Participant Guidance
Participant Communications Overview Guide (PCOG)

Customer	:	ELEXON
Contract number	:	
Business/project number	:	GIS34511
Project Manager	:	Martin Wiles
Reporting to	:	Chris Beale
Project/document reference	:	IF-00000287
Issue	:	4.0
Issue date	:	01/12/14
Status	:	Definitive
Distribution	:	As per distribution list on page 2

Prepared by	:	Nick Brooks	Author **Date:**
Approved (CGI)	:	Martin Wiles	Service Provision Manager **Date:**
Approved (CGI)	:	Chris Beale	Service Delivery Manager **Date:**
Authorised (CGI)	:		Programme Director **Date:**
Accepted (ELEXON)	:		Role **Date:**

Reviewers

Name	Role
Andrew Alcock	*Configuration Manager*
Martin Wiles	*Service Provision Manager*
Sam Daniel	*Server Infrastructure*
Andrew McDonald	*Network Infrastructure*
Chris Beale	*Service Delivery Manager*

Distribution List

Name/Role	Organisation
UKEST Programme Library	*CGI*
Participant IT Support	*Participant Organisation*

Detailed contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide an overview of BSC Central Services for organisations intending to become BSC Market Participants. It is derived from the more detailed Participant Communications Installation Guide (PCIG) which is available to participant organisations on request from the BSC Service Desk, contact details for which are provided in section 11 of this document.

1.2 Scope

Since this is an overview document, it references other more detailed procedures, documents and instructions including the Participant Communications Installation Guide (PCIG).

1.3 Summary

- Participant Communications Overview Guide.
- Guidance document for new BSC Central Services Participants.

1.4 Amendment history

date	issue	description	author	OR no.
28/04/08	0.1	First draft, derived from 09-10033301	Mark Gribble	N/A
30/04/08	1.0	Issued	Mark Gribble	N/A
09/01/09	1.1	Updated for changes resulting from Project ISIS	Paul Pettitt	N/A
17/02/09	1.2	Rebadged as IF-00000287 and further updates for Project ISIS	Mark Gribble	N/A
24/02/09	2.0	Accepted by ELEXON made definitive	Bron Roddis	N/A
01/12/14	3.0	Maintenance Update	Nick Brooks	N/A

1.5 References

tag	title	doc reference	version
[XUG]	XSec Version 3 User Guide	AS-00000184	1.0
[TUG]	Tibco User Guide	01-100308	2.4
[CRD]	Communications Requirements Document*	N/A	N/A
[IDD]	BSC Interface Definition and Design (IDD) Pt 1	07-550201	Latest

tag	title	doc reference	version
[PCIG]	Participant Guidance: Participant Communications Installation Guide (PCIG)	IF-00000018	12.1

**The CRD is an ELEXON document, available via the ELEXON website*

1.6 Abbreviations

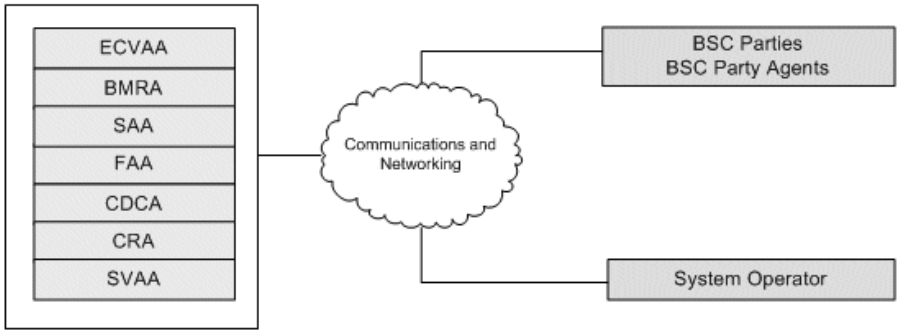
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BM	Balancing Mechanism
BMRA	Balancing Mechanism Reporting Agent
BP	BSC Party (Participant role code)
BRI	Basic Rate Interface (ISDN with two data channels)
BSC	Balancing and Settlement Code
CDCA	Central Data Collection Agent
CIR	Committed Information Rate
CRA	Central Registration Agent
CSV	Comma Separated Values
CVA	Central Volume Allocation
DNS	Domain Naming System
DPP	Daily Profile Production
DR	Disaster Recovery
DTI	Department of Trade and Industry
ECVAA	Energy Contract Volume Aggregation Agent
ECVNA	Energy Contract Volume Notification Agent
FAA	Funds Administration Agent
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HHDA	Half Hourly Data Aggregator
HSRP	Hot Standby Routing Protocol
IDD	Interface Definition and Design
IP	Internet Protocol

ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
JVM	Java Virtual Machine
LAN	Local Area Network
NAT	Network Address Translation
MDD	Market Domain Data
MPLS	Multi Protocol Label Switching
NHHDA	Non-Half Hourly Data Aggregator
NTP	Network Time Protocol
PVC	Permanent Virtual Circuit
RSA	Rivest Shamir Adleman (algorithms/creators of)
RVD	Rendezvous Daemon
RVRD	Rendezvous Routing Daemon
SAA	Settlement Administration Agent
SO	System Operator
SLA	Service Level Agreement
SVA	Supplier Volume Allocation
SVAA	Supplier Volume Aggregation Agent
TAA	Technical Assurance Agent
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

2 BSC Central Services

The services provided by CGI ("the Service Provider") to support the operation of the Balancing and Settlement Code (BSC), require market Participants to communicate electronically with CGI's systems.

