Balancing and Settlement Code

Communication Requirements Document

Version 17.0

Date : 23 February 2012

Communication Requirements Document

relating to the

requirements for sending and receiving Communications between Parties and BSC Agents

1. Reference is made to the Balancing and Settlement Code as given contractual force by the BSC Framework Agreement dated Code Effective Date and as modified from time to time.

2. This is the Communication Requirements Document ~~Version 17.0~~ referred to in Section O of the Code, relating to the sending and receiving of Communications between Parties, Party Agents, Market Index Data Providers and the following BSC Agents:

    (a)   Balancing Mechanism Reporting Agent

    (b)   Central Registration Agent

    (c)   Central Data Collection Agent

    (d)   Energy Contract Volume Allocation Agent

    (e)   Settlement Administration Agent

    (f)   Funds Administration Agent

    (g)   Technical Assurance Agent

3. This document is effective from ~~23 February 2012~~.

AMENDMENT RECORD

Version	Date	Description of Changes	Changes Included	Mods/ Panel/ Committee Refs
1.0	14.08.00	Designated Version	N/A	N/A
2.0	23.01.01	Work outstanding at Go Active, resolution of inconsistencies, inclusion of consultation comments	240	11/005
3.0	08.03.01		NCR343 & 348	08/03/01
4.0	13/08/02	Changes for BSC Systems Release 2	CP755, CP519, P52	ISG18/193
5.0	10/12/02	Changes for CVA Programme December 02 Release	CP511 CP712 CP751	ISG11/093 ISG10/082 ISG14/138
6.0	11/03/03	Changes for CVA Programme Feb 03 Release	P78	ISG24/265
7.0	24/06/03	Changes for CVA Programme Jun 03 Release and rebadging for P62	CP703, CP710, P62	ISG/13/116
8.0	05/11/03	Changes for CVA Programme Nov 03 Release and outstanding changes for Approved Modification P118	P82, P117	54/006, 60/005
9.0	03/11/04	Changes for CVA Programme Nov 04 Release	P98, P142, CP502, P82 Removal	ISG36/40 SVG36/492
10.0	BETTA Effective Date	SVA February 05 Release and BETTA 6.3	CP993, CP1091, BETTA 6.3	SVG48/004
11.0	02/11/05	Changes for CVA Programme Nov 05 Release	CP1061	ISG48/002
12.0	22/02/07	February 2007 Release	CP1160 CP1161	ISG66/04 SVG66/04
13.0	23/08/07	P197 Release	P197	P/115/04
14.0	06/11/08	November 08 Release	CP1246	ISG88/04 SVG88/02
			P214	ISG90/04 SVG90/08
15.0	26/06/09	February 09 Release	CP1263	ISG94/01 SVG94/02
16.0	04/11/10	November 10 Release	CP1328	ISG112/01 SVG112/03
			CP1329	ISG112/01 SVG112/03
17.0	23/02/12	February 2012 Release	CP1352	ISG129/02 SVG129/04
17.2	29/03/19	29 March 2019 Standalone Release	P369	TBC

CONTENTS

1. Introduction

1.1. Purpose and Scope

This document, as defined in the Code, is the only Communication Requirements Document and as such covers the communications between BSC Parties, their Agents and the BSC Agents where the communications interfaces are defined in the Data File Catalogue.

The purpose of this document is to define the communication requirements. BSCCo shall ensure these requirements are satisfied in respect of each BSC Agent.

For the avoidance of doubt, communications between SVA data parties which are specified in the SVA Data Catalogue or another Code Subsidiary Document as being made using the Managed Data Network Service are to be provided using the Managed Data Network Service. (see Section 9 below).

[P369]1.2 Main Users of the Document

The main users of this document are:

(a)   Parties;

(b)   Party Agents;

(c)   Market Index Data Providers;

(d)   The ~~Transmission Company~~National Electricity Transmission System Operator (NETSO) and Licensed Distribution System Operators; and

(e)   The following BSC Agents:

- Balancing Mechanism Reporting Agent

- Central Registration Agent

- Central Data Collection Agent

- Settlement Administration Agent

- Energy Contract Volume Aggregation Agent

- Funds Administration Agent

- Technical Assurance Agent

1.3 Balancing and Settlement Code Provision

This Communication Requirements Document has been produced in accordance with the provisions of the Code. In the event of an inconsistency between the provisions of this Code Subsidiary Document and the Code, the provisions of the Code shall prevail.

