TRADING TECHNOLOGIES

Eurex Clearing FIXML Account IDs and SSL Certificates

VERSION 7.X
DOCUMENT VERSION 7.X.0.DV1 3/5/14

LEGAL

1 Connecting to the Eurex FIXML Clearing Interface

Prerequisites

Overview

This document provides the steps necessary to create a FIXML Account and SSL certificates required for connecting to the Eurex FIXML Clearing interface for OTC trades. FIXML messages are transported to/from the FIXML OTC Router on the Eurex Gateway via AMQP (Advanced Message Queuing Protocol) over a secure connection.

The FIXML OTC Router connection to the FIXML Clearing API interface is encrypted using the Secure Sockets Layer (SSL) protocol, so gateway and FIXML Clearing Interface server authentication with certificates is required. To enable this connection, complete the following tasks:

1. Create a FIXML account ID. Refer to Creating a FIXML Account ID.
2. Generate a self-signed SSL certificate based on the FIXML account ID and export it to public and private key files. Refer to Creating SSL Certificates.
3. Create your account and upload your public key to Eurex. Refer to Uploading Certificates.
4. Verify that the FIXML public keys from Eurex have been installed in the correct location on the Eurex Gateway. Refer to Saving the Certificate Files.
5. Save your private key in the same location as the Eurex public key on the Eurex Gateway. Refer to Saving the Certificate Files.
6. Configure the FIXML OTC Router on the Eurex Gateway. Refer to the *Eurex Gateway System Administration Manual*.

Creating a FIXML Account ID

Before creating and uploading FIXML OTC Router certificates, you must create a FIXML Account ID. You will need this account ID when generating your self-signed certificate and configuring the gateway.

The following guidelines apply to all account IDs created for connecting to the Clearing Interface via TT's FIXML OTC Router:

- Account names (IDs) can be no more than 22 characters and only uppercase letters are allowed.
- Characters 1 through 5 are the Member ID of the Eurex member.
- Character 6 is always an underscore (_) separating the Member ID from the rest of the account name.
- Characters 7 through 11 identify the vendor, service provider, or the member who developed the trading application. For TT, this value is **TTGXV**.
- Characters 12 and 13 identify whether the application is a front, middle, or back office application. For TT, this value is **FO** (Front Office).
- Character 14 identifies the trade adjustment processing. For TT, this value is **B** (Automated / Manual).
- Character 15 identifies the give-up and take-up processing. For TT, this value is **B** (Automated / Manual).

- Characters 16 through 22 identify the member's application name or a combination of application name and location. For TT, these characters are optional and may contain up to 7 alphanumeric characters (no special characters allowed). For a member running multiple Eurex Gateways, the application names must be different to differentiate account IDs and avoid using the same account IDs on different gateways.

Examples of valid FIXML Account IDs:

Example: a TT account ID that connects to the exchange via the Eurex Gateway application.

```
TTGXV_TTGXVFOBBGW1
```

Example: a customer account ID for member "ABCFR" that connects to the exchange via a Eurex Gateway.

```
ABCFR_TTGXVFOBBGW1
```

References

When creating a FIXML Account ID, follow the guidelines in Section 4.1 of the "Eurex Clearing FIXML Interface Specification, Volume 2, Connectivity". Eurex documents are available in the Eurex Member section of their website.

The following is documentation for using the Certificate Database Tools:

- Mozilla Network Security Services Tools (NSS)
- certutil
- pk12util

Creating SSL Certificates

Downloading the NSS Tools

Before proceeding, go to the Mozilla Network Security Services (NSS) ftp site and download the open source NSS utilities (e.g., nss-3.12.4.zip) for creating SSL certificates.

To download the NSS tools

1. In a web browser, go to the NSS FTP directory at: ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_12_4_RTM/msvc9/WINNT5.1_OPT.OBJ
2. Select the zip file (e.g., nss-3.12.4.zip). The File Download dialog box appears.
3. Select a path and directory to save the zip file (e.g., **<root drive>:\nss 3.12.4**) and click **Save**
4. Extract the files from the zip file and save them in the directory you created (e.g., **<root drive>:\nss 3.12.4**).
5. Open a Windows **cmd** window
6. Enter the following to set the "path" environment variable to include both the "bin" and "lib" sub-directories under the NSS working folder: `C:\> set path=c:\nss 3.12.4\bin;c:\nss 3.12.4\lib`

Creating SSL Certificates for the FIXML OTC Router

Note: TT recommends contacting your Technical Account Manager (TAM) for assistance when creating SSL certificates.

