FWB / Eurex – Client & Member Reference Data Upload

How to connect via SFTP & upload files

Version 1.38

March 2019

Table of Content

1. Introduction

In order to comply with the MiFID II reporting obligations, trading participants will have to provide reference data (Client ID- short/ long code; certified Algo IDs) to the trading venues. For the upload of the respective data, we will offer customers the possibility to securely send files via the Secure File Transfer Protocol (SFTP) in addition to the file upload via the Xetra or Eurex Member Section.

In order to securely send files to the SFTP Xetra or Eurex server, the trading participant first needs to have a valid Legal Entity Identifier (LEI) and a separate SSH key pair (public/private key). For the time being, the trading participants are asked to generate this key pair themselves and send only the public key to customer.readiness@deutsche-boerse.com in **open SSH format** in order to validate the correctness of the LEI and import it into the server. Section 3 describes how such key pairs are generated in detail.

Please note that one LEI is always linked to just one SSH key and with this, the trading participant can provide data required for Xetra and/ or Eurex reference data ~~as well as for Deutsche Börse Regulatory Reporting Hub services. If a trading participant is already a Regulatory Reporting Hub user and has created the SSH key already, this key has to be used for all services.~~

This document

- Describes how to generate keys in order to connect to a SFTP server
- Explains step-by-step how to utilize user-friendly SFTP clients to get access to the server
- Describes how to generate correct inbound files
- Covers necessary contact data for technical and functional support.

2. Technical Pre-Conditions

Below are the hardware and software requirements to connect to the Xetra / Eurex server using SFTP protocol.

2.1. Hardware requirements

There are no particular hardware requirements to access to the Xetra / Eurex server via native internet. The server can be accessed with any computer running a SFTP client program. Trading Members connecting to the Common Report Engine (CRE) via a leased line can use the same connection for the transmission of short/long code mapping files. Please refer to the respective IP addresses for native internet or leased line connection in the text below.

2.2. Software requirements

To transfer files to or from a server via SFTP, a SFTP client is required. Our SFTP offering was tested with the following two commonly used clients:

- WinSCP (version 5.1.4)
- TurboFTP (version 6.30)

In this guide we describe the use of two commonly used clients in order to connect to the server successfully. Other SFTP client program like FileZilla are options that can be used but they are not described here.

3. How to generate and save SSH key pair

Please note that we recommend separate SSH key pairs for Simulation and Production for security reasons. In addition, only the public keys in the Open SSH format will be accept in our environments.

In Windows, PUTTY Key Generator (PuTTYGen) can be used to generate your SSH key pair. Note that the key pairs generated should be different. First, if needed download the PuTTYGen from the PuTTY download page PuttyGen Site and install it on your computer. Second, obtain and prepare to use a text editor such as Notepad++ that does not insert unwanted characters and metadata into a text file. After that, follow the steps below:

Step 1: Open the PuTTYGen application and select **RSA** for Type of key to generate and choose **the key length for Number of bits in a generated key**. The key length must be at least **2048**.

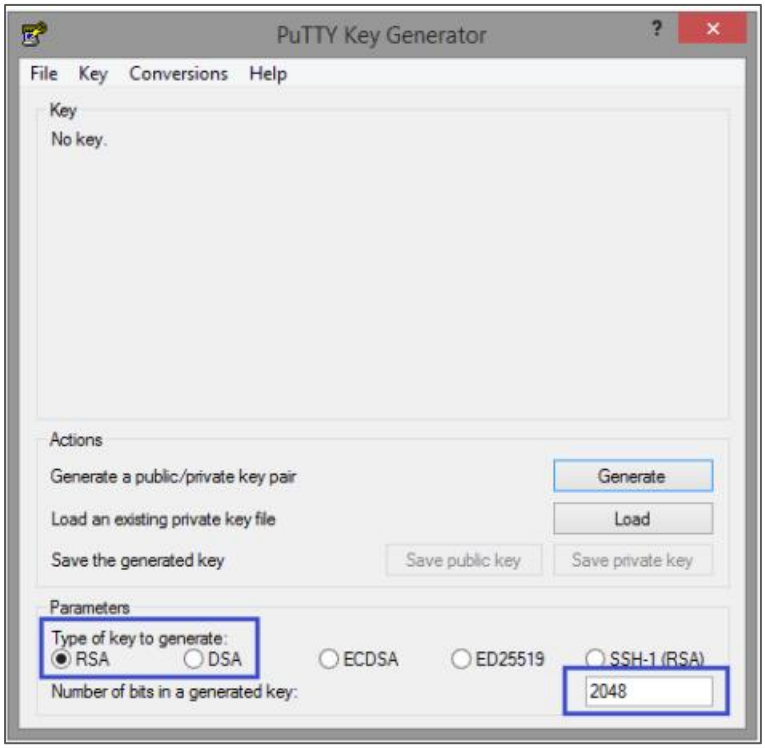


Figure 1 - Select the type and length of keys

Step 2: Click on the **Generate** button to get the prompt requesting to move the mouse for generating some randomness in keys. Then your keys will be created.