1.4 Associated BSC Procedures

BSCP01 Overview of Trading Arrangements

BSCP41 Reporting Requests & Authorisation

BSCP65 Registration of Parties and Exit Procedures

BSCP70 CVA Qualification Testing for Parties and Party Agents

BSCP71 Submission of ECVNs and MVRNs

BSCP301 Clearing Invoicing and Payment

BSCP537 Qualification Process for SVA Parties, SVA Party Agents and CVA MOAs

2. Acronyms and Definitions

[P369] 2.1 List of Acronyms

The following is a list of acronyms used in this document:

ADSL – Asymmetric Digital Subscriber Line

BMRA - Balancing Mechanism Reporting Agent

BPITs – Business Process Integration Tests

BSC - Balancing and Settlement Code

BSC CSA – BSC Central Services Agent

CCP – Credit Cover Percentage

CDCA - Central Data Collection Agent

CIR - Committed Information Rate

CPU – Central Processing Unit

CRA - Central Registration Agent

DNS - Domain Name System

DR - Disaster Recovery

ECVAA - Energy Contract Volume Aggregation Agent

ECVNA - Energy Contract Volume Notification Agent

EWS – ECVAA Web Service

FAA - Funds Administration Agent

FTP - File transfer protocol

GSP – Grid Supply Point

IA – Interconnector Administrator

ISDN - Integrated Services Digital Network

ISP - Internet Service Provider

LAN - Local Area Network

LDSO- Licensed Distribution System Operator

MOA – Meter Operator Agent

MIDP – Market Index Data Provider

MPLS – Multi Protocol Label Switching

MVRNA – Metered Volume Reallocation Notification Agent

NETSO – National Electricity Transmission System Operator

NAT – Network Address Translation

NATs - Network Access Tests

NTP - Network Time Protocol

PartID – Participant ID

PCIG – Participant Communications Installation Guide

OpenPGP – Open Source Pretty Good Privacy

PVC - Permanent Virtual Circuit

RVD - Rendezvous Daemon

RVRD - Rendezvous Routing Daemon

SAA - Settlement Administration Agent

SMRA – Supplier Meter Registration Agent

SVA –Supplier Volume Allocation

TAA – Technical Assurance Agent

TCP/IP - Transmission Control Protocol/Internet Protocol

UTC- Co-ordinated Universal Time

XSec – Participant Security Package

2.2   List of Definitions

Unless the context otherwise requires and save where otherwise defined in this document, terms and expressions defined in the Code shall have the same meaning in this document.

Communication Requirements Document Specific Definition(s).

Normal Business Hours	9.00 a.m. to 5.00 p.m.[1] Monday to Friday on a Working Day.
Participant	Parties, Party Agents and others that communicate or intend to communicate with BSC Agents.
Qualification	Recognition that a BSC Party or Party Agent has satisfied the communication requirements specified under Section O of the BSC, and that these systems have been tested according to this document.
Qualification Statement	Statement of Qualification issued by the BSC CSA on behalf of BSCCo on completion of Qualification.
Qualification Tests/ Qualification Test	Tests undertaken by a Qualifying Participant. The tests provide the appropriate level of assurance that the necessary communication links between the Qualifying Participant and BSC Agents will function correctly under operational conditions.

---

[1] Please note that certain BSC Central Services do operate outside of these core hours.

Receipt of Data	Data received by the CRA, SAA and CDCA BSC Services (other than meter readings) outside of Normal Working Hours are deemed to have been received at 08:00 on the next day.
Service Provider	The Company who provides the electronic communications service medium through which Parties and Party Agents communicate with the BMRA, CRA, CDCA, ECVAA and SAA.
User Licence	A licence allocated to an individual in a Party not to a Party.
Waiver	Recognition that a Qualifying Participant is sharing facilities with another Participant who has previously satisfied the Qualification requirements, and as such that Qualification Tests would be duplicated if undertaken by the Qualifying Participant.
XSec	Security software provided by the Service Provider.

3.   Receipt of Communication for the BMRA, SAA, ECVAA, CRA and CDCA

3.1   Deemed Receipt of Communications to and from BSC Agents.

Where the Code or any BSC Procedure requires that communications should be delivered to any of the BMRA, SAA, ECVAA, CRA or CDCA by or within a particular time, it shall be the responsibility of the Party, of the Party Agent or of the Market Index Data Provider (as the case may be) except in circumstances defined in Section G of the Code, to ensure that the communication arrives at the relevant BSC Agent System by or within the time specified in accordance with the defined Time Standard.