Network communications access to the BSC Central Services is provided through three networks, the CVA WAN (or "CVA High Grade Service") and the internet (or "CVA Low Grade Service") for CVA Services, and the Electralink DTS network (or "SVA Network") for SVA Services.



It should be noted that the focus of this document is on BMRA, ECVAA, CRA, CDCA and SAA. The FAA and TAA (not shown) involve only manual communications as specified by the Communications Requirements Document [CRD]. The System Operator is not addressed here.

2.1 Energy Contract Volume Aggregation Agent (ECVAA)

The role of the ECVAA is to collate and provide to the Settlement Administration Agent (SAA) all energy contract volume and metered volume reallocation data.

2.2 Central Data Collection Agent (CDCA)

The Central Data Collection Agent (CDCA) collects, validates, processes and aggregates metered data associated with Metering Systems registered with the Central Registration Agent (CRA). It does this within the timescales required to enable settlement to meet the Payment Calendar.

2.3 Balancing Mechanism Reporting Agent (BMRA)

The role of the BMRA is to provide near to real-time reporting of all market information disseminated by the System Operator (SO) and submitted to the Balancing Mechanism (BM) from market Participants.

2.4 Central Registration Agent (CRA)

The role of the CRA is to maintain a master register of information relating to the registration of Participants, trading units and physical plants such as Boundary Points and interconnectors.

2.5 Settlement Administration Agent (SAA)

The role of the SAA is to calculate the credit and debit payments resulting both from trades made in the Balancing Mechanism (BM) and from imbalances between contracted and actual generation or consumption.

The SAA creates and publishes a Settlement Calendar on an annual basis to ensure that all Settlement calculations and Settlement Runs are performed in a timely manner so that payments are made on the intended dates.

2.6 Funds Administration Agent (FAA)

The FAA is responsible for transacting the payments and charges applicable as determined by the SAA.

2.7 Technical Assurance Agent (TAA)

The TAA is concerned with the technical assurance of all Metering Systems registered with the CRA. The overriding aim of this service is to support the quality of meter data that is used in the settlement process. The TAA provides a vital link in the end to end assurance of settlement data by reviewing the very source of the data, the Metering System and its associated equipment.

2.8 Supplier Volume Allocation Agent (SVAA)

The SVAA is responsible for producing MDD, DPP and calculating Supplier BM Units meter volumes using data provided by the Suppliers' HHDAs and NHHDAs.

3 Electronic Interfaces to BSC Central Services

3.1 Communications Access to BSC Central Services

The interface with the SVA element of BSC Central Services is via the DTS network. This is a service provided by Electralink.

There are two methods of electronic communication with the CVA elements of BSC Central Services, referred to as the High Grade and Low Grade services.

The High Grade service is provided using dedicated communications lines installed and managed by BSC Central Services. These lines connect the Participant to BSC Central Services over an MPLS based private WAN.

The Low Grade service is provided via the public internet using connectivity provided and managed by individual Participants.

Although the primary distinction between the two grades of service is the ability of the Service Provider to commit to specific levels of performance and reliability, the guaranteed bandwidth of the High Grade service allows an enhanced method of BMRA data retrieval to be available.

3.2 Low Grade Interfaces

The interfaces available using the Low Grade Service over the public internet are:

3.2.1 Low Grade BMRA Web (BMRA)

Available at http://www.bmreports.com, the Low Grade BMRA website allows querying of current and historic Balancing Mechanism data, which is presented in tables, Java based graphs and downloadable as CSV files. The data provided is a static snapshot as the data exists at the time that the query is made.

The Sun Java Virtual Machine and Adobe Flash Player are required to use the full functionality of this site.

No authentication is required to view data, it is publicly available.

3.2.2 FTP Notification and reporting (ECVAA/SAA/CRA/CDCA)

Available at ftp.bmreports.com, the BSC Central Services FTP service allows submission of files containing BSC IDD formatted data flows to Central Services. Files placed on this server are picked up and processed, and responses and reports are placed on the server for the Participant to periodically poll for and collect.

This service requires login credentials which are supplied during the registration process.

3.2.3 ECVAA Web (ECVAA)

Available at https://www.ecvaa.com, the ECVAA web service allows an alternative method for Participants to view their positions and notify to the ECVAA service in a more interactive way than the standard FTP notification method.

The Sun Java virtual machine is required to use the functionality of this site.

This service has a login authentication process controlled by the Participant organisation and based on the security architecture used by the main BSC Central Services FTP service. It requires users to provide a username, password and a "credentials file" provided by their security administrator permitting them access to the service.

3.3 High Grade Interfaces

The interfaces available using the High Grade service over the BSC Central Services private WAN are:

3.3.1 Tibco (BMRA)

This service is only available using the High Grade service, and uses industry standard Tibco data transmission software to stream a subscription customised feed of Balancing Mechanism data to the Participant's site. The Participant can then use Tibco connectors to pass this data into their own applications or use it with the High Grade Enhanced BMRA web service detailed below in section 3.3.2.

3.3.2 Enhanced High Grade BMRA Web (BMRA)

This service is similar to the Low Grade BMRA web service described in section 3.2.1, but is enhanced for use with Tibco streamed BMRA data. Queries are initially served showing the latest available data, much as the Low Grade Service, but graphs, tables and tickers then update dynamically based on real-time data being streamed in via Tibco.

3.3.3 FTP Notification and Reporting (ECVAA/SAA/CRA/CDCA)

This is the same FTP service as described for the Low Grade service in section 3.2.2, except that it is accessed via the High Grade network.