To create SSL certifcates for the FIXML OTC Router

1. Type and enter: **`cd <root drive>:\<path to NSS tools>\bin`**
2. Create a directory for the certificate database by entering the following command: **`mkdir <certficate directory>`**

   Example:

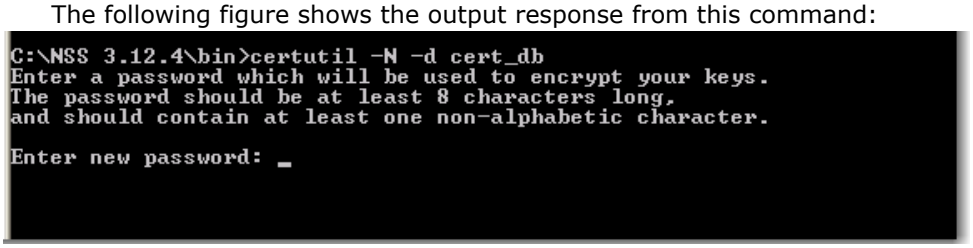
   ```
   mkdir cert_db
   ```

3. Create the certificate database by entering: **`certutil -N -d <certificate directory>`**

   Example:

   ```
   certutil -N -d cert_db
   ```

   The following figure shows the output response from this command:



Note: You will be prompted to create a password for the database; record the password as it will be used later to generate the certificate.

4. Generate a self-signed certificate by entering: **`certutil -S -d <certificate directory> -s "CN=<Account ID>" -n <certificate name> -x -t "P,," -v 12 -g 2048 -Z SHA512`**

   Example:

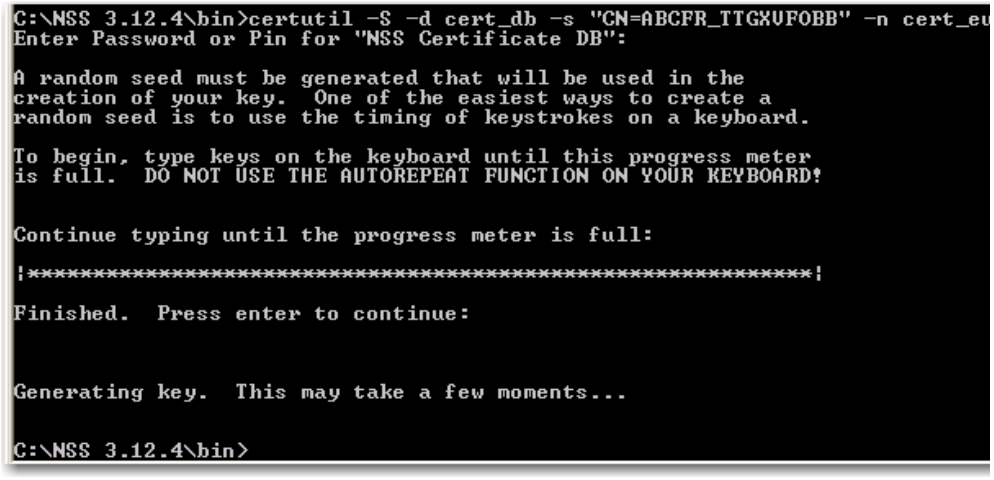
   ```
   certutil -S -d cert_db -s "CN=ABCFR_TTGXVFOBB" -n cert_eurex -x -t "P,,"
   -v 12 -g 2048 -Z SHA512
   ```

   Note: Click here for a description of certutil options and arguments.

   The `-v` argument sets how many months the certificate is valid. For more details, refer to the section called **Certificate Expiration** on page 10.

   When prompted, enter the certificate database password.