When transferring a file to a BSC Agent System, it is the responsibility of the Participant to transfer the file to the temporary receipt directory using FTP and then to move the file from the temporary receipt directory to the inbox using the 'rename' function.

Communications will be deemed to have been received by the BSC Agent, for the purposes of Settlement, at the time when the file has been moved from the temporary receipt directory to the inbox using the 'rename' function, provided that the communication (and its content) is in a form which is capable of being processed by the BSC Agent at the time when the BSC Agent is to process such communication, in accordance with the Code, for the purposes of Settlement.

For notifications made via the ECVAA Web Service, the deemed time of receipt described will be the same as the timestamp displayed on the confirmation screen once a notification file has been sent to ECVAA.

For the avoidance of doubt, a communication which is deemed to be received in accordance with the foregoing provisions of this paragraph must also fulfil, at the time of such receipt and at the time of processing, any conditions as to the validity of a communication (or the data contained in a communication) set out in the Code and/or any BSC Procedure, and the rules in this Communication Requirements Document as to when a communication is deemed to be received are without

prejudice to any other rules in the Code and/or BSC Procedures regarding the submission or receipt of data.

Communications will be deemed to have been received by the Participant when:

(a)   For a High Grade connection using the 'push' process, the electronic message has been delivered to the Participant, as described in Section 4.6.4;

(b)   For a Low Grade connection or High Grade connection using 'pull', the electronic message has been posted into the relevant directory ready to be 'pulled' by the Participant; and

(c)   For fax transmission, the fax has been sent.

(d)   For email transmission, five minutes after the email has been sent.

3.2   Deemed Receipt of Credit Default Notices

Each Trading Party shall, prior to the commencement of trading as a Trading Party under the Code, provide to BSCCo the telephone number of a telephone capable of receiving voicemail and/or text messages, specifying which message forms may be used and shall ensure that the telephone remains operative and capable of receiving voicemail or text messages as specified on that number at all times (which BSCCo will then forward to the ECVAA). Each Trading Party shall also submit an e-mail address, prior to the commencement of Trading as a Trading Party. A Trading Party, may from time to time, change the telephone number or e-mail address on giving at least 2 Business Days' notice thereof to BSCCo.

For each Trading Party in Credit Default, in accordance with Section M of the Code, the notice of Level 1 or Level 2 Credit Default shall be communicated to that Trading Party and BSCCo via email by the ECVAA and a telephone call (or voicemail and/or text messaging, if necessary) sent to the telephone number most recently notified by that Trading Party to BSCCo. The ECVAA will record the time at which this message is sent and the notice will be deemed to have been received 5 minutes after the time recorded by the ECVAA.

If the Party is in Level 1 Credit Default or a Level 2 Credit Default and BSCCo has authorised the Credit Default status, the ECVAA will notify the default status to the Trading Party and post a Level 1 or Level 2 Credit Default statement on the BMRS in relation to that Party as soon as is practicable confirming the time the notice was deemed to have been received.

In addition, Credit Default Notices, including details of Parties that have cleared Credit Default, shall be posted on the BMRA website.

3.3   Time Standard

The Service Provider shall ensure its systems are set in accordance with Co-ordinated Universal Time (UTC), adjusting the time as necessary, at least once every 24 hours.

For communications with BMRA, CRA, CDCA, ECVAA and SAA, Participants shall synchronise their systems using Network Time Protocol (NTP) to one of a number of time servers. The Service Provider makes available a list of suitable servers.

For the avoidance of doubt, in ascertaining the time at which a communication is deemed to be received in accordance with paragraph 3.1 above, the time to which the systems of either the Service Provider (or BSC Agent) or the Participant are set or synchronised when such communication is made shall not be considered conclusive evidence as to the actual time of making such communication. The time of receipt of a communication is determined by reference to 'actual' time.

4. Service Requirements – BMRA, CRA, CDCA, ECVAA and SAA

4.1. Introduction

This section defines the network communications services provided to support Participant communication with the BMRA, CRA, CDCA, SAA and ECVAA (including the ECVAA Web Service) only. The use of the term BSC Agents in this section 4 is confined to those five agents only. It describes the network infrastructure, software and security mechanisms that Participants use for the purpose of electronic communication with those BSC Agents.

The installation and maintenance is a managed service provided by the Service Provider.

