CP1328 – Communication Requirements Document Redline Text v0.1

Section 1 – Section 2.1 - No changes

Amendments to existing definitions in Section 2.2 'List of Definitions'

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	Certificate of Qualification issued by 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.
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.
~~**Service Security Office**~~	~~A Service Provider designated Office which is responsible for managing the security of the system. Contact details of the Service Security Office are published in BSCCo circulars.~~
User Licence	A licence allocated to an individual in a Party not to a Party.

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

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.

Section 3 – Section 4.4 - No changes

Amendment to Section 4.5: Update references of Service Providers Helpdesk with BSC Service Desk

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 ~~Service Provider's Helpdesk~~BSC Service Desk or Service Security Office. 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. ~~The contact details for the Service Security Office will be published in BSCCo circulars from time to time~~.

Section 4.5.1 - No changes

Amendment to Section 4.5.2: Deletion of text on Credential files as this practice is outdated

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.

~~Credentials files are created by the Administrators and are of a specific format as described within the EWS Pack (issued to Administrators requesting access to the EWS on behalf of their organisation which is acceptable to ECVAA. The Credentials file will contain fields specifying a username, password, unique identifier, the role the user is to take on (Admin, read only or edit), inactivity timeout time, time band and the effective dates of the credentials file.~~

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.

Section 4.6 – 4.8 - No changes

Housekeeping amendments to Section 4.9'Management of service': Update references of Service Providers Helpdesk with BSC Service Desk and merging of section 4.10 due to duplication of text.

4.9 Management of service and Failure

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 ~~a help desk.~~ the BSC Service Desk. Full contact details can be obtained from BSCCo through the following email address: market.entry@elexon.co.uk.

Deletion of text in Section 4.10 due to duplication of text with Section 4.9.

4.10 -This section is no longer in use

~~**Failure**~~

~~***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 a help desk. the BSC Service Desk. Full contact details can be obtained from BSCCo.***~~

Section 4.11 –Section 4.15 – No Changes

Amendments to Section 4.16: Update reference to BSCCo Service Desk with BSC Service Desk

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.

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 registering a request with the BSC Service Desk~~BSCCo help desk~~. Qualification Tests and Applications for Waivers of Qualification testing will be undertaken in accordance with BSCP70 and successful completion of Qualification will be notified by means of a Qualification Statement issued by 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.

Sections 4.17 – 8 – No Changes