F7 Release 3.1

F7 Connectivity Guide

Version: V 3.1.1
Date: 4. April 2019
In addition, according to Art. 14(1) PRIIPs Regulation the person advising on, or selling, a PRIIP shall provide the KID to r

Eurex Deutschland qualifies as manufacturer of packaged retail and insurance-based investment products (PRIIPs) and provides key information documents (KIDs) covering PRIIPs traded on Eurex Deutschland on its website under the following link: http://www.eurexchange.com/exchange-en/resources/regulations/eu-regulations/priips-kids.

In addition, according to Art. 14(1) PRIIPs Regulation the person advising on, or selling, a PRIIP shall provide the KID to retail investors free of charge.
Contents

1. Abbreviations & Definitions 5

2. Introduction 6
   2.1 Graphical User Interface, GUI 6
   2.2 Participant Application Programming Interface, F7 API 7

3. Network 8
   3.1 Repo Connectivity 8
      3.1.1 Leased Line 9
      3.1.2 Internet 9
   3.2 Connectivity security features 10
   3.3 URLs and IP ranges 10
      3.3.1 F7 GUI 10
      3.3.2 F7 API 11

4. Environments 12
   4.1 Release update timeline 12

5. Member Section 14

6. Leased Line connectivity ordering 15
   6.1 New connection 15
   6.2 Location details 16
   6.3 Connection type 17
   6.4 Data center details 17
   6.5 Request summary 18

7. F7 x.509 certificates 20
   7.1 x.509 Certificate creation with Java keytool 20
      7.1.1 Create keystore 21
      7.1.2 Export certificate for upload 22
      7.1.3 Import AMQP server certificate (F7 API only) 22
      7.1.4 Client PKCS#12 certificate for installation into the F7 GUI user’s browser 23
   7.2 x.509 Certificate creation with OpenSSL 24
      7.2.1 Step 1: Download OpenSSL 24
      7.2.2 Step 2: Create Private Key 24
7.2.3 Step 3: Create self-signed certificate 24
7.2.4 Step 4 create PKCS#12 file 27
7.3 Certificate validity period 27
7.4 Certificate upload 27
  7.4.1 User ID Configuration 28
  7.4.2 Multiple certificates attached to one User ID 28
  7.4.3 Environment 29
  7.4.4 Account Name Field 29
  7.4.5 ‘Description’ field 31
  7.4.6 Certificate upload verification 31
7.5 Username and password authentication 31
7.6 Additional IP Address check (Internet access) 31
8. Further information and contacts 33
9. Change Log 35
# 1. Abbreviations & Definitions

Please find a list of all the abbreviations used in the document.

<table>
<thead>
<tr>
<th>Abbreviation or term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMQP</td>
<td>Advanced Message Queuing Protocol</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>F7 API</td>
<td>F7 Application Programming Interface is the open and flexible interface for third party software products connecting to F7.</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>Keystore</td>
<td>A repository of security certificates (usually ones own certificates)</td>
</tr>
<tr>
<td>PKCS#12</td>
<td>Cryptographic archive file format. Here used to store digital certificates to be imported into a web browser.</td>
</tr>
<tr>
<td>POA</td>
<td>Participant owned application</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Samir and Adleman – asymmetrical cryptographic method</td>
</tr>
<tr>
<td>Truststore</td>
<td>A repository of security certificates (usually trusted certificates of others)</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator – reference to a resource (i.e. broker)</td>
</tr>
<tr>
<td>x.509</td>
<td>Public key infrastructure for digital certificates</td>
</tr>
</tbody>
</table>
2. Introduction

Deutsche Börse is continuously extending its F7 product scope, functionality and markets to improve its services and to attract additional customer groups. With the trading system F7, introduced in 2014, Deutsche Börse went a considerable step further, embracing the requirements of a state-of-the-art trading environment.

The F7 trading system serves as a solid foundation for future growth and has been designed to meet the highest demands.

Today’s global markets demand new standards of flexibility and performance. The 7 Market Technology series from Deutsche Börse Group offers a range of innovations in trading, clearing, risk management and connectivity – advanced infrastructure that lets you adapt to whatever the future brings.

This document describes the connectivity options and the ordering and setup process for F7. It considers participants who are new to the order process at Deutsche Börse but is also valid for participants, which already have Deutsche Börse infrastructure (for example existing Eurex participants, which want to order additional F7 connectivity).

2.1 Graphical User Interface, GUI

The F7 trader GUI is browser based. Extensive software installation or update processes are therefore no longer necessary. As a result, the F7 trading GUI is completely operating system independent, as long as a supported browser is used.

While running in the browser the F7 trader GUI offers the full repo trading functionality combining it with highest deployment flexibility.

A full online manual is available within the GUI. For a downloadable PDF of the GUI manual please go to:

https://member.eurexrepo.com following this path:

Repo Resources > Trading System F7 > System Documentation > Release 3.1 > Eurex Repo GUI Solutions

The F7 trader GUI can be connected either via leased lines or via an Internet connection. Chapter 2 of this document describes the differences and the bandwidth requirements, while chapters 3 and 4 guide you through the ordering process.

