they have been given permission by the Branch. Each User shall be identified by a unique User-id and individual password.

4.4.1.4 The OPS shall provide facilities to enable the Branch Manager to establish new Users and set an initial password for all Users in a Branch. Should a User forget their password the Branch Manager shall be able to reset the password. The same procedure shall apply at single Counter Position Branches and multiple Counter Position Branches.

4.4.1.5 For situations where the sole User (e.g. Branch Manager in a single Counter Position Branch) has forgotten their password, the OPS shall provide the facility to generate a unique key as part of the log-on to a specific username. This shall be telephoned to the Help Desk who shall provide the corresponding key which, when input to OPS, shall allow access to the administration facilities. The User shall then be able to reset their User password.

4.4.2 Concurrency

The Pathway solution for OPS is based on a PC infrastructure configured such that multiple activities within a Branch do not significantly impact on each other. In particular, back office processes (e.g. report production) will be operated on a logically consistent set of data which will not be affected by any concurrent counter transactions.

4.5 Peripherals

4.5.1 Horizon Service Infrastructure – OPS: Peripheral and input devices Equipment General Requirements

Peripheral and input devices supplied as part of the elements of Horizon Service Infrastructure on which OPS is provided shall be capable of detecting contention, premature removal and swapping of Smart Tokens.

4.5.2 Peripherals Flexibility

4.5.2.1 OPS and the elements of Horizon Service Infrastructure on which OPS is provided shall have the flexibility for additional peripheral equipment to be added in the future, including input devices and printers.

4.5.2.2 The Counter Position PC shall have the capability of having at least four additional RS-232 connected peripherals added to a Counter Position configuration as initially installed at roll out of the Horizon Service Infrastructure.

4.5.3 Future Flexibility for Sharing of Specialist Peripherals

OPS, and the elements of Horizon Service Infrastructure on which OPS is provided, shall be able to be connected via RS-232 ports, and shall support such connection, to specialist peripherals in such a way that the specialist peripherals may be accessed by one or more Counter Position PCs. In such a case it shall be possible to restrict access to a subset of the Counter Position PCs in each Branch. This capability shall not be applicable to PIN Pads which can not be connected to or accessed by more than one Counter Position PC at any one time.

4.6 Security

4.6.1 Security of data and audit trail for OPS

4.6.1.1 All data captured at a Branch either as part of a Transaction performed at a Counter Position or as an administration function shall form part of a unique Transaction which shall be given a unique reference number by Riposte and details stored in the message store. The format of this message store entry shall vary according to the Transaction type but will typically contain:

(a) Post Office ID;

(b) Counter Position ID;

(c) unique Transaction ID;

(d) date;

(e) time;

(f) User ID;

(g) Horizon Application; and

(h) Transaction details.

4.6.1.2 Each Counter Position PC shall contain a journal and all journal entries shall be automatically replicated to all other members of the work group. A work group shall include all the Counter Position PCs in the Branch and one of the correspondence servers, at which TMS is provided. This correspondence server forms part of a "cluster" of correspondence servers of which two are located on one Data Centre site and the remaining two located on the other Data Centre site. All Transactions associated with one correspondence server are automatically replicated to the other site. Within each site all Transactions are reliably mirrored within a multiple disk array which has no single point of failure.

4.6.1.3 Once data are stored in the message store they shall never be altered. New Transactions shall always be appended to the message store. Retrieval of data using a particular key field shall retrieve all entries containing that field.

4.6.1.4 The security of data held within OPS shall not be compromised by any Incident nor when OPS is re-established following any Incident.

4.6.1.5 Fujitsu Services shall provide synchronisation facilities which shall automatically check the status of the journal for a node when it is re-established following failure. Should the journal be out of step (e.g. through failure of the Counter Position PC) Fujitsu Services shall automatically synchronise the journal and any data files to the same state as all other journals in that work group. Synchronisation may occur from another Counter Position PC (in a multi-Counter Position Branch) or from one of the correspondence servers or the second hard disk referred to in paragraph 6.2.4.2 (in a single Counter Position Branch).

4.6.1.6 The operating system supporting the OPS shall provide assurance of access control and data integrity functions.

4.6.2 OPS Secure Suspension

4.6.2.1 The OPS and the elements of the Horizon Service Infrastructure on which OPS is provided shall provide secure time-out facilities for each Counter Position PC.

4.6.2.2 Fujitsu Services shall provide a User activated suspension which shall enable the User to either:

(a) clear the screen and leave the Counter Position PC for a short period. In such circumstances, the User session shall be reactivated by the User entering their password. Any Horizon Applications which were active shall be left active. The display presented when the suspension facility is activated shall be different to any normal desktop or Horizon Application screen; or

(b) suspend a customer session and start a second session, and thereafter swap between the two sessions until one of them has been completed.