4.2. Specification of Service

The service provides:

- secure transmission of electronic data files in both directions between the Participant systems and BSC Agents other than the BMRA; and

- provision of unencrypted Balancing Mechanism Reporting data from the BMRA service to Participant systems.

- provision of Credit Default Notices.

These facilities are provided through two grades of service delivery depending on the Participant's requirements, a High Grade or a Low Grade service. For both grades of service the FTP mechanism is used for file transfer with BSC Agents other than the BMRA.

4.2.1 High Grade Service Definition

This provides access to all services and data through private network communication.

For the BMRA service, the High Grade Service provides the capability for 24 hours a day, 7 days a week near real time information to be 'pushed' to the service users.

For the EWS, the High Grade Service provides the capability for 24 hours a day, 7 days a week, near real time notification data for Parties and Party Agents to view. Notification Agents may also create notifications from existing authorisations and submit then to ECVAA through the EWS.

The users can access this data either through browser screens (using Service Provider supplied applets to refresh the screens on receipt of updates), or through a defined programmatic interface (using TIBCo software) (BMRS data only).

4.2.2 Low Grade Service Definition

This provides access to all services and data through the public Internet, with consequently no guarantees on access times or availability.

The Low Grade Service provides access to BMRA data through a browser, but without the automatic refresh, the users are responsible for 'pulling' the data for screen based access and file downloads.

Users accessing the EWS using the Low Grade Service have access to the same services provided via the High Grade Service.

Certain items of BMRA data are also made available through the public Internet to the ETSOVista reporting platform (for republication to participants and stakeholders in the European Union's Internal Electricity Market). The file format and transfer mechanism for this interface are in accordance with specifications maintained by ETSOVista, and are outside the scope of this document.

4.3 Application for the Provision of Service

Participants shall place a service order with BSCCo for the grade of service required providing the following information:

- Party name(s);
- Contact name of individual responsible for request;
- Telephone and fax numbers;
- Email address; and
- Grade of service required.

If the Participant is ordering the High Grade Service further information may be required from the Participant by the Service Provider during the installation of this service. This information is outlined within documentation provided by the Service Provider.

A Participant may request both the High Grade and the Low Grade Service. Documentation associated with High and Low Grade Services should be ordered through the Service Provider.

One or more Participants may share the physical connection for a High Grade Service installation. Where a High Grade installation is to be shared the Participant should inform BSCCo. This request will be passed to the Service Provider who will contact the Participant to assess the impact and provide options for increasing bandwidth, if required.

If a person who is not a Party requests access to the BMRS via the High Grade service, BSCCo will not accede to this request unless the person agrees to enter into an appropriate contract with BSCCo under which the relevant costs specified in Section D of the Code can be recovered.

For access into the EWS via either High Grade or Low Grade service, a BSC Party[2] or Notification Agent will need to request access to the EWS from the Service Provider following the process described in BSCP71.

---

[2] Note that non-Parties (other than Notification Agents) may not gain access to the EWS

4.4 Availability

Planned BSC Agent downtime applies only to the BMRA and ECVAA services and will be agreed between the Service Provider and BSCCo at least a week in advance.

BSCCo will inform all Parties and Party Agents of such agreement immediately. Note that Section O paragraph O 4.3.3 of the Code specifies that Parties are not able or entitled to send or receive Communications to or from the relevant BSC Agent during planned BSC Agent downtime.

4.5 Security

The network is designed to prevent external unauthorised penetration, in accordance with commercial security standards, including the use of firewalls at the Service Provider site.

Both grades of service provide Participant data confidentiality and originator authentication for file transfer between Participant site and Service Provider site.

This is accomplished using the security utility (XSec) provided by the Service Provider that supports OpenPGP encryption. The management of the security keys is handled through the Service Provider.

The passwords used when connecting with the system must be changed at regular intervals to comply with security standards, as determined by the Service Provider. Currently, XSec keys are scheduled to expire after five years.

If Participants become aware of a security breach or wish to change their keys and passwords before the scheduled expiry time, they should immediately contact the BSC Service Desk. Participants and the Service Provider must make all reasonable endeavours to maintain the security of the system, and correct any weaknesses revealed. The Service Provider may decide to take additional security measures and transmit security instructions to Participants, as necessary.

4.5.1 *This section is not currently in use*

4.5.2 *ECVAA Web Service Security*

The security access is based on the secure protocol HTTPS. HTTPS uses a secure encrypted link between the browser and the ECVAA Additionally, an encrypted credentials file is submitted for each user at the point of logging on. ECVAA then decrypts the file and validate the users log on against that file. Where the details provided by the user when logging on do not match the details in the encrypted credential file, then the ECVAA will fail the user and prevent their logging in.

