CQG

CQG Hosted Exchange Gateways Authentication Guide

September 9, 2011 | 2011-01

Table of Contents

About this Document

This document details how the CQG gateway handles trader authentication and how the facilities are to be setup and maintained.

Because it is meant to be printed double-sided, you may notice blank pages in the .pdf. Blue, underlined text indicates either an external link or a link to another section of this document. You can navigate this document using the bookmarks in the .pdf or the entries in the Table of Contents.

The most current version of this document is always available at:
http://www.cqg.com/docs/gwauthenticationguide.pdf

Publication History

Date	Version	Changes
September 9, 2011	2011-01	Initial publication.

Related Document

CAST User Guide, two-factor authentication introduced in version 4.8 SP2.

Customer Support

Please contact FCM Support at 1-800-525-1872 if you have questions.

Two-Factor Authentication

In order to comply with regulations in some countries, CQG must provide two-factor authentication (2FA) to confirm the identity of traders when they log on to trade.

The first factor is the trader's password that was set in CAST, and the second factor is a one-time password (OTP).

FCM

FCMs decide whether to use one-factor or two-factor authentication on a per-customer basis. Obviously, if an FCM provides only one authentication system option, then that option is the default, and customers can use only that system.

Both existing and new FCMs use one-factor authentication automatically. In order to use two-factor authentication, an FCM must first set up a DS3 system and server.

Once the system is in place, the FCM uses a DS3 web-based administration tool to create and manage traders. Please note that the trader's user ID in the admin tool must be the same as the trader's user name in CAST.

Customers

FCMs decide whether to use one-factor or two-factor authentication on a per-customer basis. Obviously, if an FCM provides only one authentication system option, then that option is the default, and customers can use only that system.

Password Management

The password of a trader using one-factor authentication can be changed in CAST.

The password of a trader using two-factor authentication that allows static password changes can be changed in CAST.

The password of a trader using two-factor authentication that does not allow static password changes cannot be changed in CAST. In that case, those features are disabled, and the FCM makes the change using their DS3 tool.

Note: To complete the setup steps outlined in this document, these files must be present in the DS3 folder: ASClient.dll, ASCom.dll, unreg_ASCom.bat, UninstallAS-NT.bat, InstallAS-NT.bat, reg_ASCom.bat, AS.bat, wrapper.exe, ASClientTest.js, ASClientTest.vbs.

External Authentication System Configuration

At the moment, there is only one external authentication system that can be configured: DS3, an external authentication system based on a one-time password factor coupled with static password as the second factor of authentication.

There can be multiple external systems instances, each having different values of the parameters, all under one type DS3 External Authentication System Type = 2.

The following parameters are to be setup in the table AuthenticationSystemParam to allow connection between the CQG gateway and the remote authentication servers of DS3:

Name	Value	Description
RandomLength	8	As is.
RSAKeyLength	128	Length of RSA key. As is.
AdminDomain	1	ID of domain to which DS3 assigns the given FCM. To be obtained from DS3 by each FCM. As is.
RSAKeyIndex	2	Index of encryption key. Range 0-9. Value matches configuration on external AS server.
RSAKeyType	10	Type of key used for static password encryption, likely 10 (RSA1024, public key). As is.
EncryptedBlockLength	128	As is.
HashLength	128	Length of password hash buffer. Set by DS3. As is.
SaltLength	32	Length of salt buffer. Set by DS3. As is.
Algorithm	2	Hash algorithm used on encrypted static password, likely 2 (SHA-256). As is.
SymKeyType	3	Type of cipher algorithm used on static password, likely 3 (3DES). As is.
SymKeyIndex	0	Index of cipher algorithm key. Should match configuration on external AS server. Range 0-9. As is.
AuthenticationServer	202.172.63.146	IP address of the DS3 server that will process our verification and encoding requests. Specified by FCM.
KeyFilePath	C:\XPIT.COM\ DS3\ PRUD.KEYSTORE	Full name of the key file supplied to us by DS3 and placed on each server that needs to establish connection to external authentication servers.
KeyFilePassword	123456	Password to the keyfile. Supplied by DS3 or FCM.

Name	Value	Description
Domain	2	Arbitrary number in the range 0-31 supplied and used by DS3 or DS3 to assign traders to. As is.

These changeable parameters change most often:

- AuthenticationServer: Changes every time DS3\FCM changes where AS servers are running.
- Domain, Admin Domain: Changes every time FCM changes it for their traders. FCMs should notify CQG of such changes.
- KeyFilePassword: Changes every time DS3\FCM sends new key file.
- KeyFilePath: Changes when the CQG gateway is deployed for the first time. Should be the same on all servers because DB value is one for all.