While an individual Transaction is waiting for input from a peripheral, a pick-list or on-line interaction, or while reports or receipts are printing, these facilities may be inhibited.

4.6.2.3 Should the User who initiated the suspension be unable to re-activate the facility, the following actions may be taken:

(a) after a period of time, during which there is no active session, the session shall be automatically logged-out. A journal message will be created indicating this;

(b) the Branch Manager may assume responsibility for any uncompleted session, the Stock Unit or share thereof, by entering his own User name / password;

(c) once the Counter Position PC has logged-out, any authorised User may then use that Counter Position PC; and

(d) all the above Events shall be written to the journal.

4.6.2.4 The facility shall allow the User to resume work with the minimum delay consistent with achieving security in accordance with the provisions hereof.

4.6.3 <u>Inactivity Time-out</u>

4.6.3.1 The OPS and the elements of Horizon Service Infrastructure on which OPS is provided shall provide secure inactivity time-out facilities if the Counter Position PC is inactive for a period defined in reference data for each Counter Position PC.

4.6.3.2 Should the User be unable to re-activate the facility, the following actions may be taken:

(a) after a period of time during which there is no active session the session shall be automatically logged-out. A journal message shall be created indicating this;

(b) the Branch Manager may assume responsibility for any uncompleted session, the Stock Unit or share thereof, by entering his own User name / password;

(c) once the Counter Position PC has logged-out, any authorised User may then use that Counter Position PC; and

(d) the above events shall be written to the journal.

4.6.3.3 The facility shall allow the User to resume work with the minimum delay consistent with achieving security in accordance with the provisions hereof.

4.6.4 Encryption Key Management

4.6.4.1 The OPS shall support a reliable and secure means for the storage and transfer of data. This shall include the use of techniques used selectively and in agreement between Post Office and Fujitsu Services as specified in the CCD entitled "HNG-X Technical Security Architecture" (ARC/SEC/ARC/0003) (formerly "Security Functional Specification" (RS/FSP/001)).

4.6.4.2 With the exception of PIN Pads (in which case paragraph 4.6.4.3 shall apply), a key management system shall be in place so the encrypted data can be deciphered without risk of that cryptographic key being exposed.

4.6.4.3 Fujitsu Services shall support the use of PIN Pads and the associated cryptographic management. PIN Pads shall comply with the requirements of ISO 9564.

4.6.5 Horizon OPS Style Guide

Any Post Office Service to be offered via the OPS shall be provided in accordance with the CCD entitled "HNGX-UI Style Guide" (DES/APP/STD/0001) (formerly "Horizon Office Platform Service Style Guide" (SD/STD/001)) which shall set out, among other things, general guidelines for the Human Computer Interface. An exception to this is the Mails Application which does not conform to the "HNGX-UI Style Guide" (DES/APP/STD/0001) (formerly "Horizon Office Platform Service Style Guide" (SD/STD/001)).

5. TRANSACTION MANAGEMENT SERVICE

5.1 Purpose

This Section details the functions and capabilities provided by the TMS that shall be supplied by Fujitsu Services.

5.2 Overview

5.2.1 The TMS shall provide the interworking between the Branches and the Data Centres using the Horizon Telecommunications Infrastructure. TMS shall be provided using both the Branch and the correspondence server Equipment, presenting interfaces to the Post Office Client systems or the Post Office systems. Such interfaces shall be implemented using TMS Agents, which are specified in paragraph 5.4.1.

5.2.2 The role of TMS shall be to provide a secure and resilient messaging and journalling service which shall support the transfer of data between OPS and Post Office Client Services, and Post Office Services.

5.3 General Attributes

5.3.1 Scalability

5.3.1.1 Fujitsu Services shall provide TMS such that it shall be scaleable to meet Post Office's future business needs in accordance with the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033).

5.3.1.2 The modular nature of TMS and the Horizon Service Infrastructure shall be scaleable to enable the workload growth specified in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033) to be accommodated, subject to the relevant provisions in Schedule A5 and Schedule B4.2.

5.3.2 Data Integrity

5.3.2.1 A Horizon Application or TMS Agent shall be able to be certain, at some level, that data have been positively acknowledged as received by TMS, or a peer Horizon Application connected to TMS.

5.3.2.2 Data transfers shall be capable of being despatched as:

(a) immediate;

(b) background / trickle fed; and

(c) time deferred.