Responsibility for controlling access to the EWS is with the individual Party and Party Agent EWS administrators, whereby the administrator ensures that encrypted credential files are created and available only to the required users. Parties and Party Agents enforce their own security protocol regarding usage (time, length and re-usage) of passwords, subject to basic minimums published by the Service Provider.

The credentials file should be encrypted by the Administrator using the XSec encryption software currently used by Parties and Party Agents to protect data sent to and received from ECVAA.

4.6 Technical Specification – High Grade Service

4.6.1 Network Communications

The High Grade Service consists of a number of MPLS connection options and are detailed as follows:

Technical Specification	Line Options								
	HG1a	HG1b	HG2a	HG2b	HG3a	HG3b	HG4	DR1	DR2
Primary Line Rental:									
256Kb Lease Line	✓	✓	✗	✗	✗	✗	✗	✗	✓
512Kb Lease Line	✗	✗	✓	✓	✗	✗	✗	✗	✗
1Mb Lease Line	✗	✗	✗	✗	✓	✓	✗	✗	✗
2Mb ADSL	✗	✗	✗	✗	✗	✗	✓	✓	✗
Backup Line Rental:									
ISDN Backup	✗	✓	✗	✓	✗	✓	✓	✗	✗
2Mb ADSL Backup	✓	✗	✓	✗	✓	✗	✗	✗	✗
Support:									
5 Hour Fix on Primary Line	✓	✓	✓	✓	✓	✓	✗	✗	✓
24 Hour Fix on Primary Line	✗	✗	✗	✗	✗	✗	✓	✓	✗
1-1 Contention Ratio	✓	✓	✓	✓	✓	✓	✗	✗	✓
20-1 Contention Ratio	✗	✗	✗	✗	✗	✗	✓	✓	✗

In addition to protect against loss of the connection to the MPLS network a backup ADSL or Basic Rate ISDN line will be provided.

Variations to this standard specification to support, for example, multiple participants using the same High Grade Service will be handled by the BSCCo, in conjunction with the Service Provider, on a case by case basis.

The geographic scope of supply for communication lines is the United Kingdom. Participants who wish the connection termination to be outside the United Kingdom are required to contact BSCCo to make specific arrangements with the Service Provider.

The service includes the provision of a router with the following characteristics:

- the router will support TCP/IP;

- the interface presented on the Participant side of the private network router will be Ethernet 10/100 BaseT; and

- the router will support Network Address Translation (NAT), and the Service Provider will liaise with the Participant to ensure that the correct IP address space translations are configured.

- Participants shall order TIBCo software through BSCCo with signed Licences being returned to the Service Provider.[3]

4.6.2 *Software*

The software is:

- Participant Security Package, XSec.

- TIBCo Software[4].

4.6.3 *Responsibilities*

The Participant is responsible for placing a service order with BSCCo who will then instruct the Service Provider.

The Service Provider will then provide to the Participant:

- Participant Security Package; and

- Router and communications lines.

The Participant may also acquire:

- The TIBCo Software.

However, if a Participant is already in possession of an adequate number of the appropriate TIBCo Software licences then they do not need to take this item.

The Participant is responsible for:

- provision of one or more workstations for accessing the High Grade Web Service (optional) to the minimum specification as defined from time to time by the Service Provider;

- provision of LAN, including connection to the router;

---

[3] Participants may also use any existing TIBCO licences available to their organisation or procure TIBCO licences other than from BSCCo to access the BSC Central System TIBCO service.

[4] The TIBCo Software is optional and will be at an additional charge.

- provision of FTP client software (mandatory) and FTP server software (mandatory only for High Grade Push); each High Grade Participant must select either 'push' or 'pull' mode for receipt of files from the Service Provider. Full details of directories, user identification etc. are provided by the Service Provider;

- all cabling on the Participant side of the supplied router;

- synchronising their machine clocks with an NTP server (the Service Provider supplies an NTP service to High Grade users. Optionally the participant can instead choose to synchronise with a UTC source of their choice. The Service Provider can suggest appropriate sources);

- provision of a suitable environment for the supplied telecoms equipment, including uninterruptible power, suitable environmental conditions and reasonable provision of site access when required by the Service Provider;

- provision of IP addressing information for configuration of the router in liaison with the Service Provider as to suitable addressing ranges;

- provision of software which is capable of producing and responding to flows as defined in the BSC Central Systems IDD.