3.3.4 ECVAA Web (ECVAA)

This is the same secure web service as described for the Low Grade service in section 3.2.3, except that it is accessed via the High Grade network.

4 Participant Hardware and Software Infrastructure

This section outlines the hardware and software requirements for a BSC Central Services Participant and which parties are responsible for provision and support of both hardware and software.

4.1 Hardware Requirements

4.1.1 High Grade WAN Communications (Mandatory for High Grade)

If a Participant chooses to use the High Grade service, they place an order for this service through ELEXON. Before this order is accepted, the Participant then engages in a technical prevalidation process with the Service Provider. The Service Provider liaises with the Participant to arrange installation of dedicated comms lines and a router to connect to the Participant's network.

The Participant will be responsible for providing technical details related to the installation throughout the order process, and must allow for reasonable and timely site access for the Service Provider's supplier during installation and in the event of any fault.

The Service Provider is responsible for operation and support of the comms up to the ethernet port on the provided router. The Participant is responsible for the network that they connect to the router.

The typical High Grade Service will comprise the following hardware:

- A 256Kbps MPLS Leased Line
- A 20:1 contended, 2Mbps ADSL backup line
- A Cisco 2801 rack mountable router with a 10/100Mbps ethernet port for connection to the Participant's network.

Several other communications options are available, including options for an ISDN backup line where ADSL is not available, and options for ADSL as a primary line to reduce cost (with compromises in SLA support and contention).

Appendix A of this document lists all communications options available for the CVA WAN, with their costs, specifications and suitability for specific purposes. CGI can provide advice to participants as to the best option for a new communications requirement.

The lead-time for installation of these communications lines is 55 working days from the date that the order is placed following technical prevalidation.

The High Grade communications service is completely managed through the Service Provider.

The Service Provider will discuss networking requirements with the Participant and will use reasonable endeavours to accommodate any special requirements that the Participant has, for example:

- Custom IP addressing
- Network Address Translation
- Upgraded communications for bandwidth and/or resilience
- Automatic failover if more than one service is ordered.

It is highly recommended that in addition to the inherent security of the network managed by the Service Provider, the Participant provides a firewall for their High Grade network connection.

The standard communications described above are suitable for a Participant registering and using up to three Participant IDs, using one instance of a Tibco server to retrieve real-time BMRA data and with up to five workstations accessing the BMRA web service. If a Participant's needs are higher than this they should consult the Service Provider to establish whether a more highly specified communications option is prudent.

4.1.2 Low Grade Internet Communications (Mandatory for Low Grade)

The Participant is responsible for sourcing, ordering and maintaining their own internet connectivity.

When the Participant provides their internet connectivity, they should consider the following points:

- They should synchronise their systems using a suitable time synchronisation protocol, and NTP is recommended. The choice of NTP server will depend upon the requirements and size of the environment to be synchronised. A recommended server list can be found at http://ntp.isc.org/bin/view/Servers/WebHome.
- They should ensure that they are able to access the BSC Central Services FTP Service (further details available from the Service Provider on request) using an FTP client. They should be able to access http://www.bmreports.com and https://www.ecvaa.com through a web browser.
- It is strongly recommended that the Participant provides a dedicated firewall platform for their internet connection.

4.1.3 Servers to Host Software Infrastructure (Mandatory)

All hardware on the Participant site (with the exception of the High Grade router and associated networking equipment) is provided and maintained by the Participant. The

Service Provider does not provide hardware or support hardware on which the Service Provider supplied software is installed.

4.2 Software Requirements

4.2.1 Trading Software (Mandatory)

The Participant is responsible for providing software which is able to conform to the BSC IDD for the generation of, recognition of and response to BSC data flows.

The Service Provider cannot provide recommendations for this software, but is aware of several vendors who are able to provide suitable software and can provide a list on request.

4.2.2 FTP Transfer Software (Mandatory)

The Participant is responsible for providing software for the transfer of files via FTP between themselves and BSC Central Services. Although use of a manual FTP client is acceptable, it is recommended that an automated solution is employed. Most of the commercially available trading software incorporates this functionality.

4.2.3 XSec Encryption Software (Mandatory)

All files transferred to and from Central Services by FTP are encrypted/decrypted using a piece of proprietary software called XSec. It runs on all variants of Windows 2000 and 2003 as well as Windows XP Professional (although some functionality, such as failover, is not supported on all operating system variants). It runs as a Windows service and has a file based interface - files are placed into input directories where they are picked up by XSec, processed and placed into output directories.

XSec provides encryption and signing functionality for all files to be sent to or received from BSC Central Services and is entirely automated, such that the successful receipt of a plaintext file from XSec implies that a secure, complete and validated transfer of data from BSC Central Services has occurred.

The XSec software uses public key encryption/signing technology which requires the Participant to create private and public keys. The public keys must then be sent to the Service Provider to be verified and applied to the Central Services encryption subsystem. The Service Provider will provide advice and assistance for this. (see helpdesk contact information in section11).

XSec does not provide FTP or trading software functionality.

The Participant is responsible for providing the hardware and software environment for this software and operating it, but the Service Provider provides support and assistance in configuring and troubleshooting.

The XSec software is highly customisable in order to be able to be tailored to the requirements of each Participant, and the Service Provider will provide advice and assistance for installation and configuration.

XSec is ordered via ELEXON during registration, and a separate user guide is supplied with the software.