In both cases the connections are secured by an individual certificate (x.509). Prior to usage the certificate has to be uploaded via the Eurex Repo’s F7 Member Section and it has to be installed into the user’s browser. Chapter 5 of this document describes the steps which need to be performed to do this.

The F7 trader GUI runs with a wide range of recent browser software and operating systems.

A number of browser and operating system combinations are part of Deutsche Börse test scenarios. These combinations are considered as “supported”.


Untested combinations which have no issues reported are considered as “possible”, while combinations known to have problems are classified as “not supported”.

To fully support all features of the latest F7 simulation and production software the supported versions of Mozilla Firefox or Google Chrome have been adjusted from previous versions of this document.

- **Supported browsers** (older version may cause certain functions of the F7 trading GUI to become inaccessible)
  - Mozilla Firefox, version 61.0.1, or newer
  - Mozilla Firefox ESR, version 60.0, or newer
  - Google Chrome, version 67, or newer

- **Not supported browsers**
  - Microsoft Internet Explorer, IE

- **Supported operating systems** (others are considered possible, but untested)
  - Windows 7 SP1 or newer (32bit, or 64bit)
  - Red Hat Enterprise Linux 6.2, or newer

### 2.2 Participant Application Programming Interface, F7 API

The F7 trading platform comes with a dedicated API (F7 API). The F7 API enables message exchange (i.e. enter quote, enter IOI, etc.) in a proprietary XML based message format. Message flow is implemented via AMQP message brokers.

The interface supports request/response communication (participant triggered) as well as broadcast message flow (exchange triggered).

Any programming language can be used to develop applications connecting to this interface. The programming interface is available on leased line connections and via the Internet. Both types of connections require x.509 certificates for authentication.

For the full F7 API manual and accompanying XSD files please go to:

https://member.eurexrepo.com following this path:

Repo Resources > Trading System F7 > System Documentation > Release 3.1 > Eurex Repo Trading Interfaces

Recommended client libraries:

QPID C++ API 1.37 or newer (0.32 adds support for heartbeats on the AMQP 1.0 path)

https://qpid.apache.org/components/messaging-api/index.html

Latest version, at the point of publishing this document, is **QPID C++ 1.39**

QPID JMS 0.30.0 or newer (0.5.0 fixes an important producer flow control issue.)

https://qpid.apache.org/releases/

Latest version, at the point of publishing this document is, **QPID-JMS 0.40.0**
3. Network

In order to support the respective F7 services, Deutsche Börse Group has established an efficient infrastructure representing a dedicated global IP network. Access from a participant location to F7 must always be established via the Deutsche Börse Group’s IP network or alternatively via the Internet.

Any participant connection to the back end systems must be established via Access Points (AP). APs, to which leased lines connect, are located throughout the world in major financial centers where participants are concentrated.

This concept allows Deutsche Börse to extend its private network up to the demarcation point of the carrier at the participant’s site. Each AP is connected to the respective hosts via redundant leased lines. Participants are connected to an AP via dedicated leased lines and/or via the Internet.

3.1 Repo Connectivity

The F7 system minimizes the footprint on the participant’s infrastructure. F7 removes the local Service Connector from the client and implements a browser based GUI solution, which requires zero maintenance by the participant.

Both, the browser based GUI and the F7 API can connect to F7 either via leased line or via Internet.

In either case a client authentication is done by using x.509 certificates. The certificate is used to encrypt all data transmitted between the browser based GUI or any third party application.
3.1.1 Leased Line

All leased line connections must be ordered from Deutsche Börse – directly or via a technical service provider. The Deutsche Börse network is a highly efficient network focused on highest availability by simultaneously providing lowest latency.

F7 Trading participants who already have existing Deutsche Börse network connectivity in place are able to order a dedicated channel, providing that sufficient bandwidth is available.

As the F7 system connects each individual user directly to the trading platform, bandwidth requirements are directly proportional to the number of active users. Bandwidth consumption per active trader is expected to be around 0.420 Mbit/s. Bandwidth options are offered in the following sizes:

<table>
<thead>
<tr>
<th>Number of active users</th>
<th>Bandwidth Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.5 Mbit/s</td>
</tr>
<tr>
<td>Up to 2</td>
<td>1.0 Mbit/s</td>
</tr>
<tr>
<td>Up to 6</td>
<td>3.0 Mbit/s</td>
</tr>
<tr>
<td>Up to 12</td>
<td>5.0 Mbit/s</td>
</tr>
<tr>
<td>Up to 25</td>
<td>10.0 Mbit/s</td>
</tr>
</tbody>
</table>

3.1.2 Internet

It is possible to use the F7 trading GUI as well as the F7 API via the Internet. The previously used software VPN encryption is longer required as all traffic is secured by use of x.509 certificates for basic authentication and connection encryption.
As F7 connects each individual user of the F7 system directly to the trading platform, bandwidth requirements are directly proportional to the number of active users. Users connecting via Internet should expect:

0.420 Mbit/s bandwidth consumption per active trader

### 3.2 Connectivity security features

For the connection via Internet, the participant can choose one of the following options:

- Allow Internet access without restrictions (per default)
- Completely disable Internet access and restricting to leased line (x.509 upload page)
- Allow Internet access for registered IP addresses

Details on configuring Internet access security features can be found in chapter 7.6.

