Gas Retail Market System

GRMS FTP User Guide

Service Delivery Phase

Customer	:	Australian Energy Market Operator (AEMO)		
Contract Number	:	SOSA (WA) (dated July 2014)		
Proposal Number	:	03-184		
Business/Project Number	:	440/48513 (AEMO) and 440/49159 (AEMO)		
Project Manager	:	Cathy Langman		
Reporting to	:	Les Davey		
Document Reference	:	GRMS FTP User Guide		
Issue	:	3.2		
Issue date	:	31/10/2016		
Period of Validity	:	End of Service Delivery		
Status	:	Definitive		
Distribution	:	Name	Role/location	
		Project Team	CGI	
Prepared by	:	Gas Market Systems Team	Date:	2/6/2016
Reviewed by	:	Robert Gubbins	Date:	2/6/2016
Approved (CGI)	:	Cathy Langman Client Service Manager	Date:	2/6/2016

Amendment history

Date	Issue	Change Summary	Author
13/01/2004	0.1	Initial draft	SH
03/02/2004	0.2	Updated after review	SA/KQ
09/02/2004	0.3	Further Review updates	SH
17/02/2004	0.4	Updated after practical trial	SH
18/02/2004	1.0	Released to AEMO	IH
06/04/2004	1.1	Amend description of client/server SSL session authentication	SH
11/05/2004	1.9	Remove references to ssl. Only straight ftp will be used.	[ZG/DB]
11/05/2004	2.0	Amended version 2.0 for release	SH
16/05/2005	2.1	Minor amendments	SH
22/06/2005	2.2	Updated to include reference to implementation of CCN19 (C11/05S - transactional security for FTP)	SJM
08/06/2011	3.0	Updated to reflect AEMO as Market Operator for SA Market and REMCo as the Market Operator for the WA Market	RG
1/12/2015	3.1	Logica to CGI update Clarified AEMO and REMCo FTP Prod and Test addresses	RG
31/10/2016	3.2	Update for transition to AEMO	CS

Contents

1 GRMS FTP User Guide

1.1 Purpose

The purpose of the document is to provide a guide for participants using the FTP server. It is not intended to be a complete technical guide as there will be some dependencies on the particular FTP client used by participants. Rather, the document gives an overall description of how the FTP service has been implemented with some required settings that participants will need to configure in their own FTP client.

The document also provides an overview of the transactional security model that was implemented via CGI CCN19 (Retail Market Rule change C11/05S).

1.2 Scope

This scope of this document is to outline the GRMS FTP service. The intended audience of the FTP User Guide are the SA & WA Gas Market participants who need to connect to the GRMS using the FTP service.

1.3 Structure

This section introduces the FTP User Guide.

Section 2 provides an overview of the FTP client, IP addresses necessary to establish FTP Services and establishing an FTP session to GRMS.

Section 3 discusses Firewall considerations.

Section 4 describes the directory structure and file operations on the GRMS FTP Server.

1.4 References

Reference	Document	Source	Issue	Date

2 FTP Services

CGI has established a standard FTP service using Microsoft IIS. Authentication is based on a standard username and password model.

2.1 FTP Client

As standard FTP services are being used, any FTP client may be used to connect to the FTP server.

2.2 IP Addresses

The IP address of the SA FTP Server is 203.110.140.74 and the IP address of the WA FTP Server is 210.193.162.228.

There is also a Test SA and Test WA FTP Server that may be used for testing purposes by prior arrangement with CGI and AEMO. The IP address of the server will be provided by CGI on request. This server will not always be available and participants wishing to utilise this service should contact CGI or AEMO prior to initiating a connection in order to avoid disrupting other testing activities which may be in progress.

Authentication to both FTP servers is based on a valid username and password.

2.3 Ports & Firewall Considerations

The FTP server is configured to use standard FTP ports.

Participants accessing the FTP server from behind a firewall will need to ensure that ports 21 and 20 are open for outbound connections. FTP sessions should be opened in passive (PASV) mode, which will ensure correct operation through a firewall where Network Address Translation (NAT) is configured.

2.4 Establishing the FTP session

The user login will occur after verification of Username and Password, after which time the FTP client will have access to the authorised FTP directory.

2.5 Password Changes

FTP user account passwords are changed by the CGI operational team on a quarterly basis for security purposes. Password changes are managed via an approved process which is communicated via the TWG forum to participant technical contacts.

3 Transactional Security (VPN)

In May 2006, CGI CCN19 (REMCo rule change C11/05S) introduced a Virtual Private Network (VPN) transactional security model for FTP based communications to and from the GRMS.