4.2.4 BMRA Web Clients (Optional)

If the Participant wishes to use either of the BMRA web services (High Grade or Low Grade), they are responsible for providing their own web clients using Internet Explorer 6, Adobe Flash version 9 and Sun Java Virtual Machine (JVM) 1.5. Internet Explorer 6 is the only web client officially supported by these services.

4.2.5 ECVAA Web Clients (Optional)

In addition to the technologies required for use of the BMRA web services (Sun JVM, Internet Explorer 6), to use the ECVAA Web service a user requires a username, password and a credentials file supplied by their security administrator (within the Participant organisation). The user connects to the ECVAA Web server using an SSL enabled Internet Explorer browser and provides their username and credentials file, followed by randomly selected letters from their password.

The key component here is the credentials file. The Participant security administrator creates credentials files (using tools available from the Service Provider or by creating the files manually from specifications available from the Service Provider), specifying details such as username, password, file validity periods and user rights. The administrator encrypts these files using the XSec software discussed in section 5.2 (using the same keys employed for encryption of BSC FTP file flows) and provides the encrypted files to the user.

When the user performs a login, the ECVAA web service confirms that the credentials file supplied is from a verified source (established by means of decryption with the Participant's public keys) and that the credentials being supplied by the user match those in the credentials file.

It is recommended that a separate installation of XSec on a standalone machine is used for credentials file encryption, and the Service Provider supplies a targeted software installation pack for this purpose.

Note: The Service Provider's staff will never ask the Participant for their ECVAA web username or password, and users of the system should be advised that they should not provide these details under any circumstances.

4.2.6 Tibco Data Transmission Software (Optional – High Grade Only)

If the Participant has a High Grade Service and wishes to use the BSC Central Services BMRA Tibco data stream, they are responsible for providing a Tibco RVRD (server) and as many RVDs (clients) as they require.

The Tibco software can be sourced through ELEXON (Windows only), purchased directly from Tibco or the Participant can use any Tibco architecture they may already have within their organisation, subject to licence agreements

A separate Tibco user guide detailing Tibco setup specific to BSC Central Services is provided on request by the Service Provider.

The Tibco software has two components known as the RendezVous Daemon (RVD) and the RendezVous Routing Daemon (RVRD). The server (RVRD) is used to transfer data between sites, and then redistribute this data to local clients (RVDs).

The Service Provider operates a central RVRD which publishes real-time BMRA data. The Participant configures their own RVRD which connects to the BSC Central Services central RVRD and receives this data. The Participant RVRD then relays this data to local RVDs (e.g. workstations using the High Grade enhanced BMRA web service).

RVRD is a cross platform product, but is most commonly run on Windows. The Service Provider distributes, supports and tests only Windows environments. If the Participant wishes to use a non Windows Tibco configuration they should therefore ensure that they provide adequate platform support, and should source their Tibco software independently of ELEXON.

The Participant must contact the Service Provider before configuring an RVRD to ensure that the correct configuration is being used to avoid conflicts with other parts of the Tibco network.

In its default configuration, the RVRD server communicates with its RVD clients by using a local subnet broadcast, requiring the clients to reside on the same local network as the server. This is explained more in the networking section 9.

The Service Provider supports the specific application and configuration for Tibco that is being used for BMRA, and is also able to provide limited support and assistance for the Tibco product itself, with the ability to refer product defect queries directly to Tibco. The Service Provider will supply upon request their Tibco User Guide [TUG].

Note: The Tibco BMRA service only publishes current data. It is not able to be used for supply of historical data.

Note: Tibco data is also provided as day-behind flat files through the ELEXON Portal at https://www.elexonportal.co.uk. This is known as the BMRA Data Archive.

4.2.7 FTP Server Software (Optional – High Grade Only)

When a Participant sends files to BSC Central Services, they place the files on the BSC Central Services FTP server. When BSC Central Services respond, the default behaviour is that response files are placed on the BSC Central Services FTP server for the Participant to periodically poll and collect.

However, if a Participant is using the High Grade service, they may elect to provide an FTP server on their own site which BSC Central Services can push files out to directly as soon as they are generated. This is entirely optional.

5 Detailed Operation of Services

5.1 FTP Service Usage

A detailed description of how to use the BSC FTP Service is provided to participants by the Service Provider upon registration together with the XSec software and the full Participant Communications Installation Guide [PCIG]

5.2 XSec Software

The XSec software distributed by the Service Provider is required for all incoming and outgoing files. Operation and configuration of this software are covered by its own documentation, but this section provides a brief overview of its features and usage.

5.2.1 Application Overview

The XSec application uses PGP based public key encryption and signing to secure the contents of files transferred between Participants and BSC Central Services. It operates as a Windows service and is compatible and tested with Windows XP Professional as well as all variants of Windows 2000 and Windows 2003. It uses the .NET framework 1.1.

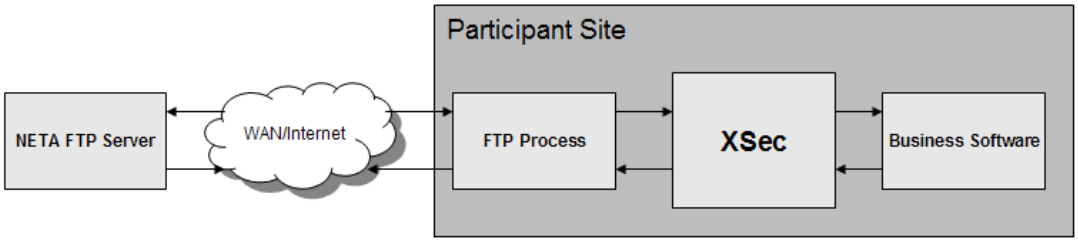
It uses a file based interface, polling input directories to look for files to encrypt/decrypt, and placing the processed files into output directories where it is assumed that other processes will pick them up.