Please note: any changes (adding or deleting of data) to these settings will take affect on the next business day.

For the connection via leased line, the incoming IP address is checked against the known network information for the corresponding participant. In case a participant has a Service Provider, the IP address is also checked against the known networks of the Service Provider.

On login via leased line it is checked if the IP-address of the user is part of the corresponding network.

### 3.3 URLs and IP ranges

**3.3.1 F7 GUI**

The F7 GUI can be accessed via links or URLs. These URLs differ based on the type of connection (Leased line vs. Internet) and based on the environment (Production vs. Simulation vs. Advanced Simulation).

Any of these four URLs can be placed in the bookmarks of the user’s browser, or placed as links on the desktop.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Type</th>
<th>URL</th>
</tr>
</thead>
</table>
3.3.2 F7 API

The F7 API connection gateways are accessed via direct IP addresses. These IP addresses differ based on the type of connection (Leased line vs. Internet) and based on the environment (Production vs. Simulation vs. Advanced Simulation).

<table>
<thead>
<tr>
<th>Environment</th>
<th>Type</th>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation</td>
<td>Leased Line</td>
<td>simu-f7-api.vpn.eurexrepo.com</td>
<td>11575</td>
</tr>
<tr>
<td></td>
<td></td>
<td>193.29.95.217 / 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>simu-f7-api.eurexrepo.com</td>
<td>11575</td>
</tr>
<tr>
<td></td>
<td></td>
<td>193.29.90.166 / 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td>Leased Line</td>
<td>advsimu-f7-api.vpn.eurexrepo.com</td>
<td>11975</td>
</tr>
<tr>
<td>Simulation</td>
<td></td>
<td>193.29.95.220 / 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>advsimu-f7-api.eurexrepo.com</td>
<td>11975</td>
</tr>
<tr>
<td></td>
<td></td>
<td>193.29.90.169 / 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td>Production</td>
<td>Leased Line</td>
<td>prod-f7-api.vpn.eurexrepo.com</td>
<td>11475</td>
</tr>
<tr>
<td></td>
<td></td>
<td>193.29.95.218 / 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>prod-f7-api.eurexrepo.com</td>
<td>11475</td>
</tr>
<tr>
<td></td>
<td></td>
<td>193.29.90.167 / 255.255.255.240</td>
<td></td>
</tr>
</tbody>
</table>

Depending on the AMQ client library used, the connection URIs need to use the fully qualified domain names for certificate handshake.
4. Environments

F7 offers the following dedicated environments for customer access:

- **Production**
  Production trading, full size resources, “real money”

- **Simulation**
  Simulation meant to get acquainted with new functionality. Aimed at GUI uses and software developers (API). Less powerful resources, compared to Production.

- **Advanced Simulation**
  Dedicated environment for software regression testing. Aimed at software developers (API). Limited resources.

4.1 Release update timeline

When a new software version of F7 is being rolled out, it is installed in the Simulation environment first.

Roughly six weeks later the Production environment is then updated to the new version as well. During these six weeks the Simulation environment is used by software vendors to adjust their software to the new F7 release. At the same time traders can acquaint themselves with new features in the F7 trading GUI.

During these six weeks, while the Simulation environment is already on a new F7 release and the Production environment is still on the previous release, the Advanced Simulation environment becomes a valuable resource for software developers who need to develop or test software which runs on the current production release.

The following diagram depicts a typical F7 release rollout over all three environments for a fictitious update from F7 release 99 to release 100:

![Diagram showing release update timeline for F7 environments](image)

Please note, while F7 Advanced Simulation has dedicated network addresses it shares the client x.509 certificates (see chapter 7) with the regular Simulation environment. Any x.509 certificate uploaded for F7 Simulation is automatically valid for F7 Advanced Simulation too.
Initial member and user setup for Advanced Simulation is taken from the Simulation environment. After this initial synchronization, both environments will remain independent of each other and no further member / user synchronization will be done.
5. **Member Section**

The Eurex Repo member section can be entered via this web address:

https://member.eurexrepo.com

It is also accessible from the Eurex Trading, Eurex Clearing and Xetra member section by using the switch portal link at the top of the page.

This leads you to the welcome page of the Eurex Repo member section.
6. Leased Line connectivity ordering

In order to start the order process press “Technical Connection” and select “Requests & Configuration” on the left hand side of the page.

An overview of your installations and their respective configuration is displayed.

6.1 New connection

Select the tab “New Request” and then press “New Connection”

You have now entered the line order frame. Use the “Dedicated Leased Line Connections” tick mark for leased line orders.
This is also true if you already have a dedicated line where additional space is available.

The next step is the location selection and the selection of the person who is the “Line Responsible”.

### 6.2 Location details

For the location, you can select an existing location or create a new location. The new location creation is self-explanatory.
In order to select the “Line Responsible” you have to press “Select”. A new pop up window shows the persons who are already registered for your company and allows to edit them or to create a new contact.

