

CONFIDENTIAL

SCHEDULE B3.3**HNG-X 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 |
| 2.0 | 25/01/07 | Baseline copy of 1.1 |
| 3.0 | 23/02/09 | Baseline copy of 2.1 |
| 3.1 | 13/05/09 | Applying changes as per CCN1258 |
| 6.0 | 06/07/09 | Moving all schedules to V6.0 as agreed with Fujitsu |
| 6.1 | 23/12/09 | Applying changes as per CCN 1268 |
| 6.2 | 05/01/10 | Applying changes as per CNN 1272 |
| 6.3 | 31/03/10 | Applying changes as per CCN1276a |
| 6.4 | 01/04/10 | Applying changes as per CCN1270 |
| 7.0 | 10/05/10 | Moving all schedules to V7.0 as agreed with Fujitsu. |
| 8.0 | 21/02/12 | Applying changes specified in CCN1294d |
| 9.0 | 13/01/14 | Applying changes as per CCN1349,1311b, 1328b and CCN1400 |
| 10.0 | 10/09/15 | Applying changes as per CCN1418, CCN1420a and as subsequently amended in this CCN1506 and moving all Schedules to V10.0 in accordance with CCN1506 |
| 11.0 | 31/03/16 | Applying changes as per CCN1423c, CCN1427 and moving all Schedules to V11.0 in accordance with CCN1604 |
| 12.0 | 03/07/17 | Applying changes as per CCN1610, CCN1614a, CCN1618a, CCN1621 and moving all schedules to V12.0 |
| 13.0 | | Updating as per CCN1629, CCN1632 and CCN1650c and moving all Schedules to v13.0 |

CONFIDENTIAL

SCHEDULE B3.3

HNG-X CENTRAL AND TELECOMMUNICATIONS INFRASTRUCTURE

1. HNG-X SERVICE INFRASTRUCTURE

1.1 Introduction

1.1.1 This Schedule B3.3 records and specifies the HNG-X Service Infrastructure that shall be provided by Fujitsu Services in order to deliver the Business Capabilities and Support Facilities described in Schedule B3.2 from Trigger Point T5 (Data Centre Ready for HNG-X). Prior to Trigger Point T5 (Data Centre Ready for HNG-X), the provisions of Schedule B4.3 shall apply.

1.1.2 The HNG-X Service Infrastructure comprises, in the period up to 31st March 2015:

(a) Branch Infrastructure, the provisions relating to which are set out in Schedule B3.4;

(b) HNG-X Central Infrastructure;

(c) HNG-X Telecommunications Infrastructure; and

(d) POLSAP Central Infrastructure (from the POLSAP R1 Go Live Date)

and in the period from 1st April 2015, the

(a) HNG-X Central Infrastructure;

(b) HNG-X Telecommunications Infrastructure; and

(c) POLSAP Central Infrastructure (from the POLSAP) R1 Go Live Date).

1.1.3 The HNG-X Service Infrastructure provides functions and capabilities used to deliver the Business Capabilities and Support Facilities, and the Operational Services.

1.1.4 The provisions of this Schedule shall not apply in respect of the HNG-X Central Infrastructure or HNG-X Telecommunications Infrastructure, and accordingly it does not form part of the HNG-X Service Infrastructure.

1.2 HNG-X Central Infrastructure

1.2.1 Subject to paragraph 1.3.4(f), Fujitsu Services shall provide all equipment at the Data Centres necessary to provide the Business Capabilities and Support

CONFIDENTIAL

Facilities. 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).

- 1.2.2 The Transfer Asset Register shall be updated in accordance with the timetable contained in paragraph 3.2.1 of Schedule E.
- 1.2.3 Fujitsu Services shall maintain all increases in the capacity of the HNG-X Service Infrastructure which Fujitsu Services have agreed to make at the request of Post Office.
- 1.2.4 Fujitsu Services shall 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.
- 1.2.5 Fujitsu Services may replace, upgrade, remove or decommission hardware and software from time to time comprised in the HNG-X Service Infrastructure provided that it continues at all times to comply with its obligations in paragraphs 1.2.3 and 1.2.4 (unless agreed otherwise under the Change Control Procedure).
- 1.2.6 Fujitsu Services shall use the facilities of the DR Data Centre to provide a testing environment, which shall be known as the SV&I Rig which shall support functional testing until 31st March 2020
- 1.2.7 Fujitsu Services shall maintain at their Bracknell location the Integration (INT) Rig which shall support integration testing until 31st March 2020
- 1.2.8 Fujitsu Services shall maintain at their Bracknell location the Component Integration and Test (CIT) Rig which shall support development testing until 31st March 2020.
- 1.2.9 Any additional test configurations that are required to support changes to Post Office's business shall be dealt with through the Change Control Procedure.
- 1.2.10 Fujitsu Services shall, before 31st March 2018, detail £100,000 of investment value in maintaining the supportability of the HNG-X Test Infrastructure which will be funded by Fujitsu Services. The specific utilisation of these funds will be as agreed between the parties and may be utilised on infrastructure refresh and/or Services. All changes will be managed in accordance with the Change Control Process.