   After entering the password, continue typing random characters from the keyboard until the progress meter is full. Refer to the following figure.



5. Verify that the certificate has been created in the database by entering:
   `certutil -L -d <certificate directory> -n <certificate name>`

   Example:

   ```
   certutil -L -d cert_db -n cert_eurex
   ```

   The following figure shows the command response:

```
C:\NSS 3.12.4\bin>certutil -L -d cert_db -n cert_eurex
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            00:98:2d:6a:c2
        Signature Algorithm: PKCS #1 SHA-512 With RSA Encryption
        Issuer: "CN=ABCFR_TTGXVFOBB"
        Validity:
            Not Before: Fri Jun 01 16:05:24 2012
            Not After : Sat Jun 01 16:05:24 2013
        Subject: "CN=ABCFR_TTGXVFOBB"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    a9:61:de:33:a5:ab:84:ea:a5:19:4a:fa:04:cc:9d:26:
                    dc:61:fc:3a:6b:64:74:a5:2f:ea:53:41:58:86:5a:b4:
                    cc:f8:9b:38:06:23:50:9c:d7:88:b7:2a:de:4f:da:a5:
                    bf:29:82:a7:cf:c6:5f:17:86:56:2f:fc:90:1a:08:42:
                    d8:8d:44:d5:22:29:e3:14:7e:0b:9c:9c:d3:9c:52:cd:
                    44:d4:dc:ed:e3:3d:40:e4:32:58:66:b6:ee:1a:07:af:
                    57:f7:a9:1d:69:80:37:63:c0:ac:ac:ee:d4:92:8a:29:
                    e4:01:2a:1b:fa:3d:cd:06:45:6a:72:8b:80:24:8f:21:
                    5d:60:72:f6:16:ec:1d:a5:b4:2b:be:34:f1:31:fc:98:
                    f3:50:ec:9f:d0:ae:d2:5f:3b:b0:d9:7d:e3:c8:60:dd:
                    57:49:81:5a:7e:ac:4f:86:45:34:17:05:5d:61:a5:22:
                    b1:fd:37:a9:86:af:16:ec:c5:50:6f:a2:98:66:61:b3:
                    dd:2a:45:ec:6c:ea:57:d1:1d:eb:50:b7:f1:fc:35:73:
                    92:76:fc:0e:a3:03:f7:21:ad:c4:df:4b:e8:3d:fe:d5:
                    0f:f8:36:38:ce:08:7d:75:87:94:fd:11:9f:f9:40:16:
                    b8:0a:ae:0a:72:37:43:c6:5c:56:57:ad:96:c7:1c:db
                Exponent: 65537 (0x10001)
    Signature Algorithm: PKCS #1 SHA-512 With RSA Encryption
    Signature:
        0f:07:39:ab:f0:12:c6:c1:c8:bd:06:c2:9c:48:7f:e9:
        fe:6f:b2:3d:ea:33:33:ac:45:85:7d:46:77:2f:46:dc:
        3b:30:39:92:03:91:c1:29:85:dd:d3:4c:08:72:cf:0b:
        fc:89:00:e6:05:0a:4f:bf:e8:9b:6c:30:12:93:e3:40:
        98:d2:23:38:d1:e7:d7:d3:a4:91:86:9f:49:b9:37:fe:
        2f:fe:35:f4:72:41:fe:19:47:db:c7:5e:ef:3e:f1:08:
        93:34:48:a5:f6:02:05:76:04:57:1a:b4:d6:b9:2e:e6:
        93:e8:d2:dc:e1:0d:0c:78:86:21:37:e5:8b:f7:be:a9:
        3f:09:70:fe:71:69:f6:76:03:b9:13:f0:a7:31:3d:e1:
        05:b5:ca:92:f6:30:19:cb:88:82:b1:f1:f7:3c:b1:2d:
        15:36:0c:89:77:98:f2:2d:ac:da:cb:ea:d6:df:73:33:
        b8:c8:c1:ae:24:22:46:ba:dc:21:b8:07:94:9d:2c:2d:
        30:b5:a4:87:f5:58:6c:63:37:68:36:84:aa:95:aa:7a:
        a7:48:59:37:67:f0:58:9e:e6:6f:56:95:54:a3:79:3d:
        b5:94:9b:2f:76:e4:3c:50:df:8d:19:f4:6a:b3:d8:74:
        51:b1:86:e2:39:69:ab:d6:90:e3:57:87:81:21:66:bd
    Fingerprint (MD5):
        82:7F:50:7A:2F:FC:0B:5A:59:9C:8C:0E:66:DA:11:57
    Fingerprint (SHA1):
        62:59:F9:1F:56:9B:DD:F2:35:A8:69:AE:74:F8:07:9B:1D:3B:40:00

    Certificate Trust Flags:
        SSL Flags:
            Valid Peer
            Trusted
            User
        Email Flags:
            User
        Object Signing Flags:
            User


C:\NSS 3.12.4\bin>_
```