Please note that the “Line Responsible” should be a person who always has immediate access to the location where the line will be delivered. This person will be contacted by the carrier.

Here you can also use the tick box at the bottom of the frame in order to choose a second location with another “Line Responsible”.

### 6.3 Connection type

The next step is to select the connection (type). For F7 you can choose one channel on a leased line or two channels on two leased lines (for highest reliability). Please tick the appropriate box in order to achieve this.

In the lower half of the screen, under “Market/Channels” you have to choose “Eurex Repo” by scrolling down and selecting the tick box, then choose the participant ID (“Member ID”) used for this connection, the bandwidth and finally the Base Installation in which this line should be placed. For a new installation, select “New Base”.

### 6.4 Data center details

The next step is important when a new physical line has to be delivered. In order to achieve a smooth handling by all involved parties, room and line details have to be specified.
Room description, floor, room number, media, interface are mandatory fields. It has to be specified if a line installation can be done within business hours or not, whether the router and end facility are located in the same room or not and if it is Rack-mountable or a Desktop (stand-alone) device.

If this is a new location, a new room can be created; else, an existing room can be used.

In the case, that you have ordered two lines into two different locations (split location) also the room in the second location has to be selected or created and specified in an additional step.

### 6.5 Request summary

In the next step, an overview of the request is shown. By pressing “Add to the request basket” your request is then placed in the request basket. Please review this page thoroughly and add the overall “Technical Contact” for this request (typically the person who also will perform the connection test).
It is advisable to use the "Check Request" in order to perform a consistency check of your request. Tick the box in order to agree to the conditions and finally press "Approve" in order to finalize this order.
7. **F7 x.509 certificates**

To ensure the highest possible level of security and privacy against eavesdropping, a two-factor authentication is required for every participant. Both parts of the authentication process need to be completed successfully before access to the F7 GUI is granted or an F7 API application can connect.

The two-factor authentication process involves on the one hand the creation and usage of self-signed SSL certificates to establish and ensure an encrypted connection between the participant and F7.

Certificate authentication is required for both Internet and Leased Line access.

On the other hand, every single GUI or API user has to be authenticated by means of the individual username and password to be able to log into the GUI or API.

**Please note:**

Certificates can have user or participant scope or some other participant specific scope (e.g. location, unit, market etc.). Every participant needs at least one certificate in order to access F7 but may use an unlimited number for various reasons. In any case, the uploaded certificate must match the PKCS#12 file installed in the browser.

For a successful upload to the portal, a self-signed SSL certificate (crt.-file) is required which needs to comply with the following parameters:

- RSA and DSA key algorithms and SHA-2 signature algorithms (e.g. SHA224, SHA256, SHA384, SHA512) are supported
- Compliant with X.509v3 standard
- Key length needs to be between 1976 and 4096 bits
- Only letters and numbers (no special characters) are allowed
- Letters have to be in upper case, i.e. no lower case letters are to be accepted
- The total length must not be shorter than 15 and not longer than 22 characters
- The Common Name (CN) is also the complete account name and is composed as follows:
  - 5-digit participant ID followed by 3 digits “GUI” or “API” depending on the application the certificate will be used for, thereafter a free user defined string from 7 to 14 characters must be used for your internal description

While the procedure described in the next chapter outlines the preferred way of creating certificates for GUI and API users with the Java keytool, chapter 7.2 describes an alternative way of GUI certificate creation with the tools provided by OpenSSL.

It is recommended to follow the procedure described in the chapters below as close a possible to create valid certificates. For technical reasons F7 connectivity only accepts self-signed certificates (as described in the procedures below). Certificates signed by a third party CA will not allow access to the F7 system. It is not recommended to use any kind of certificate extensions and add information like eMail addresses to the certificate.

Please note, that during the SSL handshake such additional information (i.e. eMail addresses added to the certificate) would be visible to all clients attempting an SSL connection.

F7 certificates have a validity of up to three years (1090 days) maximum. All examples below use a validity of one year (365 days).

### 7.1 x.509 Certificate creation with Java keytool

The following chapter outlines the procedure for creating a self-signed x.509 certificate, the creation of a keystore and a truststore, and finally the import of the F7 API broker certificate into the truststore, using the Java tool “keytool”.

Java keytool is part of the standard Java distribution. It is a key and certificate management utility, organizing certificates in keystores and truststores, which can then be accessed by Java applications.

This chapter describes the recommended procedure for F7 GUI and F7 API users. Chapter 7.1.4 describes how to extract a browser compatible certificate for GUI usage.

Please note, in the following examples the following is assumed:

- You have the keytool in your PATH.
- You are in a directory where you have write permissions to create files.

Four files will be created:

- A keystore, containing your private key(s)
- A truststore, containing the public key(s) from other parties (i.e. F7)
- A public certificate for upload to the Eurex Repo Member section
- A private certificate for installation into the browser of a F7 GUI User

The following examples use a participant ID “INTER” – replace this with your own participant ID.

The following examples always use a password “mypass”. Change this to a password of your own choice.

All parameters, which should be changed according to your individual setup, are underlined.