5.3.3 Exclusivity

5.3.3.1 No computer system shall be connected to the Horizon Central Infrastructure or to those elements of the Horizon Telecommunications Infrastructure which are employed exclusively in the provision of the Infrastructure Services without the approval of Post Office.

5.3.3.2 Fujitsu Services shall maintain a register of computer systems with which such connections are allowed.

5.3.3.3 The Horizon Central Infrastructure and Horizon Telecommunications Infrastructure shall provide links into other computer systems as required to support the introduction of new or re-engineered Transactions required by Post Office.

5.3.3.4 The identity of any computer system with which a link is to be established shall be authenticated.

5.3.3.5 Fujitsu Services shall produce reports detailing any attempt to establish a link which is rejected. Fujitsu Services shall provide these reports to Post Office on request. Such reports will not be required where the link is between TMS and the Banks; and the rejection is due to a failure of the Banks; or between TMS and the MA and the rejection is due to a failure of the MA.

5.4 General Service description

5.4.1 Interface support

5.4.1.1 TMS shall interface with each instance of OPS within each Branch.

5.4.1.2 Fujitsu Services shall support the interfaces between the Horizon Service Infrastructure and the following:

(a) Santander;

(b) Merchant Acquirer;

(c) e-pay;

(d) those AP Clients listed as “POL” in the spreadsheet associated with the CCD entitled “Automated Payments System Client List” (including, without limitation, the DVLA On-Line link); and

(e) Post Office systems connected in accordance with the CCD entitled “HNG-X RGM Technical Interface Specification” (DES/NET/TIS/0005) (formerly “Horizon to Post Office Technical Interface Specification” (TI/IFS/008)).

5.4.1.3 The development and implementation of the interfaces specified in paragraph 5.4.1.2 shall principally take the form of TMS Agents which act upon Transactions originated within the Branches, and the Horizon Central Infrastructure which receives Transactions or data from Post Office, Client systems, Merchant Acquirer or e-pay.

5.4.1.4 The TMS Agents described in paragraph 5.4.1.3 shall support the transfer of data between OPS and TMS within a Branch, or between TMS and the Horizon Central Infrastructure within the Data Centres. The style of processing carried out by TMS Agents will be one of immediate (in support of real-time transactions), or batch (in support of bulk processing).

5.4.1.5 Further TMS Agents to support additional Post Office services or additional Client services may be agreed from time to time between Post Office and Fujitsu Services.

5.4.2 Data delivery

5.4.2.1 TMS shall provide for the distribution and collection of both file and record level data to and from the OPS.

5.4.2.2 Overnight Fujitsu Services shall produce a report of those Branches which have not been polled in the last 24 hours (including date of report, FAD code of each unpolled Branch and the date when that Branch was last polled), and that report shall be e-mailed to Post Office's business support unit.

5.4.2.3 Large data transfers shall be capable of being delivered in the same order as sent.

5.4.3 File Operations

5.4.3.1 The Horizon Central Infrastructure shall support the transfer of files between the data centres and computer systems which are attached to the Horizon Service Infrastructure.

5.4.3.2 The Horizon Central Infrastructure shall provide a file distribution function which shall be responsible for transfer, monitoring and retry of files.

5.4.3.3 The Horizon Central Infrastructure shall support the following functions, without limitation:

(a) triggering of transfers;

(b) reporting of transfer failures and retry of these transfers;

(c) verifying that file transfers are to/from pre-defined computer systems in the register referred to in paragraph 5.3.3.2.

5.4.4 File Processing

5.4.4.1 Data file processing shall be provided by the Horizon Central Infrastructure, optionally supported by TMS Agents. Conventional file processing facilities shall be provided as required by the Horizon Applications, including without limitation:

(a) validation of data files;

(b) concatenation and merging of files;

(c) generation of many data files from one data file;

(d) reformatting of the contents of a data file;

(e) generation of control totals;

(f) reconciliation of control totals; and

(g) production of reports, financial and other summaries.

5.4.5 Data Transfer Methods

5.4.5.1 The Horizon Central Infrastructure will support the automatic collection and delivery of data files to/from Post Office or Client systems.

5.4.5.2 The interfaces between the Data Centres and Post Office or Client systems shall support real and delayed time initiation of activities.

5.4.5.3 The Horizon Central Infrastructure will support the transfer to the EDG of files of Transactions records, such records having been produced by the Automated Payment Service in live operational use or for testing purposes. This facility will enable these data files to be transferred using a file push mechanism that will place the data files into predefined locations within the EDG. Subject to paragraphs 5.8 and 5.9 of Schedule D1, any changes to the Horizon Central Infrastructure as a result of the migration of the related Client systems from their existing interfaces with the Infrastructure to the EDG shall be dealt with through the Change Control Procedure.