For reliability, processes delivering files to XSec should always place files using instantaneous move operations to avoid the possibility of part written files being processed. XSec contains some protection against this, but in general it should be ensured that XSec's input directories are not written into directly.

BSC Central Services allows for this in the FTP push process described above by initially transferring the file to a temporary directory before renaming to a final destination. This final destination directory can be an XSec input directory.

5.2.2 Integration with Other Processes

XSec sits between the Participant's business software and the process which transfers files to and from BSC Central Services Central Services as per the diagram below:



5.3 Tibco Rendezvous Software

The High Grade Participant's Tibco RVRD server connects to the BSC Central Services Central RVRD to send subscriptions and receive real-time BMRA data. This software is covered by its own documentation which is provided to Participants on request, but this section covers some high level technical considerations for the Participant to be aware of in usage of the RVRD.

5.3.1 Approval of New RVRDs

Before configuring or connecting a new Tibco RVRD, the Participant must contact the Service Provider through the BSC Service Desk. The Service Provider will work with the Participant to ensure that this new RVRD will not cause any problems or conflicts to Participant or BSC Central Services infrastructure, and will configure access to the BSC Central Services RVRD.

5.3.2 RVRD Unique Naming

If the Participant chooses to use more than one Tibco RVRD, they must ensure that these RVRDs are configured with unique names on the BSC Central Services Tibco network. Presence of multiple RVRDs with the same name leads to conflicts which can cause loss of data and disruption of the RVRD network.

5.3.3 Offline/Standby Servers

The Participant should consult the Service Provider and the Tibco User Guide [TUG] about offline or standby servers installed with the Tibco software. This is to ensure that licensing rules are being correctly interpreted and to ensure that no situation can occur where the standby server might become active at the same time as another server with the same RVRD name.

5.3.4 BMRA Subject Naming

The messages distributed via the Tibco application are divided into logical segments using Tibco subject names. These are dot (.) delimited text strings which split BMRA data into hierarchical structures.

This can be useful for data analysis if the Participant is using the data for an application other than the High Grade Enhanced BMRA web site, such as a Tibco connector into their own application or database. This subject naming is covered in detail in the Tibco documentation supplied by the Service Provider during registration and in the BSC Interface Definition Documents (IDD) available from ELEXON's website.

6 Participant Disaster Recovery

The architecture used by BSC Central Services allows for Participants to provide resilience to disaster in their own systems. This section explains options that the Participant may wish to consider when designing their BSC Central Services infrastructure.

6.1 High Grade Push/Pull Switching

High Grade Participants are permitted at any time to switch between the push and pull modes of BSC Central Services file delivery by contacting the BSC Service Desk and requesting the change. This must be authorised by a BSCP38 Category A authorised signatory for the Participant ID/s in question. In emergencies this change can be carried out quickly, but Participants should ideally try to provide at least 48 hours notice.

Requesting a switch from push to pull is not necessary in some DR scenarios such as a loss or failure of the Participant's FTP server (since in the event of failure to push files, these files will be left on the BSC Central Services FTP server ready for pull), but it is realised that a Participant may wish to carry out a more controlled cutover under some circumstances, for example where their live FTP server is still active, but they wish to use their DR site.

Similar authorisation and notice should be provided when the Participant wishes to resume their original configuration.

6.2 High Grade Push to a Different Server

If a Participant has two sites on the BSC Central Services High Grade network and uses the FTP push option to have files delivered to their main server, then a move to their DR site will require the Participant to inform the Service Provider of the alternate IP address, login and directory structure details of the DR server if they wish files to be pushed to their DR site.

This is achieved by calling the BSC Service Desk, and in emergencies can be carried out at short notice. Authorisation from a BSCP38 Category A authorised signatory for the Participant ID in question is required.

It is highly recommended if a Participant wishes to use a DR facility that they do not use FTP push mode. Using pull mode instead provides greater flexibility for moving to DR without dependence on the Service Provider.

6.3 High/Low Grade Switching

All High Grade Participants are also automatically configured to be able to use the Low Grade internet based service, and in the event of a complete failure of access to the High Grade service the Participant may use the Low Grade FTP and web services as a disaster recovery strategy.

If the Participant wishes to use this as a disaster recovery strategy, they should ensure that their networks and firewalls are configured to allow their systems to access both networks. In most cases all that is required to switch to using the Low Grade service is a change of target from the High Grade IP addresses to the Low Grade IP Address (or preferably the Fully Qualified Domain Name for the Low Grade service). No involvement is required from the Service Provider for this type of switch.

The change from high grade to low grade, or vice versa, does not affect the file sequence numbers used for file transmissions. If there is any doubt as to which files have been transferred then the Participant operations staff will need to liaise with the Service Provider's staff, via the BSC Central Services helpdesk, to establish the most recent file received of each type.

6.4 Resilient High Grade Networking

If a Participant wishes to use more than one connection to the High Grade network in order to provide a disaster recovery position or improve their resilience, the Service Provider can work with them to find a suitable option.

The BSC Central Services networks team, contactable through the BSC Service Desk, can advise on these and other advanced network configurations.