1.3 HNG-X Telecommunications Infrastructure

- 1.3.1 The HNG-X Telecommunications Infrastructure consists of:
 - (a) for Branches where the Branch Network Service is provided by Fujitsu Services, Branch Telecom Infrastructure – those networking elements that provide connectivity between the Branches and the Data Centre; or for Branches where Replacement Services to the VSAT BB communications method to Branches are being provided by the Next Supplier, infrastructure providing connectivity between the Branches and the Data Centre shall be provided by the Next Supplier- the

CONFIDENTIAL

infrastructure providing connectivity between the Branches and the Data Centre provided by the Next Supplier; and

- (b) Central Telecom Infrastructure – those network elements that provide connectivity from the Data Centre to other sites.

1.3.2 Branch Telecom Infrastructure

- (a) The Branch Telecom Infrastructure, in Branches where the Branch Network Service and CMT Service is provided by Fujitsu Services, Fujitsu Services shall use one or more of the following communications methods between the Branch Infrastructure and the Data Centres:
 - (i) Until 15th January 2018, Integrated Services Digital Network (ISDN) - communications method to connect to the data centre where ADSL cannot be used or if in the Kingston Communications area;
 - (ii) Until 15th January 2018, Public Switch Telephone Network (PSTN) which shall be introduced on a Branch by Branch basis on commencement of Associated Change Workstream A7 (Branch Router Rollout);
 - (iii) Asymmetric Digital Subscriber Line (ADSL) - Primary communications method for Branches;
 - (iv) Sub-paragraph removed by CCN1621.
 - (v) General Packet Radio Service (GPRS) / Enhanced Data GSM Environment (EDGE) and 3G which shall be introduced on a Branch by Branch basis on commencement of Associated Change Workstream A7 (Branch Router Rollout); or
 - (vi) Sub-paragraph removed by CCN161.
 - (vii) Internet Virtual Private Network – to enable Branches to connect from Internet connections. This is subject to agreed connection specifications and concurrency limits as stipulated in Schedule D1 Annex A “BRANCH AND COUNTER POSITION LIMITS”.
- (b) These connections may be used as either primary or backup network connections, although there may be restrictions on the size of the Branch that can be supported on some technologies. Additionally there are restrictions on the technologies that are supported for a Branch's primary (storage) location. All such restrictions are set out in PA/PER/033.
- (c) 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

CONFIDENTIAL

be set out in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033).

- (d) The response time Service Levels defined in Schedule C1 and each applicable Service Description apply to this Schedule B3.3 providing that at least 90 per cent of Transactions are undertaken in Branches that use ADSL as their primary network connection. If the proportion of the connected Branches using ADSL drops below this level then changes will be handled under the Change Control Procedure.
- (e) With regard to the BNS Report Part 1 and BNS Report Part 2 (as defined below):
 - (i) Within 1 month of date of signature of CCN 1400, Fujitsu Services shall agree with Post Office via the Change Control Procedure the preparation of a comprehensive study of the current Branch Network which shall, as a minimum, cover the following aspects of the current Branch Network Service:
 - (a) Branch Routers. The availability and any changes required to maintain Sarian/Digi firmware support through to 31st March 2017 (note hardware is part of the Engineering Service);
 - (b) Branch Routers. The compatibility of the current branch routers with expected changes in WAN technologies (where WAN provider engaged as part of study);
 - (c) Cisco Summary Router firmware and hardware support. What options are there given that this product goes "end of supported life" with Cisco in mid 2015;
 - (d) ADSL. What changes, if any, are expected with the TalkTalk LLU copper product prior to end of March 2017;
 - (e) ADSL. What changes, if any, are expected with the BT IP Connect copper product prior to end of March 2017;
 - (f) C&W Energis / RemoteConnect. Confirm what if any changes may be required with respect to the PSTN Bootloader access; and
 - (g) Utimaco NT4 VPN. Confirmation that the date goes forward to March 2017,

with respect to any known issues which may affect the Branch Network Service prior to 31st March 2017 (the "BNS Report Part 1"). If requested by Post Office within 2 weeks of date of signature of CCN 1400 Fujitsu Services shall also include in this study some or all of the following:

- (h) ADSL – Kingston copper ADSL;
- (i) VSAT branch hardware (Disk, IDU etc);
- (j) VSAT Atlantic Bird, Euro Bird and Italy Base Station;
- (k) Cisco Internet Branch Routers (at VSAT, BFPO and KDSL) firmware support;
- (l) Orange/Voda – roadmap for 2G and 3G technologies;
- (m) Orange/Voda – SIM cards standards;
- (n) Orange/Voda – data centre connectivity issues; and
- (o) C&W Energis / Remote Connect – ISDN / PSTN branch connectivity; and
- (p) BT individual ISDN2e lines,

CONFIDENTIAL

to determine if there are any other issues which may affect the Branch Network Service prior to 31st March 2017 (the “**BNS Report Part 2**”). The BNS Report Part 1 and the BNS Report Part 2 (if any) shall be referred to as the “**BNS Report**”. Fujitsu Services shall produce Part 1 of the report within 3 months of the signature of the Change Note and if requested by Post Office in accordance with clause (e) (i) above Part 2 of the report within 4 months of the signature of the Change Note.

- (ii) The preparation of the report shall be chargeable to the Post Office, the cost of the BNS Report Part 1 shall be capped at £70,000 (exc. VAT) and the cost of the BNS Report Parts 1 and 2 combined shall be capped at £120,000 (exc. VAT).
- (iii) The Parties shall jointly review the BNS Report and shall use reasonable endeavours to challenge the BNS Report and work with third parties to minimise and mitigate the elements of the Service that need refreshing, upgrading or a change to the terms support associated with any spares, hardware, software or firmware which form part of the current Branch Network Service. The Parties shall use reasonable endeavours to agree any changes to the BNS Report within 30 Working Days of the date that the BNS Report is delivered to Post Office.
- (iv) The Parties acknowledge and agree that the preferred outcome is that no changes to the infrastructure of the Branch Network Service are required. The Parties shall work collaboratively together so as to achieve this outcome so as to ensure that no or minimal capital expenditure is required from Post Office.
- (v) If the Parties are unable to agree the BNS Report then the Subject Leads for the Relationship best qualified to deal with the BNS Report, taking into account its nature and the responsibilities of each Subject Lead, shall convene an occasional meeting of the relevant Relationship in accordance with paragraph 3.3 of Schedule A2 to agree the BNS Report. If the matter is not resolved at a Relationship level it shall be escalated via the existing Dispute Resolution Procedure.
- (vi) Once agreed, any items identified in the BNS Report shall be deemed to be BNS R&R Required Items.
- (vii) Post Office may purchase such BNS R&R Required Items from any Tower Contractor or any other third party. Until 31st March 2015, as set out in Schedule B1 (Branch Hardware Implementation), only Fujitsu Services may implement such BNS R&R Required Items into the Services (at Post Office's additional cost, where such costs are not recoverable under the Charges) unless the relevant Service is partially terminated in accordance with Schedule E, paragraph 9.1. After 31st March 2015, Post Office may request the appropriate Tower Contractor to implement the BNS R&R Required Items (where the previous way to implement such an item was performed by an element of the Services that has been partially terminated) but Fujitsu Services retains the right (acting reasonably) to sample test and check correct implementation of such BNS R&R Required Items.
- (viii) Once BNS R&R Required Items have been implemented then Fujitsu Services shall provide the Services and comply with the Service Levels to which those Refresh Items relate.
- (ix) With regard to BNS R&R Required Items listed in the BNS Report Part 1, Post Office shall procure and/or implement the BNS R&R Required Items set out in the BNS Report Part 1. In the event that Post Office fails to procure and/or implement the relevant BNS R&R Required Item, then Fujitsu Services shall not be liable for any

CONFIDENTIAL

service failure directly attributable to Post Office not proceeding with, implementing and/or making available the BNS R&R Required Item listed in the BNS Report Part 1.