Tip: Record the dates that the certificate is valid so that you can recreate them before they expire. The dates are listed in the "Validity:" section of the certificate displayed on the screen after entering the **`certutil -L`** command.

6. To export the certificate to a public key file, type and enter: **`certutil -L -d <certificate directory> -n <certificate name> -a > <filename>.crt`**

   Example:

   ```
   certutil -L -d cert_db -n cert_eurex -a > cert_eurex_public.crt
   ```

7. To export the certificate to a private key file, type and enter: **`pk12util -d <certificate directory> -n <certificate name> -o <private key filename> -W <certificate file password>`**

   Example:

   ```
   pk12util -d cert_db -n cert_eurex -o cert_privkey.p12 -W auth

   NOTE: The private key filename is user-defined and does not require a
   filename extension, but will work correctly if one is added (e.g.,
   cert_privkey.p12, certificate.key, etc.).
   ```

   Command response:

   ```
   C:\NSS 3.12.4\bin>pk12util -d cert_db -n cert_eurex -o cert_privkey.p12 -W auth
   Enter Password or Pin for "NSS Certificate DB":
   pk12util: PKCS12 EXPORT SUCCESSFUL

   C:\NSS 3.12.4\bin>
   ```

   After entering the command, enter a certificate file password at the prompt. The certificate file password can be different from the certificate database password, and is used by the FIXML OTC Router for decrypting the file locally on the gateway machine.

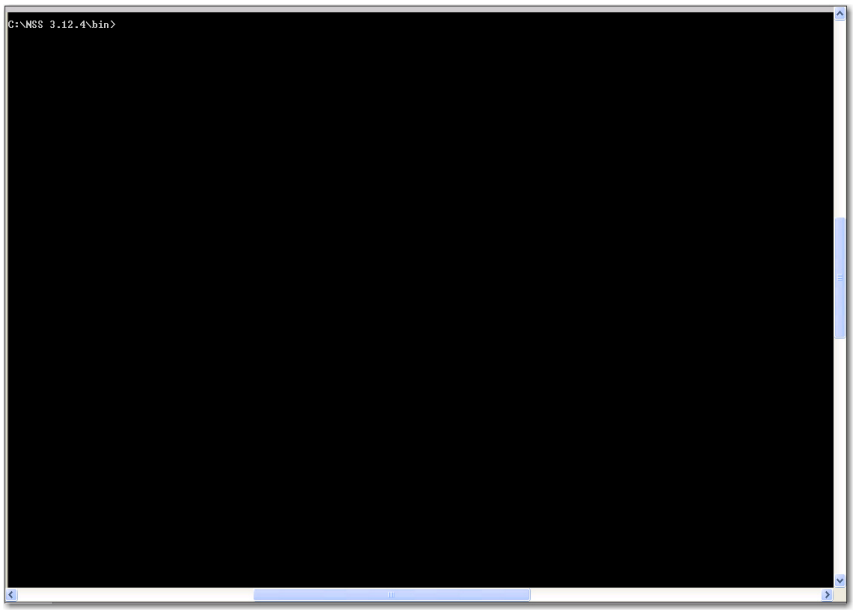
   Tip: Record the certificate file password that you created; this password will be used to configure the FIXML OTC Router on the Eurex Gateway.

Video: Creating SSL Certificates

Note: Adobe Reader 9 or higher is required to view the demonstration video.