Further, it is not mandatory but strongly recommended that the Participant:

- obtain a contract with an ISP for Internet connectivity to allow the Participant to use the Low Grade Service, ordered from BSCCo, as a backup mechanism and provide any necessary hardware, cabling and software to support the link; and

- provide and configure a firewall to protect the Participant's LAN.

4.6.4   Boundary of Responsibility

The High Grade communications service will terminate at the LAN interface of the router at a Participant's site. The router will be supplied and installed as part of the installation of the private line. The Participant is responsible for the connection of the router to the Participant's Local Area Network (via a firewall if this is required).

4.7 Technical Specification - Low Grade Service

4.7.1 Network Communications

Network Communication is through the public Internet.

4.7.2 Software

The software is:

- Participant Security Package, XSec.

4.7.3 Responsibilities

The Participant is responsible for placing a service order with BSCCo who will then instruct the Service Provider.

The Service Provider will then provide the Participant with:

- Participant Security Package, XSec.

The Participant is responsible for:

- provision of a workstation and operating system software to the minimum specification as defined from time to time by the Service Provider;

- provision of FTP client software. When using FTP to send files, Internet-connected Participants must always 'push' files to the BSC Agents. Across the Internet, Participants must always 'pull' files from the BSC Agents. Full details of directories, user identification etc. are provided by the Service Provider;

- obtaining a contract with an ISP for Internet connectivity; provision of any necessary hardware, cabling and software to support the link;

- synchronising the workstation with an Internet NTP server (the Service Provider will supply suitable DNS information, if one is not supplied by the Participant's ISP);and

- provision of software which is capable of producing and responding to flows as defined in the BSC Central Systems IDD.

Further, it is not mandatory but strongly recommended that the Participant:

- provide and configure a firewall to protect the Participant's workstation, if this is required.

4.8   Installation

The full technical details of installation are provided by the Service Provider after receipt of a service order

The Service Provider will undertake basic tests, as part of the installation, to ensure that Participants can communicate with the BSC Agents.

The Participant must make all reasonable endeavours to allow site access to the Service Provider for installation and subsequent maintenance.

4.9   Management of Service

The Participant acquires a fully managed service for High Grade Services which includes the maintenance of the communication lines, router, and software provided. The Service Provider operates the BSC Service Desk. Full contact details can be obtained from BSCCo through the following email address: market.entry@elexon.co.uk .

4.10   This section is no longer in use

4.11   Termination

On termination of High Grade Service the Participant shall be responsible for allowing the Service Provider to remove all communication lines and routers and returning all software and documentation, other than that required for the Low Grade Service.

In the event of withdrawal or expulsion from participation under the Code, a Party shall permit the Service Provider to remove all communication lines and routers and shall return to the Service Provider all software and documentation, and OpenPGP encryption details.

Termination of the service will be immediate upon receipt by the Service Provider of notice from BSCCo. Communication lines and routers will be removed as soon as practical thereafter.

4.12   Disaster Recovery and Standby Sites

The High Grade Service specification applies to all physical sites at which it is installed. A Participant may request variations to the specification for its disaster recovery site. This should be raised through BSCCo where it will be handled on a case by case basis.

4.13   Restrictions

The TIBCo and security services provided by the Service Provider require a Windows operating system environment. The currently supported versions of the Windows operating systems are available on request from the Service Provider.

The software licences are provided for the sole purposes of access to the BSC Agents. They may not be transferred to another organisation. Nor can they be used for the operation of another computer system.

4.14 Variations

All requirements for variation to the service specifications given in this document must be raised through BSCCo where they will be handled on a case by case basis. Any cost differential will be agreed for the variation and reflected as a separate charge.

4.15 Service Upgrades

From time to time it may be necessary to upgrade the software. Additional charges may apply at this time.

4.16 Testing of Participants' Communication

Participants' ability to communicate with the BSC Agents will be tested, with the exception of Non Party access to the BMRS via the High Grade Service. This testing will encompass Qualification Tests – where the ability of Participants to send and to receive appropriate flows (as defined in the Data File Catalogue) as part of an integrated business activity will be tested.

BSC Parties and CVA MOAs are able to opt out of some or all tests if they so choose. It should be understood that this shall be entirely at their own risk.

ECVNAs and MVRNAs will need to complete all the tests. Therefore all flows in any one of the groups defined in the tables below must be successfully tested before any flows in that group may be used.