7.1.1 Create keystore

The first step is to create a F7 certificate and a keystore to store the new certificate in. The command line example below determines the parameters of the certificate (RSA algorithm, key size 2048, one year validity, SHA256 signature and a keystore file name “INTER.ks” and a store password “mypass”):

```
keytool -genkey -keyalg RSA -keysize 2048 -validity 365 -sigalg SHA256withRSA -alias inter -keystore INTER.ks -storepass mypass -keypass mypass -dname CN=INTERAPITRDFR123
```

It is important that the entered Common Name (-dname CN=) always consists of the own participant ID, in this example “INTER” followed by “GUI” or “API” depending on the application the certificate will be used for and a free identifying string.

- The first 5 digits are your participant ID (“INTER” in this example)
- The next 3 digits identify the purpose of the certificate. If the certificate will be used for GUI access “GUI” has to be entered. If the certificate is used to connect to the API “API” has to be entered.
- Thereafter a free user defined string from 7 to 14 characters must be used for your internal description.

The Common Name must be identical to the free text field of the account name provided during the upload of the self-signed certificate into the member section.

At this point, a keystore file “INTER.ks” has been created, containing one certificate with an alias name “inter” for reference.
7.1.2 Export certificate for upload

Now the certificate for INTER will be extracted from the keystore previously created. Note the option "-rfc" to ensure the output format will be accepted by the member section when uploading the certificate to the Eurex Repo webpage.

```bash
keytool -export -rfc -alias inter -file INTER.cer -keystore INTER.ks
```

The name of the exported file for upload to the member section is "INTER.cer". It should look similar to the example output below:

```
-----BEGIN CERTIFICATE-----
MIIDaDCCAlCgAwIBAgIEU7ErtzANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJERE
TPEMA0GAEUECBMBGSGVzc2VuMRJwEAYDQYJKoZIhvcNAQEBBQADSwAwDgYDVQQK
-----BEGIN CERTIFICATE-----
MIIEaDCCAlCgAwIBAgIEU7ErtzANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJERE
TPEMA0GAEUExCzAJBgNVBAYTAlMGCMgCzAJBgNVBAMTD0JvZ1JldGNoIE15OGlO
-----BEGIN CERTIFICATE-----
MIIEaDCCAlCgAwIBAgIEU7ErtzANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJERE
TPEMA0GAEUExCzAJBgNVBAYTAlMGCMgCzAJBgNVBAMTD0JvZ1JldGNoIE15OGlO
-----BEGIN CERTIFICATE-----
MIIEaDCCAlCgAwIBAgIEU7ErtzANBgkqhkiG9w0BAQsFADB2MQswCQYDVQQGEwJERE
TPEMA0GAEUExCzAJBgNVBAYTAlMGCMgCzAJBgNVBAMTD0JvZ1JldGNoIE15OGlO
```

Upload the X.509v3 compliant .cer-file into the member section via Internet. See chapter 7.4 for details.

7.1.3 Import AMQP server certificate (F7 API only)

In case the keystore / truststore is used for the F7 API the AMQP server/broker certificates provided by F7 need to be imported into a truststore.

The server / broker certificate of F7 API can be downloaded in the Eurex Repo Member Section > Repo Resources > Trading System F7 > System Documentation > Network Access.

Please note, there are two ZIP files for download available. One for the F7 simulation environment and one for the F7 production environment:

- Production F7 API broker/server certificates for Internet and leased line to import into your Truststore
- Simulation F7 API broker/server certificates for Internet and leased line to import into your Truststore

Please note: The F7 server/broker certificates do expire periodically – usually every three years. Eurex Repo will inform you via Implementation News and technical info mail when the server/broker updates are due for an update.

Please note:

- The F7 server/broker certificates do expire periodically – usually every three years.
- Eurex Repo will inform you via Implementation News and technical info mail when the server/broker updates are due for an update.

There are two certificates in each of the BrokerCerts.zip, one for leased line access (contains "vpn" in the filename) and one for Internet access.
The following example uses the AMQP server/broker certificate by F7, which is stored in a file “simu-f7-api_eurexrepo_com_cert.crt” (Internet Access, Simulation). It has to be imported in a truststore (INTER.ts) by the following command:

```
keytool -import -file simu-f7-api_eurexrepo_com_cert.crt -keystore INTER.ts
-storepass mypass -alias f7apiserver
```

Or alternatively for leased line, Simulation with file “simu-f7-api_eurexrepo_com_cert.crt”

```
keytool -import -file simu-f7-api_vpn_eurexrepo_com_cert.crt -keystore INTER.ts
-storepass mypass -alias f7apivpnserver
```

Both, leased line and internet server certificates can be imported into the same truststore.

If no truststore “INTER.ts” existed before, it will be created automatically by importing the first broker / server certificate.

The alias can be chosen freely. “f7apiserver” / “f7apivpnserver” are only used as an example above.