To view the video in full-screen mode:

1. Click the image to activate.
2. Right-click the video and select **Full screen Multimedia**
3. To exit, right-click and select **End Full screen Multimedia**



Saving the Certificate Files

The FIXML connection also requires that the FIXML Order Router authenticates the server certificates of the Eurex AMQP brokers before the SSL sessions can be established. Eurex's public key files for the exchange brokers are installed automatically on your machine during a Eurex Gateway install or upgrade.

To ensure that the private key file and Eurex's public key are accessible to the FIXML Order Router, both certificates should be stored in the same location on the Eurex Gateway (e.g., **<root drive>:\tt\config**).

When configuring the FIXML OTC Router on the gateway, the location of the private certificate is set using the client_certificate_file parameter in **hostinfo.cfg**. The Eurex *public* certificates are installed in the **\config** directory automatically during clean installs and upgrades.

Refer to the *Eurex Gateway System Administration Manual* for FIXML OTC Router configuration details.

Certificate Expiration

The validation period of the certificates is set using the `-v <valid months>` argument used when generating them. TT recommends 12 months (`-v 12`), but the maximum is 36 months. Newer client certificates need to be created when the old ones expire.

For the Eurex server certificates, they will release new ones once their old ones expire.

To check the validity dates of your private certificate, enter the following:

- **`cd <root drive>:\<path to NSS tools>\bin`**
- **`pk12util -l <filename>.p12 -W <certificate file password>`**

  The dates are listed in the "Validity:" section of the certificate displayed on the screen.

Uploading Certificates

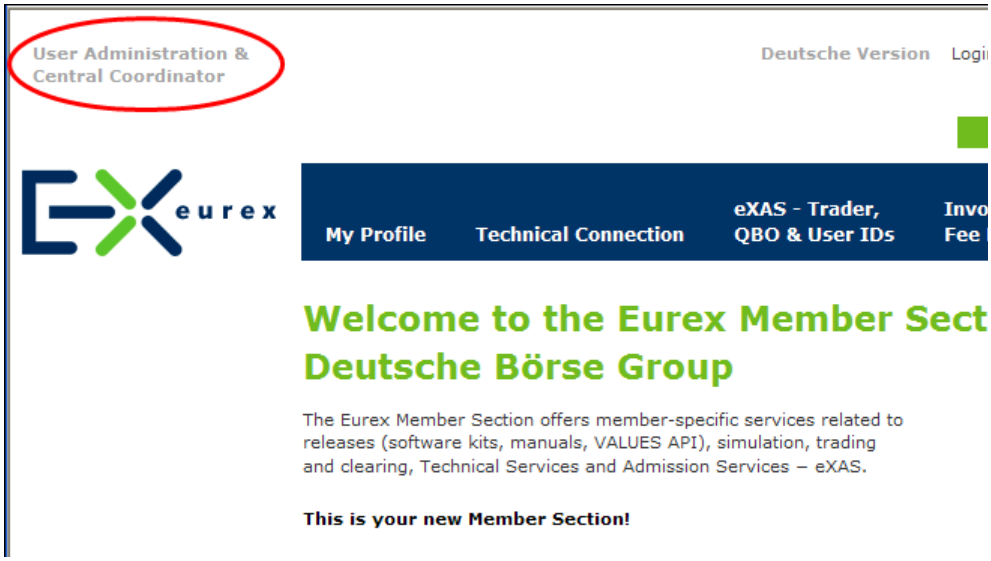
Overview

Because account authentication during connection is done by using certificates, you have to upload the public key of your certificate to Eurex and assign the key to your FIXML account.

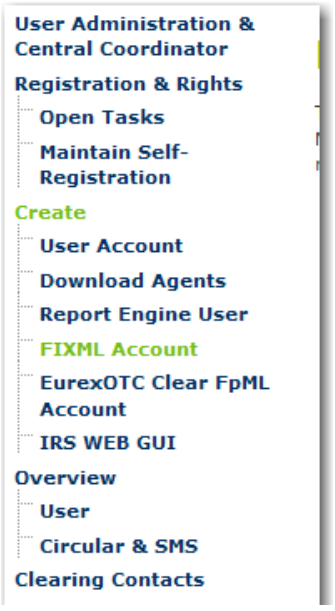
Uploading the FIXML OTC Router Certificate to Eurex

To upload the FIXML OTC Router certificate to Eurex

1. Login to the Eurex Member section.
2. Click **User Administration & Central Coordinator** at the top left corner of Member page.