- (x) With regard to Refresh Items listed in the BNS Report Part 2, Post Office may at its sole option determine whether to implement all, some, or none of BNS R&R Required Items set out in the BNS Report Part 2. In the event that Post Office decides to proceed with some or none of the Refresh Items listed in the BNS Report Part 2, then Fujitsu Services shall not be liable for any service failure directly attributable to Post Office not proceeding with, implementing and/or making available the BNS R&R Required Items listed in the BNS Report Part 2.”

1.3.3 Central Telecom Infrastructure

The Central Telecom Infrastructure provides network connections:

- (i) between Data Centres and Post Office sites;
- (ii) between Data Centres and Client sites;
- (iii) between Data Centres and Fujitsu Services support sites;
- (iv) between the Data Centres and third party support sites;
- (v) between the two Data Centres (intercampus links); and
- (vi) for the test service including any test Branches.

1.3.4 Interface support for Post Office services or Client services

- (a) The HNG-X 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 shall be defined in the relevant TIS and shall support real and delayed time initiation of activities.
- (b) The HNG-X Telecommunications Infrastructure and HNG-X Central Infrastructure shall provide a file distribution function which shall be responsible for the transfer, monitoring and retry of files as specified in the relevant AIS and / or TIS.
- (c) The HNG-X 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.
- (d) Additional Post Office services or additional Client services which require an additional interface may be agreed from time to time between Post Office and Fujitsu Services and shall be specified in an additional TIS and / or an additional AIS.

CONFIDENTIAL

- (e) Interface Support for Santander
 - (i) 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 includes 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:
 - (1) provision of a suitable physical operating environment for Fujitsu Services' equipment used for or in connection with the communications link including the following:
 - (A) 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
 - (B) provision of environmental conditions as reasonably required by Fujitsu Services.
 - (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.
- (f) Interface Support for CAPO and LINK
 - (i) 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 1.3.4(g), 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:
 - (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:
 - (A) ensuring the physical security of all equipment which is located on Fujitsu Services and/or any

CONFIDENTIAL

such third party's premises to protect against unauthorised access; and

(B) provision of environmental conditions as reasonably required by CAPO and/or LINK;

(2) permitting CAPO and/or LINK (including their respective contractors) to gain access (at reasonable times and on reasonable notice, and subject to paragraph 1.3.4(g)) 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) 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.

(g) Post Office Communications Links Services

Post Office shall, in relation to paragraph 1.3.4(f), be responsible for ensuring that:

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

(ii) 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:

(1) keep confidential, and 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;

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

(3) return such Confidential Information held in tangible form to Post Office, and to 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,

CONFIDENTIAL

other than as required by law;

- (iii) 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
- (iv) 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; and
- (v) 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 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.

1.4 Exclusivity

- 1.4.1 No computer system shall be connected to the HNG-X Central Infrastructure or to those elements of the HNG-X Telecommunications Infrastructure which are employed exclusively in the provision of the HNG-X Services without the approval of Post Office.
- 1.4.2 Fujitsu Services shall maintain a register of computer systems with which such connections are allowed.
- 1.4.3 The HNG-X Central Infrastructure and HNG-X 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.
- 1.4.4 The identity of any computer system with which a link is to be established shall be authenticated.
- 1.4.5 Fujitsu Services shall produce reports detailing any attempt to establish a link (specified in paragraph 1.4.3) 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 the HNG-X Central Infrastructure / HNG-X Telecommunications Infrastructure and the Banks; and the rejection is due to a failure of the Banks; or between the HNG-X Central Infrastructure / HNG-X Telecommunications Infrastructure and the MA and the rejection is due to a failure of the MA.

1.5 Continued Support of operating systems and Software

CONFIDENTIAL

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

1.6 Functional Title or Code

Fujitsu Services shall ensure that each component of the HNG-X 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 HNG-X Service Infrastructure.

1.7 POLSAP Central Infrastructure

From 5th October 2016 POLSAP Central Infrastructure is detailed in the CCD entitled "POLSAP Hosting-Service, Service Description" (SVM/SDM/SD/2191).

1.7.1 Not Used.

1.7.2 Not Used.

2. SECURITY**2.1 Introduction**

This section covers the security provisions relating to the HNG-X Service Infrastructure.