### 7.1.4 Client PKCS#12 certificate for installation into the F7 GUI user’s browser

Finally, the following command exports the certificate in a format which can be imported into the browser of a F7 GUI user:

```
keytool -importkeystore -srckeystore INTER.ks -destkeystore INTER.p12 -deststoretype PKCS12
```

Enter destination keystore password: mypass
Re-enter new password: mypass
Enter source keystore password: mypass
Entry for alias inter successfully imported.

Import command completed: 1 entries successfully imported, 0 entries failed or cancelled

The PKCS#12 file will be saved automatically in the current working directory. Afterwards install the PKCS#12 file into the very same web browser which will be used to access the F7 trading GUI later - please note that not all browsers are supported (see chapter 2.1 for supported browsers).

Please refer to your individual browser documentation on how to manage browser certificates. For example, for Firefox this information can be found following this link:


By following the steps in the chapters 7.1.1 to 7.1.4 four files have been created:

- INTER.ks # Keystore, containing your own certificate
- INTER.ts # Truststore, containing trusted certificates
- INTER.cer # Cert for Upload to the Eurex Repo webpage
7.2 x.509 Certificate creation with OpenSSL

The following chapter outlines an alternative procedure for creating a self-signed x.509 certificate and a PKCS#12 file for installation into a F7 GUI user’s browser using the tool “OpenSSL”.

Please note, in the following examples the following is assumed:

- You have the OpenSSL binary in your PATH.
- You are in a directory where you have write permissions to create files.

The following examples use a participant ID “INTER” – replace this with your own participant ID.

Three files will be created:

- A private key (INTER.key)
- A self signed certificate for upload to the Eurex Repo Member section (INTER.crt)
- A private PKCS#12 certificate for installation into the browser of a F7 GUI User (INTER.p12)

The following examples use “mypass” where an individual passphrase needs to be entered. Change this to a passphrase of your own choice.

All parameters, which should be changed according to your individual setup, are underlined.

7.2.1 Step 1: Download OpenSSL

Download and install “OpenSSL” (recommended freeware tool) to create keys, self-signed certificates and PKCS#12 certificate files (recommended source: www.openssl.org, version 1.1.0g or 1.0.2n).

Avoid 1.0.1 versions up to and including 1.0.1f due to heartbleed bug.

7.2.2 Step 2: Create Private Key

Create a private key by using OpenSSL (e.g. RSA private key, 2048 bit).

Example command line for the participant ID INTER:

openssl genrsa -des3 -out INTER.key 2048

This results in:

Generating RSA private key, 2048 bit long modulus
.................................................................+++
.................................................................+++
e is 65537 (0x10001)

Enter pass phrase for INTER.key: mypass
Verifying - Enter pass phrase for INTER.key: mypass

After entering the necessary information, the private key will be saved automatically in the current working directory.

7.2.3 Step 3: Create self-signed certificate

The participant has to create a “self-signed certificate”.

INTER.p12 # Cert for installation into the browser
A “self-signed certificate” can be created by using OpenSSL (.crt-file compliant with X.509v3 standard and a validity of 365 days). For creation, the passphrase for the private key created above is required.

Example command line for the participant ID INTER:

```bash
openssl req -new -x509 -sha256 -days 365 -key INTER.key -out INTER.crt
```

This results in:

Enter pass phrase for INTER.key: mypass

The user is asked to enter the information that will be incorporated into his certificate request (the so-called Distinguished Name or a DN.)

There are quite a few fields to be filled in.

All fields except the Common Name should be left blank by entering “.”.

```
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: INTERGUIFRTRD123
E-Mail Address []:.
```

It is important that the entered Common Name always consists of the own participant ID, in this example “INTER” followed by “GUI” or “API” depending on the application the certificate will be used for and a free identifying string.

- The first 5 digits are your participant ID (“INTER” in this example)
- The next 3 digits identify the purpose of the certificate. If the certificate will be used for GUI access “GUI” has to be entered. If the certificate is used to connect to the API “API” has to be entered.
- Thereafter a free user defined string from 7 to 14 characters must be used for your internal description.

The Common Name must be identical to the free text field of the account name provided during the upload of the self-signed certificate into the member section.

After entering the necessary information, the self-signed certificate will be saved automatically in the current working directory.

- Participant may check the generated “self-signed certificate” by using OpenSSL.

Example command line for the participant ID INTER:

```bash
openssl x509 -text -in INTER.crt -noout
```

This results in:

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
8:e3:e3:0b:97:63:7c:3c
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=INTERGUIFRTRD123
Validity
Not Before: Nov 28 16:53:26 2011 GMT
Not After: Nov 27 16:53:26 2012 GMT
Subject: CN=INTERGUIFRTRD123
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
e2:37:ec:0f:9b:bd:45:25:31:1b:be:fa:1c:00:80:
f0:b7:a2:11:ff:1e:00:20:81:62:d7:da:b5:9b:ab:ad:
8a:2d:6e:cc:88:0a:bd:a3:ce:b0:c6:70:e8:7d:2d:
3a:a3:32:3d:58:09:4f:92:32:8e:2f:ff:ee:43:
14:dd:94:7c:00:4a:8c:1f:ad:29:52:01:0e:28:0d:
5e:0d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:
DirName:/CN=INTERGUIFRTRD123
serial:8E:E3:E3:0B:97:63:7C:3C
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
1d:bf:7d:04
Upload the .crt-file (X.509v3 compliant) into the member section via Internet. See chapter 7.4 for details.