7 Overview of Manual Data Flows

At times it will be necessary to perform manual communications between the Participants and BSC Central Services. The following are the types of manual interface that can be used:

- E-mail
- Fax
- Post

Manual flows to Central Systems will usually be in the form of BSCP forms sent to IMServ. Examples of which are: BSCP70, BSCP71 and BSCP301.

All manual data flows sent by Participants to the BSC Central Services must have a unique reference number provided, in an alphanumeric format with a maximum of ten characters.

Some manual data flows may be sent electronically. However, only those listed in the flow role tab of the Interface Definition and Design (IDD) spreadsheet are supported.

7.1 E-mail Communications

Upon receipt of an e-mail, the sender's details will be checked against the authorisation register within CRA. If the sender is an authorised party, then the e-mail will be positively acknowledged. If the authorisation check fails, a negative acknowledgement will be sent.

Please note, e-mails must contain the manual flow as an attachment and not inputted as text into the body of the e-mail.

E-mails will be acknowledged using the standard manual acknowledgement process. See section 7.4.

Following acknowledgement, the e-mail will be forwarded to the relevant team for processing.

The BSC Central Services e-mail address that Participants must use for BSC Central Services related manual flows is **BSCCentralServices@imserv.com**

Note: E-mail is not secure so authentication is limited. For some flows this is not an appropriate method of communication. Email may only be used for defined manual flows and ad-hoc communications.

7.2 Fax Communications

Faxed flows must be sent to a dedicated BSC Central Services fax number. This will interface with the CGI Consortium e-mail system such that the fax is presented as an attachment to an e-mail.

From this point onwards the process is the same as for the e-mail medium.

The BSC Central Services fax number that Participants must use for BSC Central Services related manual flows is **0870 8335601**.

7.3 Postal Communications

All post must be addressed to specific BSC Central Services addresses.

Manual communication flows which involve BSCP form submission (with the exception of forms submitted through the Online Forms service) should be addressed to:

Central Registration Agent (or CDCA as appropriate)
The BSC Central Services
IMServ Europe Ltd
Scorpio
Rockingham Drive
Linford Wood
Milton Keynes
MK14 6LY
United Kingdom

All manual communications flows not resulting in a BSCP Form submission should be addressed to the BSC Central Services Help Desk at:

BSC Service Desk
CGI
Waterton Cross Business Park
South Road
Bridgend
CF31 3UL

From the point of receipt, the process is the same as for the e-mail media.

7.4 Manual Acknowledgement Process

Each Participant/role combination will have one manual acknowledgement route, which will be fax or e-mail. When Participants initially register with CRA they will be required to provide an e-mail address and fax number, which will be used for manual acknowledgements. E-mail will be the preferred method for communicating manual acknowledgements. However, if an e-mail address is not provided then acknowledgements will be sent via fax.

All manual acknowledgements, irrespective of the input media sent will be sent to the address using the standard acknowledgement media (fax or e-mail).

The acknowledgement will be a standard format Word document containing the following information:

- Flow type
- Participant's sending reference (as detailed above)
- Acknowledgement reference (unique reference generated by BSC Central Services)
- Date/time received.

The date and time of sending of the manual acknowledgement will be recorded.

7.5 Security

The management and handling of all incoming manual information is covered by the ISO27001 and ISO17799 security accreditation of the organisations processing this information.

Security is built into this process through:

- Restriction of e-mail access to authorised users only for both incoming and outgoing media
- Secure routing of faxes directly to e-mail
- Routing of incoming post to authorised users only
- Secure routing of acknowledged data to authorised users only
- Storage of paper communications in a fire safe.

7.6 Manual Flows to Participants

Each Participant/role combination will have one manual message route, which will be fax or e-mail. All manual messages will be sent to the address using the standard message media (fax or e-mail).

The method for communicating manual flows to Participants, is detailed in section 7.4.

8 Overview of Electronic Data Flows

A common format is used for data files transferred electronically between the BSC Central Services and the BSC Parties and their Agents. These files use the ASCII character set. They consist of:

- A standard header
- A collection of data records using standard format
- A standard footer.

The format of these files and individual record arguments are specified in the Interface Definition and Design (IDD). The IDD is listed in the references section of this document, and can be found under BSC & Related Documents: Interface Definition Documents. This section details some of the core information from these documents, along with important considerations in the generation and processing of the data flows.

8.1 Sequence Numbering

Since the order in which flows are processed can have an important effect on processing, BSC Central Services uses file sequencing to ensure that all files are processed in the intended order. All flows to and from BSC Central Services contain a sequence number in the header record of the file, which wraps around to zero when it reaches its maximum limit.

A separate sequence series is used for each combination of source Participant ID, source role code, destination Participant ID and destination role code. So, for example flows in different directions between a specific BSC Central Services role code and a specific Participant role code would operate using different sequence series.

The exception is the case of receipt acknowledgement files, which carry the sequence number of the file being acknowledged.

Sequence numbering is independent of the method of delivery, so Participants switching between the High and Low Grade services do not need to reset their sequence numbers.

There is no automatic process by which the BSC Central Services will alter the value of any next expected sequence number which it holds (either up or down), apart from the normal increment when a file is received with a valid header. The only method by which a BSC Party or Agent can achieve a change in the value of the next expected sequence number held by a BSC Central Services will be by manual agreement, via the BSC Service Desk.

8.2 Sequence Handling

It is accepted that in some circumstances it may be possible for files generated by BSC Central Services or by the Participant to be received by the other party out of sequence order. In this circumstance the receiving party should negatively acknowledge the file as being out of sequence, but to improve the resilience and automation of the sequencing system BSC Central Services has a sequence handling procedure to allow some flexibility for flows submitted in an incorrect order.