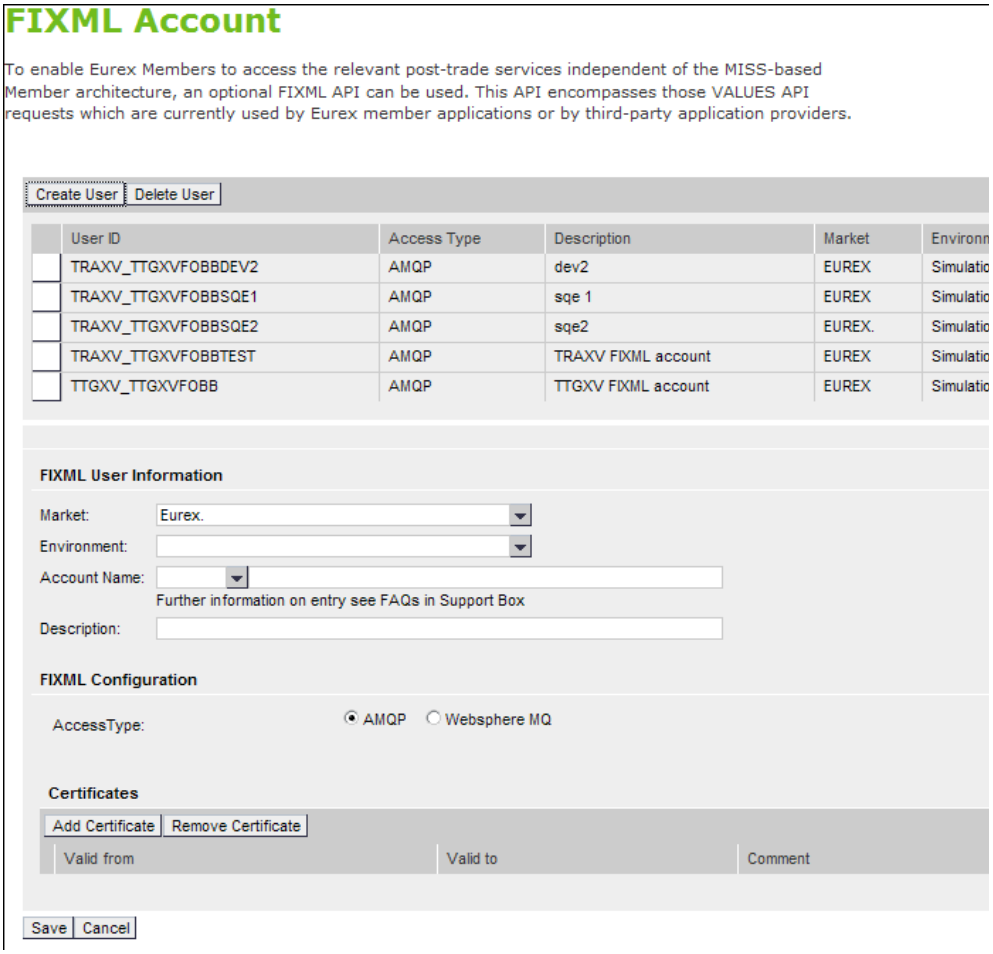


3. Under **Create** in the left navigation click **FIXML Accoun**t



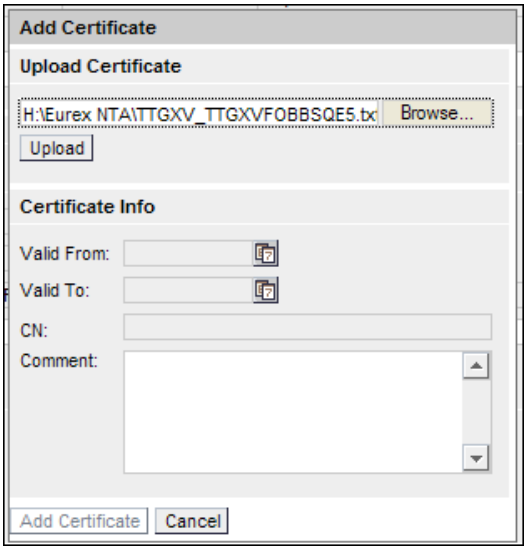
4. Click **Create User** to populate the FIXML User Information and select a FIXML Configuration. When entering the **Account Name**, use the same FIXML

Account ID that was used to create the certificate.



If the account already exists, double-click the existing account ID and verify that the account name is the same one used to create the certificate.

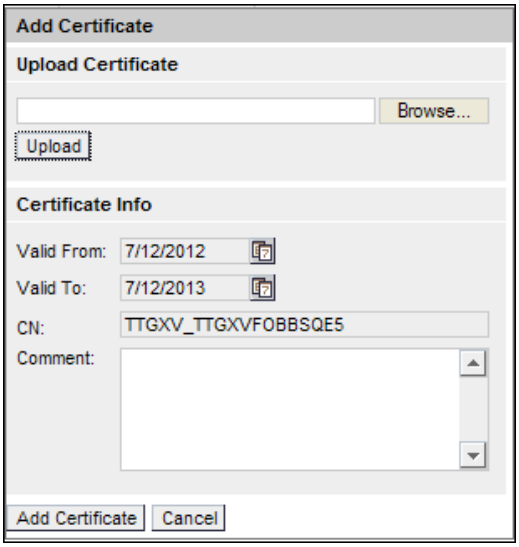
5. Click **Add Certificate**
6. Browse to the public certificate file and click **Upload** (the Account Name must match the Account Name used when creating the public certificate)



7. Click **Add Certificate** at the bottom of the window.

   By default, the certificate is valid for one year from the time it was created.

The dates cannot be changed in the **Certificate Info** pane



8. Click **Save**

Troubleshooting

FIXML OTC Router Connectivity Failure

A common connectivity issue is when the gateway fails to connect to the Eurex FIXML Clearing Interface and writes the following message to the Order Server log:

```
17.01.2013 16:20:06.773 | 11060 | INFO | 10082990 |
Ses.ENSLO_TTGXVFOBBDEFIX5 | Establishing an AMQP connection for member
ENSLO via amqp:ssl:ecag-fixml-simu1.deutsche-boerse.com:10170
17.01.2013 16:20:06.811 | 11060 | WARNING | 10082991 |
Ses.ENSLO_TTGXVFOBBDEFIX5 | Failed to open the AMQP connection: The