**7.2.4 Step 4 create PKCS#12 file**

The participant creates PKCS#12 file by using the stored private key and the self-signed certificate (.crt-file) in OpenSSL.

Example command line for the participant ID “INTER”:

```
openssl pkcs12 -export -clcerts -in INTER.crt -inkey INTER.key -out INTER.p12
```

The PKCS#12 file will be saved automatically in the current working directory. Afterwards install the PKCS#12 file into the very same web browser, which will be used to access the F7 trading GUI later - please note that not all browsers are supported (see chapter 2.1 for supported browsers).

Please refer to your individual browser documentation on how to manage browser certificates. For example, for Firefox this information can be found following this link:


**7.3 Certificate validity period**

To ensure security we recommend a validity period of 365 days for certificates. The maximum validity accepted is three years (1090 days). The upload of a new certificate in good time prior to the end of the validity period is required.

Please note: Any uploaded certificate will become active on the following business day. The F7 system is not actively informing users about approaching certificate expiry dates. Please ensure to replace expiring certificates in due time.

**7.4 Certificate upload**

For a secure connection to the F7 GUI or API the participant has to upload a self-signed certificate file to the member section, while additionally installing the complementary browser certificate file (in the format ‘PKCS#12’ in his web-browser.

For uploading a certificate, navigate to the Eurex Repo member section, select “Technical Connection” and then “Eurex Repo Certificates” under the menu “Technical User Administration”: 

7.4.1 User ID Configuration

To upload a certificate it is required to create an account in the member section by clicking on “Create user”.

The user ID created here has to be identical to the Common Name (CN) used in the certificate about to be uploaded.

For example to upload a certificate with CN="INTERAPITRD1234" a user account "INTERAPITRD1234" needs to be created.

Please note that the member section is only used for the certificate handling for a participant.

All requests to personal user/trader logins needs to be requested by submitting a ‘User Setup Form’ (“Händler Antrag” / “Info User Antrag”) to Eurex Repo.

7.4.2 Multiple certificates attached to one User ID

Although technically possible, it is not recommended to add multiple certificates to the same user in the member portal.
When multiple certificates are added to the same user ID as shown in the screenshot above, only one of those certificates will be usable at any given time.

In situations where certificates expire and you want to upload a new certificate, it is rather recommended to create a new user in the portal and to create the new certificate with a new Common Name (CN).

### 7.4.3 Environment

Select the environment the new certificate will be used in: production or simulation.

Please note: as stated in chapter 4, certificates uploaded for the Simulation environment become automatically usable for the Advanced Simulation environment too.

### 7.4.4 Account Name Field

The Account Name consists of a drop-down list and a free text field.

- In a first step the participant ID needs to be selected from the drop-down list. All participant IDs, for which an account can be setup, are selectable here (e.g. INTER).
• In the free text field, a 10 to 17 digit uppercase alphanumeric value has to be provided. The participant ID (e.g. ITNER) is not to be entered here as it has been selected already in the drop-down.
  o The first 3 digits identify the purpose of the certificate. If the certificate will be used for GUI access “GUI” has to be entered. If the certificate is used to connect to the API “API” has to be entered.
  o Thereafter a free user defined string from 7 to 14 characters must be used for your internal description.

Please note: The information in both fields “Account Name” has to match the Common Name of the certificate.

The complete Account Name should look like this:
The Common Name (CN) of the certificate must match the account name. For our example participant ID the name of certificate would look like this ‘INTERGUIEREPOUSER’ or “INTERGUltrdfri123” or “INTERAPItrdfri123” from the examples used earlier in this document.

Please note: If the Account Name and the Common Name of the certificate differ, it will not be possible to upload the certificate. The Account Name of the certificate must contain the string “GUI” or “API” after the 5-digit participant ID, else the certificate will be rejected by F7.

7.4.5 ‘Description’ field

As the field ‘Description’ is a free text field any information can be provided. However, for a better overview it is recommended to provide some information regarding the certificate (e.g. technical information), the participant (e.g. participant ID) and the environment in which the certificate is being used.

Example for participant ‘INTER’:

| Description | Certificate for INTER |

7.4.6 Certificate upload verification

If a problem occurs during the upload process or if a mandatory field is empty, an error message will appear in the member section (see two examples below).

- Account Name does not match common name (=CN) of certificate!
- The certificate does not contain a Common Name (CN)

If no error message appears after clicking on ‘save’ the certificate has been uploaded successfully to the member section and the new account should be displayed in the overview screen, including ‘User ID’ and ‘Description’.

Uploaded certificates are transferred and activated nightly to the F7 trading system. Uploaded certificates will become usable on the next business day.

7.5 Username and password authentication

In order to login and use the F7 trader GUI or a third party application the participant must complete the second part of the two-factor authentication process - username and password authentication.

7.6 Additional IP Address check (Internet access)

Default any user of the given participant is permitted to access the application from any IP address. If the participant wants to restrict the default access, a list of IP addresses can be entered in the member section. As a result, it will only be possible to access the application from these IP addresses.