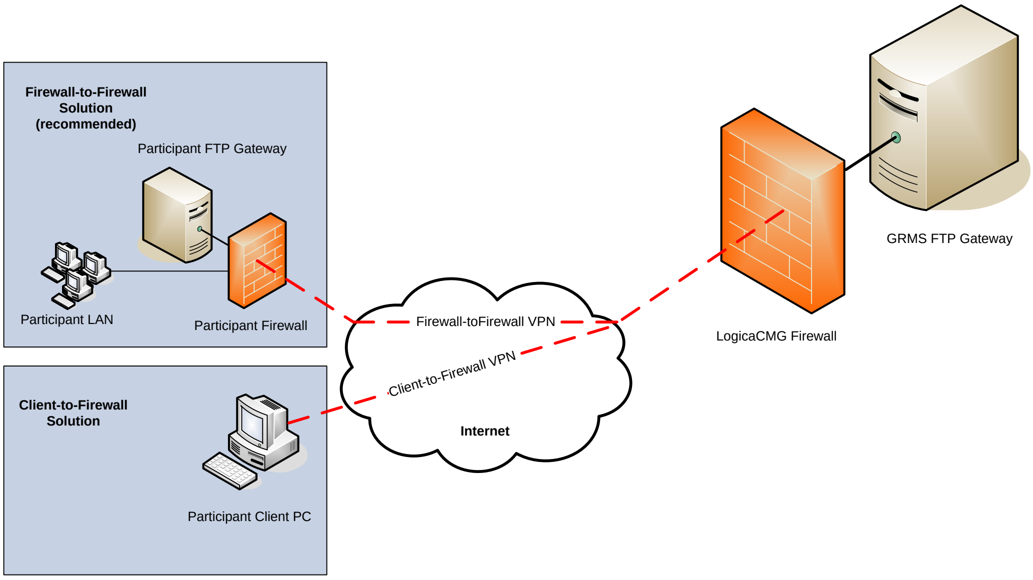
A VPN ensures the security of transactions by establishing an encrypted tunnel between the connection termination points. This means that data cannot be deciphered by a third party, even if it is captured during transit.

VPN is currently the industry best practice for secure, point-to-point style connections using the Internet as a cost effective medium. VPN technology is relatively mature, is reliable and is reasonably simple to implement and maintain.

The VPN terminates at the same firewall appliance in CGI's Production data centre as the VPN for the NSW/ACT GRMBS and as such, provides a convergence of technologies across the SA/WA & NSW/ACT Markets. This synergy enables organisations participating in the above markets to use a single VPN connection to CGI whilst maintaining cross-environment security.

In most cases, the implementation of VPN connections between the GRMS and participant FTP gateways will be in the form of a firewall-to-firewall IPSEC solution, although for technical reasons, some participants have chosen to implement a client-to-firewall solution whereby a VPN client application within the participant organisation maintains an IPSEC connection to the CGI firewall behind which the GRMS FTP gateway is hosted. All connections will be encrypted using the 3DES protocol.

A high level solution overview showing both connection types is illustrated in the diagram below.



The VPN solution is currently implemented at the GRMS Production site only as a result of technical limitations at the DR site. In the event of a disaster scenario, FTP gateway connections will need to revert to standard FTP as an interim measure.

3.1 VPN Technical Information

Specific technical details are available from CGI on request.

4 FTP Directory Structure and File Operations.

The following information is extracted from the SAWA [ICD].

Each organisation will have a directory specific to them for each jurisdiction in which they are active from which they may send or receive files to/from GRMS. This directory will have sub-directories for each GBO ID used by that organisation. Under each of the directories will be the *in* and *out* directories i.e.:

/*GBO_ID*/[SA | WA]/*GBO_ID*/in

/GBO_ID/[SA | WA]/*GBO_ID*/out

For example, Acme Retail participates in the SA market as a retailer. The same organisation acts as a shipper and swing service provider. It has the following GBO IDs.

ACMERRET	For the retailer (user) entity
ACMERSHPD	For the shipper entity on the D pipeline
ACMERSSPD	For the swing service provider entity on the D pipeline

Acme Retail would have the following directories on the FTP server:

/ACMERRET/SA/ACMERRET/in	(for messages from the participant to GRMS)
/ACMERRET/SA/ACMERRET/out	(for messages from GRMS to the participant)
/ACMERRET/SA/ACMERSHPD/in	(for messages from the participant to the GRMS)
/ACMERRET/SA/ACMERSHPD/out	(for messages from GRMS to the participant)
/ACMERRET/SA/ACMERSSPD/in	(for messages from the participant to the GRMS)
/ACMERRET/SA/ACMERSSPD/out	(for messages from GRMS to the participant)

When an organisation logs onto the server, their ‘home’ directory will be

/ACMERRET

From here, they can change directory to the appropriate GBO ID directory. This allows a representative from the organisation to submit files in multiple roles (and hence GBO IDs) in the same log on session.

Once each participant has been registered, usernames / passwords and the actual directory will be provided to the participant organisation.