specified network password is not correct.  (c:\tt-
dev\eurex_os_7_16\middleware\qpid\0.14\dev\src\qpid\client\windows\sslco
nnector.cpp:185)
```

The most likely cause of connectivity failure is an incorrect password configured on the FIXML OTC Router. Specifically, the password used for configuring the `client_certificate_password` parameter in **hostinfo.cfg** for the gateway's FIXML connection does not match the password created when exporting the private certificate.

To resolve this issue, do the following:

1. At the cmd prompt, type and enter: **`pk12util -l <filename>.p12 -W <certificate file password>`**

   Result: If the password is correct, the certificate displays on the screen.

   If the password is incorrect, the following messages appear.

   ```
   pk12util: PKCS12 decode not verified: The security password entered is
   incorrect.
   pk12util: PKCS12 decode not verified: security library: improperly
   formatted DER-encoded message.
   ```

2. If the certificate password is correct, use this password to reconfigure the `client_certificate_password` parameter in **hostinfo.cfg**.
3. If the certificate password is incorrect:
   - Obtain the password entered for the `client_certificate_password` parameter in **hostinfo.cfg** and use it to recreate the private key file.
   - Recreate the private key file by entering: **`pk12util -d <certificate directory> -n <certificate name> -o <filename>.p12 -W <`**`client_certificate_password` **`from hostinfo.cfg>`**