5.4.6 End to End Recovery

End-to-end recovery facilities shall be performed by Fujitsu Services in accordance with the CCD entitled "HNG-X Business Continuity Framework" (SVM/SDM/SIP/0001) (formerly "Business Continuity Framework" (CS/SIP/002)).

6. GENERAL INFRASTRUCTURE SERVICES REQUIREMENTS

6.1 Introduction

This section contains characteristics common to both the OPS and TMS Infrastructure Services.

6.2 Links from OPS to TMS

6.2.1 General

6.2.1.1 Each instance of OPS within Branches shall interface with TMS to allow the transfer, in both directions, of authorised data files and messages.

6.2.1.2 The transfer of data between OPS and TMS shall be secure, complete, accurate and robust.

6.2.1.3 Within OPS it shall be possible for OPS to identify whether data from OPS have been received by TMS or not.

6.2.2 Data Replication

6.2.2.1 Fujitsu Services shall use data replication and synchronisation techniques to ensure that data transfer between Counter Positions at which OPS is provided and between instances of OPS at each Counter Position and the TMS are secure, complete, accurate and robust.

6.2.2.2 Once a Transaction has been settled at a Counter Position, TMS shall commit the full Transaction details to that Counter Position PCs message store. The Transaction details shall simultaneously be automatically replicated to all other Counter Position PCs in the Branch so that the data are securely captured. In addition, Fujitsu Services shall automatically replicate Transaction details to a remote server at which TMS is provided.

6.2.2.3 The OPS Counter Position PCs and TMS servers are known as "nodes".

6.2.2.4 All data and message transfers from a single node shall be generated in a strict numbered sequence with a unique node identification. Any attempt to introduce a fraudulent message shall be automatically detected and rejected by OPS.

6.2.2.5 An additional pseudo random sequence number produced from a cryptographic algorithm can also be included to provide a very high level of message integrity as agreed between the Parties from time to time, such agreement not to be unreasonably withheld. Details of the use of the cryptographic algorithm are contained in the CCD entitled “HNG-X Technical Security Architecture” (ARC/SEC/ARC/0003) (formerly “Security Functional Specification” (RS/FSP/001)).

6.2.2.6 Data and message transfers shall be resilient to either network or node failure. When the failure condition is resolved the nodes shall automatically synchronise and complete any data or message transfers that are required to ensure these nodes are in a consistent state.

6.2.3 Data Integrity

6.2.3.1 Fujitsu Services shall use techniques to ensure data integrity within the OPS and as part of data/message transfer between OPS and TMS, including:

(a) cyclic redundancy checks shall be calculated for all journal records, including Reference Data;

(b) digital signatures shall be used for all data where assurance of content and source are required; and

(c) data encryption shall be used selectively on certain data fields.

6.2.3.2 All messages and data shall have a cyclic redundancy check applied when they are initially committed to the journal and this shall be checked every time the message or data is accessed. This shall protect against accidental corruption and casual tampering. Any failure of a cyclic redundancy check shall cause the message to be rejected and retrieved from alternate nodes.

6.2.3.3 In the event that nodes fail, recovery shall take place through the use of the following techniques: associating of Post Office and correspondence server nodes, message numbering, marker (message high and low water marks) exchange message transfers to equalise water marks, and in accordance with the CCD entitled “Post Office Site Failure Contingency Procedures”.

6.2.3.4 Where Post Office requires the origin of data to be authenticated, Fujitsu Services shall apply a digital signature to the data prior to transmission and shall then check it upon receipt. Digital signature techniques and the data to which they are applied shall be described in the CCD entitled “HNG-X Technical Security Architecture” (ARC/SEC/ARC/0003) (formerly “Security Functional Specification” (RS/FSP/001)).

6.2.3.5 Fujitsu Services shall automatically detect any attempt to alter data and shall log such attempts for subsequent investigation by Fujitsu Services. Details of all such attempts shall be passed to Post Office.

6.2.4 Recovery

6.2.4.1 Fujitsu Services shall perform general recovery processes as specified in the CCD entitled “HNG-X Business Continuity Framework” (SVM/SDM/SIP/0001) (formerly “Business Continuity Framework” (CS/SIP/002)).

6.2.4.2 The Counter Position PC in all single Counter Position Branches shall be fitted with a second hard disk which shall be exchangeable to facilitate rapid exchange of systems and Transaction data in the event of a system failure other than a hard disk failure.

6.3 PIN Pad Firmware Distribution

Fujitsu Services shall provide and maintain firmware distribution facilities to ensure the distribution of firmware from the Data Centres to PIN Pads. The facility shall meet the software control requirements of ISOP 9564.