Testing is initiated by the Participant as outlined in BSCP70. CVA Qualification Tests and Applications for Waivers of CVA Qualification testing will be undertaken in accordance with BSCP70 and successful completion of CVA Qualification will be notified by means of a Qualification Statement issued by the BSC CSA on behalf of BSCCo.

Parties or Party Agents who have not registered to use either the High Grade service or the Low Grade service and who have elected not to receive any electronic data flows by completing the procedure defined in BSCP41 – Reporting Requests & Authorisation will not be required to undertake tests relating to any electronic data flows. Such tests, if requested by the Party or Party Agent, will be undertaken at the point when the Party or Party Agent registers to use either the High Grade service or the Low Grade service.

Where a Party or Party Agent shares an administrative organisation or software with another Party or Party Agent, tests relating to any specific flow may be waived at the discretion of BSCCo on production of evidence that the specific flow has previously been successfully tested using the same version and configuration of the software which is involved in generating or receiving the flow. Such a waiver is not automatic and BSCCo may require tests to be undertaken where there is any doubt as to the

degree of sharing of administrative function, the identification of the software product or module, the nature of the configuration or any other matter of doubt.

Any intention of changes to software that may directly affect one or more data flows must be notified by the Party to BSCCo. BSCCo may require Participants to re-test if a significant risk to interfaces is identified.

4.17 Qualification Tests

The set of data flows a Participant will test depends on the capacity or role of the Participant, as defined in section 5.

The tests are carried out by the Service Provider on behalf of the relevant BSC Agents.

In each case the flow must be of valid format and contain valid values, it is not necessary for the file or message to include valid business data, and it is accepted that the data may not be valid in respect of its relationship to other data held by that Participant or the Service Provider.

4.17.1 *Correct generation of all Relevant Files / Messages and Transfer to the Service Provider.*

(a) Electronic Data Flows

For each relevant data flow the Participant must demonstrate that their application can generate a valid file / message containing test data (the file / message must be in the correct format and contain valid values) and deliver this to the destination system (via an appropriate network). The receipt and recognition of this flow by the Service Provider will demonstrate the correct generation of the flow by the Participant.

Evidence that the test has been successfully completed will include evidence from the Participant that the file was generated from the application concerned and, where applicable, evidence that the application has accepted the resulting acknowledgement.

(b) Manual Data Flows

This section is no longer in use.

4.17.2 *Receiving Valid Files / Messages Generated by the Service Provider.*

(a) Electronic Data Flows

For each relevant data flow the Participant must demonstrate that their application can receive, recognise and accept a valid flow (via the appropriate network) at the application designated to be the recipient for that flow.

On receipt of a file / message the application must be able to demonstrate that the file / message has been received, and that the structure of the flow has been recognised and validated.

Evidence that the test has been successfully completed will include evidence from the Service Provider in the form of a file print out of the generated file. The receiving Participant will provide a file printout of the file received. Some evidence that the file has been received and understood by the receiving application must be provided. This may include database extracts, screen prints etc.

(b)   Manual Data Flows

This section is no longer in use.

4.17.3   Correct Rejection of all Received Invalid Files / Messages.

(a)   Electronic Data Flows

Tests under this heading are not intended to be exhaustive. The tests are to show the general readiness of the Participant.

A number of invalid files will be produced by the Service Provider which are relevant to each Participant capacity or role. Each Participant must be able to demonstrate that they correctly reject these flows. The invalid flows will only test for incorrect format or structure of the file. Invalid business content is out of scope.

Evidence that the test has been successfully completed consists of the receipt of an automatic rejection at the Service Provider, together with a confirmation from the Participant that the data flow was seen and errors detected.

(b)   Manual data flows

This section is no longer in use.

5. Definition of Data Flows to be Tested

The flows to be tested are specified below. The flows are identified by reference to the CVA Data Catalogue.

5.1 Registration Activity

5.1.1 Flows requiring testing

Flow	Dir'n	Roles	Name
CRA-I014	to	All	Registration Report

5.2 Metering Activity

5.2.1 Flows to be tested when triggered by registration

Some flows are only applicable where Parties are the Registrant for Meters. Parties who are not Meter Registrants are not required to test the relevant flows.