The system described is that used by BSC Central Services. It is highly recommended that Participant software incorporate a similar system.

If a file is received by BSC Central Services with a sequence number greater than that expected for the given sequence series, it is not automatically negatively acknowledged. Instead, it is put in a holding queue to wait for the next expected sequence numbered file to arrive.

If after a specified number of out of sequence files are received, or after a specified period of time has elapsed (whichever occurs sooner), the next expected sequence number has not been received then any out of sequence files which have been in the holding queue are negatively acknowledged as being out of sequence.

The values used by BSC Central Services for this purpose are 99 files (variable upon request per Participant) or 13 minutes. These values are chosen by BSC Central Services to comply with the service levels required for acknowledgement of files submitted by Participants, but are a good suggested starting point for Participants implementing a similar system.

Factors which would affect the choice of values for a Participant would be the volume of files transferred during a typical delivery and criticality of alerting their users should a problem occur.

8.3 Acknowledgements

As discussed above, each flow (other than an acknowledgement itself) sent to or from BSC Central Services expects a response file to be generated to acknowledge successful or unsuccessful receipt. The scope of this acknowledgement is to indicate that the file is in the correct format, that its sequence number is that expected and that its data integrity can be verified (by means of a checksum in the footer record). An acknowledgement, sometimes referred to as a "Comms Ack" from BSC Central Services does not signify that the data within the flow has been accepted. This is notified via other flows such as ECVAA acceptance feedback reports.

The acknowledgement file format is specified in detail in the BSC Central Services Interface Definition and Design (IDD) documents. Each file consists of:

- A header (AAA) record which among other information contains the name and sequence of the flow being acknowledged

- An acknowledgement (ADT) record which specifies the type of acknowledgement being provided, response codes indicating positive or negative receipt and optional description of errors

- A standard footer record containing a checksum for the flow.

8.4 Handling Negative Acknowledgements

The progression of sequence numbers following a negative acknowledgement from BSC Central Services depends on the nature of the error in the original file (which is specified in the acknowledgement code of the ADT record).

- If a file is rejected because of problems with the HEADER, the sequence number is not "used" and so the next expected sequence number remains unchanged. [NACK codes 1,2,3]. A corrected file (with the same sequence number) should be submitted next.

- If a file is rejected because of problems with the BODY or TRAILER (record count, checksum), the sequence number is used and the next expected sequence number is incremented. [NACK codes 4,5,6,7] A corrected file (with a new sequence number) should be submitted next.

9 Networking Information

This section provides more detailed information to assist network administrators in the ordering, configuration and usage of the BSC Central Services electronic interfaces.

9.1 High Grade

After registering interest for a High Grade service with ELEXON, but before placing an order, the Participant will be contacted by the Service Provider to arrange for installation of communications lines to the Participant's site.

9.1.1 Information and Site Access

The information initially required by the Service Provider will include:

- The exact termination point (specified down to the room) where the communications lines and router are to be installed
- Site contact details
- Site access details, including timescales and any special requirements for engineers accessing the Participant site
- Specification of the lines and router required.

As described earlier in this document, the standard communications product supplied to the Participant is a 256Kbps Leased Line with a 2Mbps 20:1 contended ADSL backup, presented on X21 and through a Cisco 2801 router.

The lead time for installation of this standard circuit is 55 working days, and the order can only be placed with the communications supplier after technical details have been confirmed. It is not necessary at this early stage for an IP schema to be agreed, this can be planned during the order process.

Access to the BSC WAN can only be achieved through the Service Provider.

9.1.2 Features and Specifications

The standard Cisco 2801 router provided to the Participant is completely managed through the Service Provider. The Participant cannot manage, login or configure the router.

The Cisco 2801 router is rack mountable and only has provision for one power supply (a dual powered router requires an upgrade to a much more costly model).

The Service Provider supports delivery of service to the Ethernet port on the router provided, but the Participant is responsible for keeping the router constantly powered and in an appropriate environmental setting.

The network termination equipment provided for MPLS and ADSL lines varies dependent upon line access speed and site requirements.

9.1.3 Planning an IP Schema

The Service Provider will discuss IP schema selection and design with the Participant when the High Grade order is placed, or may be contacted before this point through the BSC Service Desk.

9.1.4 Firewall Configuration

The Service Provider will provide the participant with details of the required firewall rulebase during the High Grade line installation process.

9.1.5 Provision for BSC Central Services Disaster Recovery

If BSC Central Services invokes their Disaster Recovery plan, no action is required by the High Grade Participant. If employed, the BSC Central Services Disaster Recovery site will be address translated and presented to the Participant as if it were the Live service site. No IP configuration or firewall rulebase changes are required by the Participant.

9.2 Low Grade

Low Grade Participants provide their own internet connectivity in order to be able to use the internet based Low Grade service. The following provisions should be made.