External Authentication System Setup

DS3 Authentication Server (AS)

CQG configures a firm to access a particular DS3 AS for trader validation.

DS3 AS supports multiple 2FA approaches, including OTPs received via SMS and hardware tokens (e.g. Vasco). The FCM can use any OTP method for 2FA. DS3 AS also supports strong encryption to meet end-to-end encryption requirements for static passwords.

Every trader must be associated with a corresponding user in the DS3 AS. Association is done by username/userID. When a Trader attempts to log on, the GW uses the firm's AS to validate trader credentials.

CQG

The firm works with DS3 to obtain and install a DS3 AS. The AS can run from the firm’s data center or from a hosted services offering from DS3. In either case, the firm is using a particular DS3 AS for authentication.

The firm then provides the following information to CQG. DS3 should be able to help with most of these values, as they are related to AS configuration:

- AS IP address.
- SSL keyfile: used for establishing a secure connection to the AS.
- SSL keyfile password.
- AS domain number: where the firm will create AS users that correspond to GW Traders.
- RSA key type: type of key used for static password encryption; likely 10 (RSA1024, public key).
- RSA key index: index of encryption key; should match firm's AS configuration (0-9).
- Hash algorithm type: hash algorithm used on encrypted static password; likely 2 (SHA-256).
- Symmetric key type: type of cipher algorithm used on static password; likely 3 (3DES).
- Symmetric key index: index of cipher algorithm key; should match firm's AS configuration (0-9).

FCM Administrator

To configure a new user, the FCM administrator:

- Uses a DS3 AS web-based administration tool to create an AS user (userID=<X>) and to assign an OTP source (e.g. hardware token identified by serial number) to the AS user.
- Uses CAST to create trader (username=<X>). Note that username in CAST must match userid in DS3 AS.

Trader

The trader begins the log on process by entering the username and password. If the trader is configured to use DS3 AS, the trader is prompted for the OTP.

To authenticate the trader, the system passes username, encrypted static password, and OTP to DS3 AS. If AS reports that both static password and OTP are valid, the trader is considered authenticated and logged on to the gateway.

Installing Authentication System Components

Each server running Session Manager, Web Service, or the CAST gateway component must have a DS3 service and a component to connect to that service, called ASClient, installed.

1. Ensure that Java is installed and configured properly (listed in PATH) by using the java command in the command prompt. While CQG used version 1.6.0 in testing, versions 1.3 and higher should work.
2. Create a folder to contain the binaries and keystore files of the AS service. Please note that technically there is no requirement to keep the binaries and the certificate (keystore) files in the same folder. For simplicity, we assume that the files are in the same folder c:\xpit.com\ds3. All further folders names are relative to this one.
3. Extract the supplied DS3 archive with the files into that folder.
4. Install the DS3 service. First, change to subfolder ASClient/bin, then run batch file InstallAS-NT.bat. We recommend that you install from the command prompt, which allows you to see the installation outcome and detect any problems.
5. Optionally, manually register .NET ASClientAssembly.dll assembly using regasm. This registration will be done automatically in the install time by GIM.
6. Verify that the installation was successful. Open Services system applet, and start the "DSSS AuthServer Service." Depending on your preferences, set startup type to **Automatic** or **Manual**. We recommend automatic to ensure that the service starts every time the server is rebooted, but you may have an opposing policy.

   Another way of checking the installation success and service readiness is to inspect the log file, usually located at ASClient/logs/wrapper.log and then it resembles this file:

   ```
   STATUS | wrapper  | 2011/04/25 21:08:23 | --> Wrapper Started as Service
   STATUS | wrapper  | 2011/04/25 21:08:23 | Launching a JVM...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Wrapper: Starting Wrapper...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Wrapper (Version 3.1.2)
   http://wrapper.tanukisoftware.org
   INFO   | jvm 1    | 2011/04/25 21:08:24 |
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Wrapper: Instantiating ClientCall...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Wrapper: Starting ClientCall...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Starting ClientCall...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Binding to 127.0.0.1 at port 55178...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Starting ClientCall Daemon...
   INFO   | jvm 1    | 2011/04/25 21:08:24 | Waiting for incoming connection...
   ```

   Note that the file name and location can be changed in ASClient/conf/wrapper.conf.
7. Run one of the test batch files to confirm successful connection to the remote AS servers and user authorization. Make sure that the value in the file for “KeyFilePath” is correct for your install. The files are set up for our CQG Test connection. If you are not using the test connection, you must first update the file and change the values specified by the FCM or DS3, at a minimum “AuthenticationServer” and ”KeyFilePassword” are likely unique. To run the scripts, use either command "cscript ASClientTest.js" or "cscript ASClientTest.vbs".