Flow	Dir'n	Role	Name
CDCA-I010	to	Registrant	Exception Report for missing and invalid meter period data
CDCA-I012	to	Registrant	Report Raw Meter Data
CDCA-I014	to	Registrant	Estimated Data Report
CDCA-I029	to	Registrant	Aggregated GSP Group Take Volumes
CDCA-I030	to	LDSO	Meter Period Data for Distribution System
CDCA-I041	to	Registrant (IA)	Interconnector Aggregation Report
CDCA-I042	to	Registrant of BM Unit only	BM Unit Aggregation Report
CDCA-I054	to	Registrant	Meter Status Report
SAA-I006	from	Registrant (IA)	Interconnector Deemed Metered Amounts
SAA-I017	to	Registrant (IA), MIDP	Issue SAA Data Exception Reports

5.3 Trading Flows

5.3.1 Flows Requiring Testing

Flow	Dir'n	Roles	Name
ECVAA-I007	to	Trading Party	ECVNAA Feedback
ECVAA-I008	to	Trading Party	MVRNAA Feedback
ECVAA-I009	to	Trading Party	ECVN Feedback
ECVAA-I010	to	Trading Party	MVRN Feedback
ECVAA-I013	to	Trading Party	Authorisation Report
ECVAA-I014	to	Trading Party	Notification Report
ECVAA-I022	to	Trading Party	Forward Contract Report
ECVAA-I028	to	Trading Party	ECVN Acceptance Feedback
ECVAA-I029	to	Trading Party	MVRN Acceptance Feedback
SAA-I014	to	Trading Party	Settlement Reports

5.4 Party Agent Flows

5.4.1 ECVNA Flows Requiring Testing

Flow	Dir'n	User	Name
CRA-I014	to	ECVNA	Registration Report
ECVAA-I004	from	ECVNA	ECVNA
ECVAA-I007	to	ECVNA	ECVNA Feedback
ECVAA-I009	to	ECVNA	ECVNA Feedback
ECVAA-I013	to	ECVNA	Authorisation Report
ECVAA-I014	to	ECVNA	Notification Report
ECVAA-I028	to	ECVNA	ECVN Acceptance Feedback

5.4.2 MVRNA Flows Requiring Testing

Flow	Dir'n	User	Name
CRA-I014	to	MVRNA	Registration Report
ECVAA-I005	from	MVRNA	MVRNAs
ECVAA-I008	to	MVRNA	MVRNA Feedback
ECVAA-I010	to	MVRNA	MVRNA Feedback
ECVAA-I013	to	MVRNA	Authorisation Report
ECVAA-I014	to	MVRNA	Notification Report
ECVAA-I029	to	MVRNA	MVRN Acceptance Feedback

5.4.3 MOA Flows Requiring Testing

Flow	Dir'n	User	Name
CRA-I014	to	MOA	Registration Report
CDCA-I010	to	MOA	Exception Report for Missing and Invalid Meter Period Data
CDCA-I014	to	MOA	Estimated Data Report
CDCA-I054	to	MOA	Meter Status Report

5.5 MIDP Flows Requiring Testing

Flow	Dir'n	User	Name
BMRA-I015	from	MIDP	Market Index Data
SAA-I030	from	MIDP	Market Index Data

6. Communications Relating to the FAA

The FAA shall send Advice Notes, Confirmation Notices and Advice Note Backing Sheets to a Party by e-mail to the Payment Notice e-mail address submitted by that Party from time to time in accordance with BSCP301. All other notices or other communications contemplated by the Code or Code Subsidiary Documents to be given by the FAA to a Party shall be sent to the contact e-mail address submitted by that Party from time to time in accordance with BSCP301.

Notices or other communications sent by e-mail between the FAA and Parties shall, for the purposes of the Code and Code Subsidiary Documents, be deemed to have been received one hour after being sent in the absence of any undeliverable return receipt received by the sender, except that if the time at which the e-mail is deemed to have been received falls after 17.00 hours on a day, the notice or other communication shall be deemed to have been received at 09.00 hours on the following day.

The FAA shall send separate e-mail messages for each Advice Note, Confirmation Notice or Advice Note Backing Sheet.

No testing of communications between Participants and the FAA will be required.

Qualification Tests are not required for the FAA under this document.

7. Service Requirements – TAA

All communications with the TAA will be by telephone or email. Parties who need it will be provided with the necessary telephone numbers and email address(es).

No testing of communications between Participants and the TAA will be required.

Qualification Tests are not required for the TAA under this document.

8. Managed Data Network Service

This service is provided by Electralink under the Data Transfer Services Agreement and all interfaces are defined in the SVA Data Catalogue.