9.2.1 Firewall Configuration

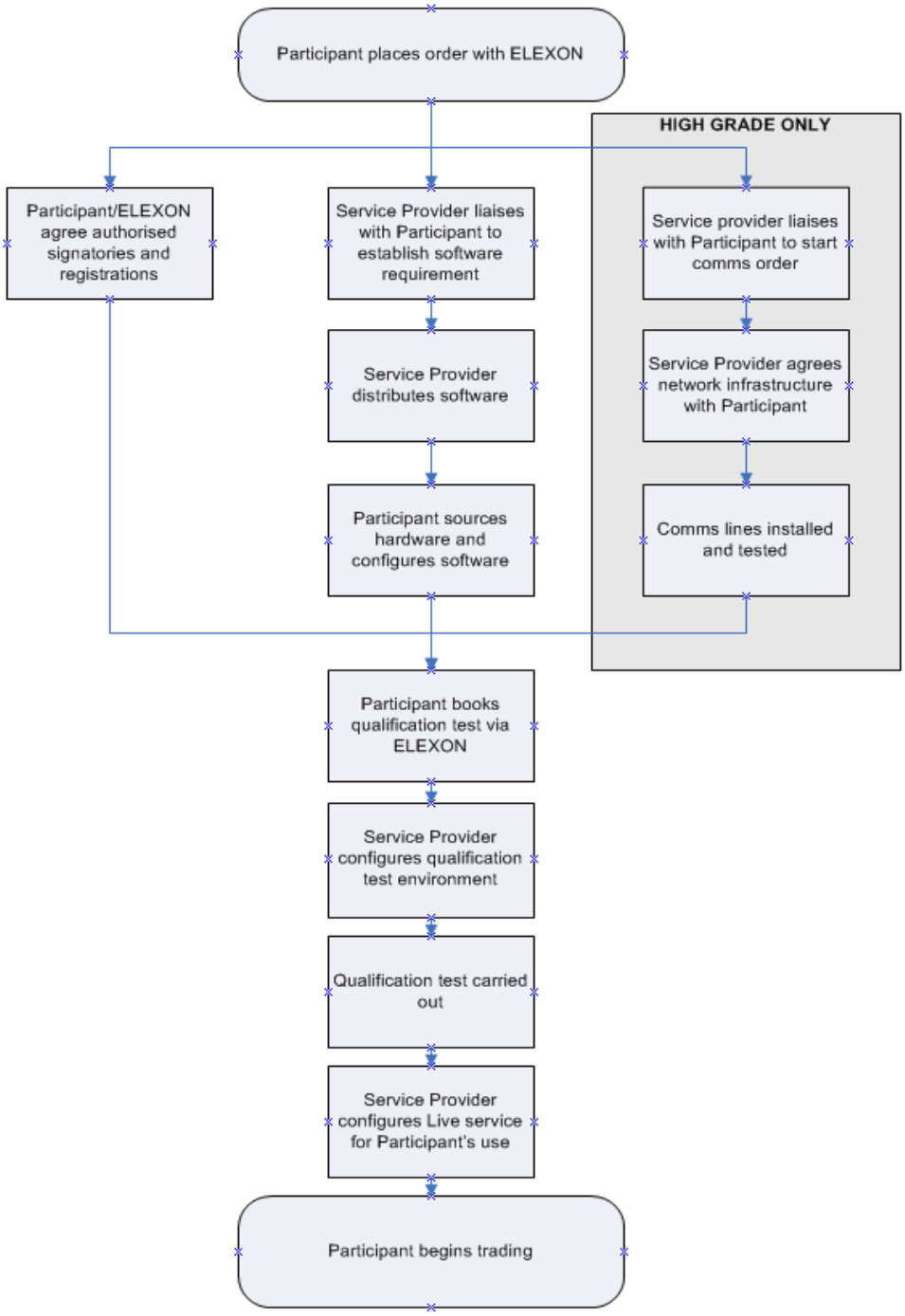
The Service Provider will provide the participant with details of the required firewall rulebase upon application for access to the Low Grade service.

9.2.2 Provision for BSC Central Services Disaster Recovery

If BSC Central Services invoke their Disaster Recovery plan, the IP addresses of these services will change, but the fully qualified names will map to the new IP addresses. Details of the IP addresses used will be supplied to the participant upon application for access to the Low Grade service.

10 Summary Overview – Steps in the Comms Setup Process

This section briefly shows the steps that a Participant should plan for during the comms setup process. They assume entry of a completely new Participant and do not directly apply to other circumstances, such as addition of Participant IDs for existing users.



11 Service Desk

For further information relating to communications with the BSC Central Systems please contact the BSC Service Desk on **0870 010 6950** or by email at **bscservicedesk@cgi.com.**

Appendix A - CVA WAN Communications Options

The matrix below shows the communications options available for the new CVA WAN. This is provided to assist you in making a decision as to the most appropriate option.

Please note that CGI are on hand to advise you and help you choose the correct option.

	Line Options									
	HG1a	HG1b	HG2a	HG2b	HG3a	HG3b	HG4	DR1	DR2	Low-Grade
Trading Profile										
High Volume Trading	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
Low Volume Trading	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Trading near gate closure	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
TIBCO Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Primary Line Specification										
256Kb Leased Line	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗
512Kb Leased Line	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
1Mb Leased Line	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
2Mb ADSL	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
Backup Line Specification										
ISDN Backup	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗
2Mb ADSL Backup	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
Support Specification										
5 Hour Target Fix Time	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗
24 Hour Target Fix Time	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
No Bandwidth Contention	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗
20:1 Contention Ratio	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗

- Options DR1 & DR2 can only be used in conjunction with a Primary High Grade Line
- All ADSL options have a possible 20 - 1 contention ratio
- Lease line speeds are the same for upload and download
- ADSL upload speeds are restricted to 256Kb
- ADSL may not be available in all areas
- Leased Line and ADSL routers are rack mountable
- Costs can be found in the Schedule of Specified Communications Charges