Here is an example where access is limited from one IP address only:
Internet access for the given participant can be completely blocked by setting the corresponding radio-button.

Information about IP address checks is transferred and activated nightly to the F7 trading system. Any changes (e.g. adding or deleting IP addresses) will become effective on the next business day.
8. **Further information and contacts**

Eurex Repo’s web page [http://eurexrepo.com](http://eurexrepo.com) is the central source for all relevant information regarding F7. General information and FAQs can be found within: *Trading System F7*.

Additional items are also available:

- **Access the Member Section “Requests & Configuration”**
  [www.eurexrepo.com > Member Section > Technical Connection > Requests & Configuration](http://www.eurexrepo.com)

- **Documents for F7, including F7 API documentation, are available at:**
  [www.eurexrepo.com > Member Section > Repo Resources > Trading System F7 > System Documentation > Release 3.1](http://www.eurexrepo.com)

During simulation phases an additional source of information is available:

- **For most up-to-date information, please check our Implementation News at:**

Implementation News is updated regularly and informs participants about possible maintenance downtimes, updated documentation, and any other technical ad-hoc information relevant for using the F7 simulation environment.

To stay conveniently up to date, a RSS feed is provided too:

Please do not hesitate to contact us in case of any questions.

<table>
<thead>
<tr>
<th>Technical Support</th>
<th>Functional Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Technical Support</td>
<td>Eurex Repo Administration &amp; Operation</td>
</tr>
<tr>
<td>+49 (0) 69 2 11-1 08 77</td>
<td>+41 (0) 43 430 72 20</td>
</tr>
<tr>
<td><a href="mailto:cts@deutsche-boerse.com">cts@deutsche-boerse.com</a></td>
<td><a href="mailto:funchelp@eurexrepo.com">funchelp@eurexrepo.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Eurex Repo Sales</th>
<th>Member Section Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eurex Repo Sales</td>
<td>+49-(0) 69-2 11-1 78 88</td>
</tr>
<tr>
<td>+49 (0) 69 2 11-1 40 40</td>
<td><a href="mailto:member.section@deutsche-boerse.com">member.section@deutsche-boerse.com</a></td>
</tr>
<tr>
<td><a href="mailto:sales@eurexrepo.com">sales@eurexrepo.com</a></td>
<td></td>
</tr>
</tbody>
</table>
### 9. Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Chapter, page</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td>9-Aug-2014</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.5</td>
<td>1.2, 2.3.2</td>
<td>02-Nov-2015</td>
<td>Updated for F7 1.5. Added info about API broker fqdns and recommendations for QPID client libraries.</td>
</tr>
<tr>
<td>1.7</td>
<td>5.9, 5.11</td>
<td>13-Jan-2016</td>
<td>Updated for F7 1.7. Added info about certificate and IP filter transfer times</td>
</tr>
<tr>
<td>1.7.1</td>
<td>5.</td>
<td>22-Feb-2016</td>
<td>Improved chapters describing x.509 certificate creation</td>
</tr>
<tr>
<td>1.7.2</td>
<td>5.</td>
<td>08-Mar-2016</td>
<td>Usage of self-signed certificates only added. Certificate creation streamlined to include CN only.</td>
</tr>
<tr>
<td>2.0.0</td>
<td>5.</td>
<td>07-Jun-2016</td>
<td>Improved chapters describing x.509 certificate creation</td>
</tr>
<tr>
<td>2.0.1</td>
<td>5.1.3</td>
<td>27-Jun-2016</td>
<td>Updated link to broker certificate download</td>
</tr>
<tr>
<td>2.4.0</td>
<td>5.4.2</td>
<td>14-Jul-2017</td>
<td>Added info about adding multiple x.509 certificates with identical CNs to one account</td>
</tr>
<tr>
<td>2.4.1</td>
<td>1.2</td>
<td>28-Aug-2017</td>
<td>Updated qpid-jms to 0.24.0 (latest version)</td>
</tr>
<tr>
<td>2.6.0</td>
<td>All</td>
<td>14-Jan-2018</td>
<td>Updated for F7 2.6. Introducing F7 Advanced Simulation.</td>
</tr>
<tr>
<td>2.6.1</td>
<td>All</td>
<td>19-Feb-2018</td>
<td>Correction on header layout</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Updated qpid-jms to 0.29.0 (latest version)</td>
</tr>
<tr>
<td>2.6.2</td>
<td>2.1</td>
<td>07-Mar-2018</td>
<td>Updated supported browser versions for F7 GUI usage</td>
</tr>
<tr>
<td>3.0.0</td>
<td>All</td>
<td>25-Jul-2018</td>
<td>Updated for F7 3.0</td>
</tr>
<tr>
<td>3.0.1</td>
<td>7</td>
<td>26-Oct-2018</td>
<td>Added note about additional information disclosed during SSL handshake.</td>
</tr>
<tr>
<td>3.1.1</td>
<td>All</td>
<td>4-Apr-2019</td>
<td>Updated for F7 3.1</td>
</tr>
</tbody>
</table>