6.4 Functional Title of Code

Fujitsu Services shall ensure that each component of the Horizon Service Infrastructure is clearly marked with a functional title or code so that it can be readily identified in the relevant documentation and related to its proper place in the Horizon Service Infrastructure.

7. NBS SPECIFIC BUSINESS CONTINUITY REQUIREMENTS

7.1 Each Data Centre (if required to support the NBS on its own as a result of a failure of the other Data Centre) shall have the capability in normal operation, with no failures having occurred:

7.1.1 to support the Contracted Volumes in relation to the NBS and Debit Card as defined in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033); and

7.1.2 to support Fujitsu Services' obligations in respect of NBS Service Levels set out in Annex 3 to Schedule B4.4 without preventing or impairing that Data Centre's support for Fujitsu Services' obligations in respect of the Service Levels for other Services in existence at the Amendment Date.

7.2 The Data Centres (including NBS elements) will be configured such that no single point of failure within the Data Centres will cause the NBS to fail with both Data Centres in operation.

7.3 Switchover to backup systems within the Data Centres and for the network connections within the Data Centres:

7.3.1 for real-time elements of the NBS affecting Banking Transactions at Counter Positions shall be automated with the exception of the persistent store which shall be manually switched over; and

7.3.2 for non-real time elements may be automated or manual.

7.4 The Central Network

7.4.1 The loss of a major switching node within the Central Network shall not cause the NBS to fail and should such loss occur Fujitsu Services (in addition to its other obligations under this Agreement) shall use all reasonable endeavours to procure that any shortfall in system performance is recovered within seven days of that loss.

7.4.2 The Central Network shall be configured such that there shall be no single point of failure within the Central Network.

7.5 The Santander Circuit

7.5.1 The Santander Circuit shall be configured such that there shall be no single point of failure (including site failure) within the Santander Circuit.

7.5.2 The Santander Circuit shall have the capability in normal operation, with no failures having occurred to that link:

7.5.2 (a) to support the Contracted Volumes for Santander in relation to the NBS as defined in the CCD entitled ”Horizon Capacity Management and Business Volumes” (PA/PER/033); and

7.5.2 (b) to support Fujitsu Services’ obligations in respect of NBS Service Levels set out in Annex 3 to Schedule B4.4.

8. ASSOCIATED DOCUMENTS

8.1 The following CCDs are associated with this Schedule B4.3:

	Document Reference	**Document Title**
1	PA/PER/033	Horizon Capacity Management and Business Volumes
2	BP/DES/003	Counter Hardware Design Specification
3	CR/SPE/025	Introduction of the Mobile Configuration
4	NB/PDN/010	PIN Pad Product Specification
5	SD/STD/001 (Replaced) DES/APP/STD/0001	Horizon Office Platform Service Style Guide (Replaced) HNGX-UI Style Guide
6	RS/FSP/001 (Replaced) (ARC/SEC/ARC/0003)	Security Functional Specification (Replaced) HNG-X Technical Security Architecture
7	BP/DOC/008	Automated Payments System Client List

8	TI/IFS/008	Horizon to Post Office Technical Interface Specification
9	CS/SIP/002 (Replaced) SVM/SDM/SIP/0001	Business Continuity Framework (Replaced) HNG-X Business Continuity Framework
10	BP/PRO/003	Post Office Site Failure Contingency Procedures **[CAT F]**
11	SD/DES/005	Horizon OPS Reports and Receipts - Post Office Account Horizon Office Platform Service
12	Not Used	
13	Not Used	
14	CR/SPE/025	Introduction Of The Mobile Configuration
15	AP/DOC/004	Software Sub-licence for Smart Card Security Software
16	TD/STD/004	Generalised API for OPS/TMS Technical Design Standard
17	Withdrawn in CCN1616b	
18	Not Used	
19	SVM/SDM/PRO/0013	Calculating Mean Time Between Failure and Availability Process
20	Not Used	
21	DES/NET/TIS/0006	CAPO-HNG-X Technical Interface Specification
22	DES/NET/TIS/0008	VOCALINK – HNG-X Technical Interface Specification
23	DES/NET/TIS/1839	Santander HNG-X Technical Interface Specification
24	AS/IFS/002	Horizon to EDG - Technical Interface Specification for Track and Trace
25	POLSAP/DES/GEN/SPE/0002	POLSAP Technical Interface Specification

26	DES/NET/TIS/0004	Streamline HNG-X Technical Interface Specification
27	Not Used	

8.2 There are no CRDs associated with this Schedule B4.3.