2.2 Encryption Key Management

2.2.1 The HNG-X System shall support a reliable and secure means for the transfer of data to the Data Centre. 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)

2.2.2 With the exception of PIN Pads (in which case paragraph 2.1.4 of Schedule B3.4 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.

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

3. BUSINESS CONTINUITY**3.1 Introduction**

This paragraph 3 covers the business continuity provisions relating to the HNG-X Service Infrastructure.

3.2 End to End Recovery

CONFIDENTIAL

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

3.3 Business Continuity

3.3.1 Data Centre Resilience

- (a) One Data Centre will be used to support the Business Capabilities and Support Facilities (the "Live Data Centre") with a second Data Centre providing DR (the "DR Data Centre"). There are network components (appliances and platforms) at the DR Data Centre which contribute to the provision of Business Capabilities and Support Facilities.
- (b) The DR Data Centre will under normal operation be used for testing except where it needs to be used for business continuity tests. The DR Data Centre will also host some live network components.
- (c) Each Data Centre shall have the capability in normal operation with no failures or a single failure having occurred:
 - (i) to support the Contracted Volumes as defined in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033); and
 - (ii) to support Fujitsu Services' obligations in respect of Service Levels set out in Schedule C1 and each applicable Service Description.
- (d) Each Data Centre will be configured such that the failure of a single component will not cause the Business Capabilities and Support Facilities to fail. For the avoidance of doubt, Fujitsu Services will inform Post Office of those major Data Centre components whose failure may result in the need to invoke DR. There is a single high capacity WAN circuit into each Data Centre. Should the link into one Data Centre fail then a patch via the other Data Centre will be used.
- (e) Switchover to backup systems within the Data Centre and for the network connections within the Data Centre:
 - (i) for real-time elements of the Business Capabilities and Support Facilities shall be automated; and
 - (ii) for non-real time elements may be automated or manual.
- (f) Switchover from the Live Data Centre to the DR Data Centre will be manually initiated.
- (g) In the event that the DR Data Centre needs to be used to run the live service or if the DR Data Centre itself is unavailable, there will be no

CONFIDENTIAL

significant test environment available. In this scenario, limited testing (sufficient to test minor fixes needed to keep the live service operational) will be available at a Fujitsu Services development site. However such testing facilities will not be sufficient to test releases.

3.3.2 The Central Network

- (a) The Central Network comprises the network communications between the Data Centres and the switches used by Fujitsu Services (or Fujitsu Services' Sub-contractor which operates such network) to:
 - (i) Until November 15th January 2018, answer ISDN calls from Branches;
 - (ii) convert asynchronous transfer mode (ATM) communications from ADSL Branches into internet protocol (IP) communications; or
 - (iii) convert leased line communications from Branches into internet protocol (IP) communications
 - (iv) convert wireless wide area network (WAN) protocols from Branches into internet protocol (IP) communications,(the "Central Network").
- (b) The loss of a major sub-contractor network switching node within the Central Network shall not cause the complete loss of the Branch Telecom Infrastructure. However, should a loss of a major sub-contractor network switching node within the Central Network 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.
- (c) The Central Network shall be configured such that there shall be no single point of failure within the Central Network. Some failures in the Central Network may require the Branch to re-establish communications with the Data Centre.

3.3.3 The Santander Circuit

- (a) The Santander Circuit shall be configured such that there shall be no single point of failure (including site failure) within the Santander Circuit.
- (b) "The Santander Circuit shall have the capability in normal operation, with no failures or a single failure having occurred to that link:"

CONFIDENTIAL

- (i) to support the Contracted Volumes for Banking Transactions for Santander as defined in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033); and
- (ii) of supporting Fujitsu Services' obligations in respect of Service Levels set out in Schedule C1 and each applicable Service Description.

4. ASSOCIATED DOCUMENTS

4.1 The following CCDs are associated with this Schedule B3.3.

| | Document Reference | Document Title |
|---|--------------------|--|
| 1 | PA/PER/033 | Horizon Capacity Management and Business Volumes |
| 2 | SVM/SDM/SIP/0001 | HNG-X Business Continuity Framework |
| 3 | ARC/SEC/ARC/0003 | HNG-X Technical Security Architecture |
| 4 | Not Used | |

4.2 There are no CRDs associated with this Schedule B3.3.