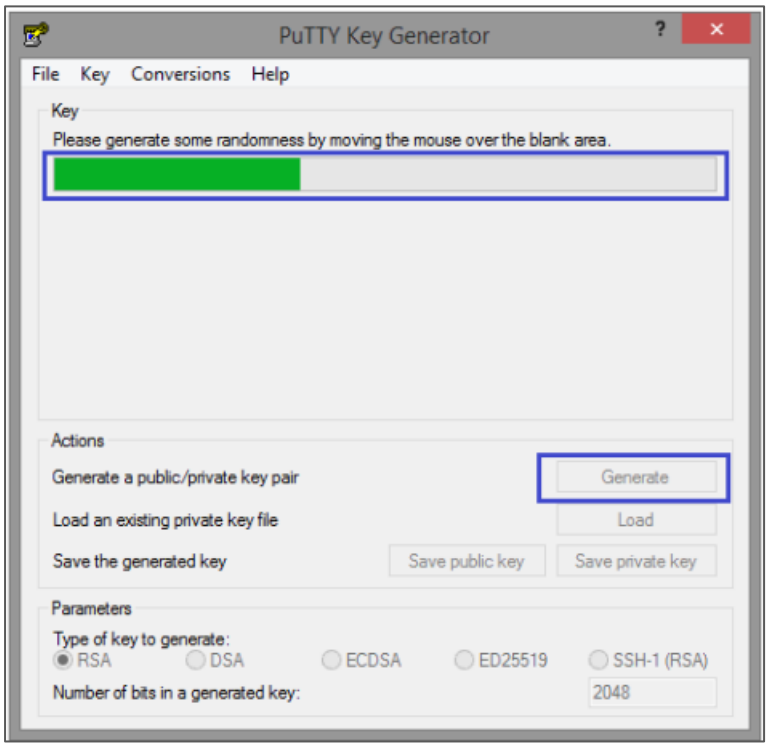


Figure 2 - Generate randomness in keys

Step 3: Put a suitable comment in the **Key comment** field so that you will remember what the keys are used for. Also type a passphrase in the **Key passphrase** field to use when accessing the private key and confirm it in **Confirm passphrase** field. You could use a key without a passphrase, but this is NOT recommended. This

passphrase is designed to encrypt the private key on disk, so you will not be able to use the key without first entering the passphrase.

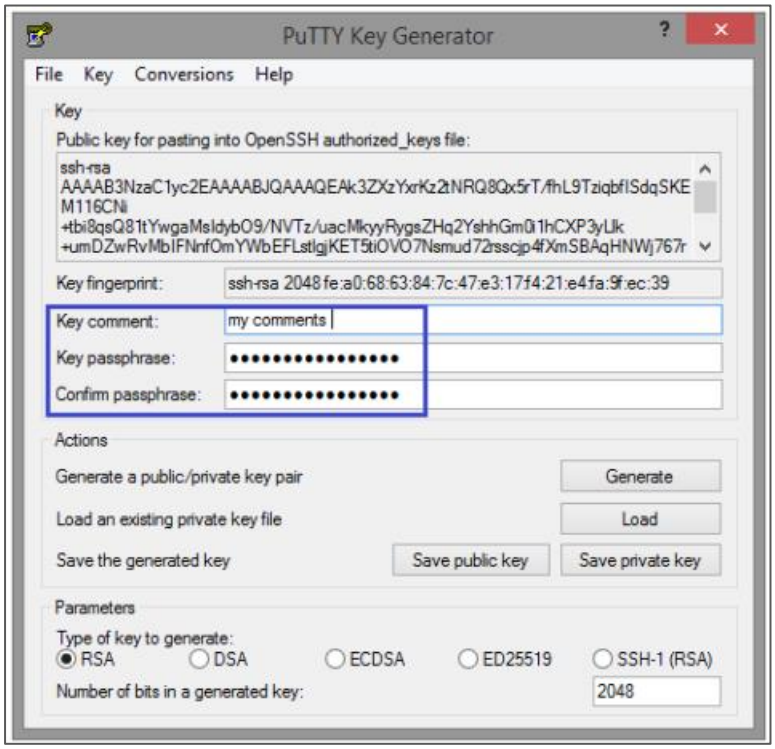


Figure 3 - Enter comment and passphrase

Step 4: Click on the **Save private key** button to keep the private key securely in a local repository. The key should have the extension **".ppk"** and named according the following rule (See Figure 4):

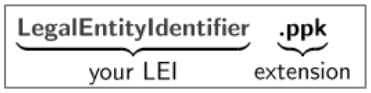


Figure 4: Naming convention for private key

Example: 529900G3SW56SHYNPR95.ppk

Step 5: As mentioned before, the public keys must be generated in the Open SSH format and only this format is supported by the SFTP service. Since using the "Save public key" button in the upper window of Figure 3 will save the key in the not supported PEM/OpenSSL format, users need to do the following to save the public key:

Select and copy the complete text in the box labelled **"Public key for pasting into OpenSSH authorized keys file"**. To do that, first open Notepad++ and confirm that the End of Line (EOL) format is set to **UNIX/OSX Format** as Figure 5 shows. This will ensure that there are no extraneous characters in the public key file.

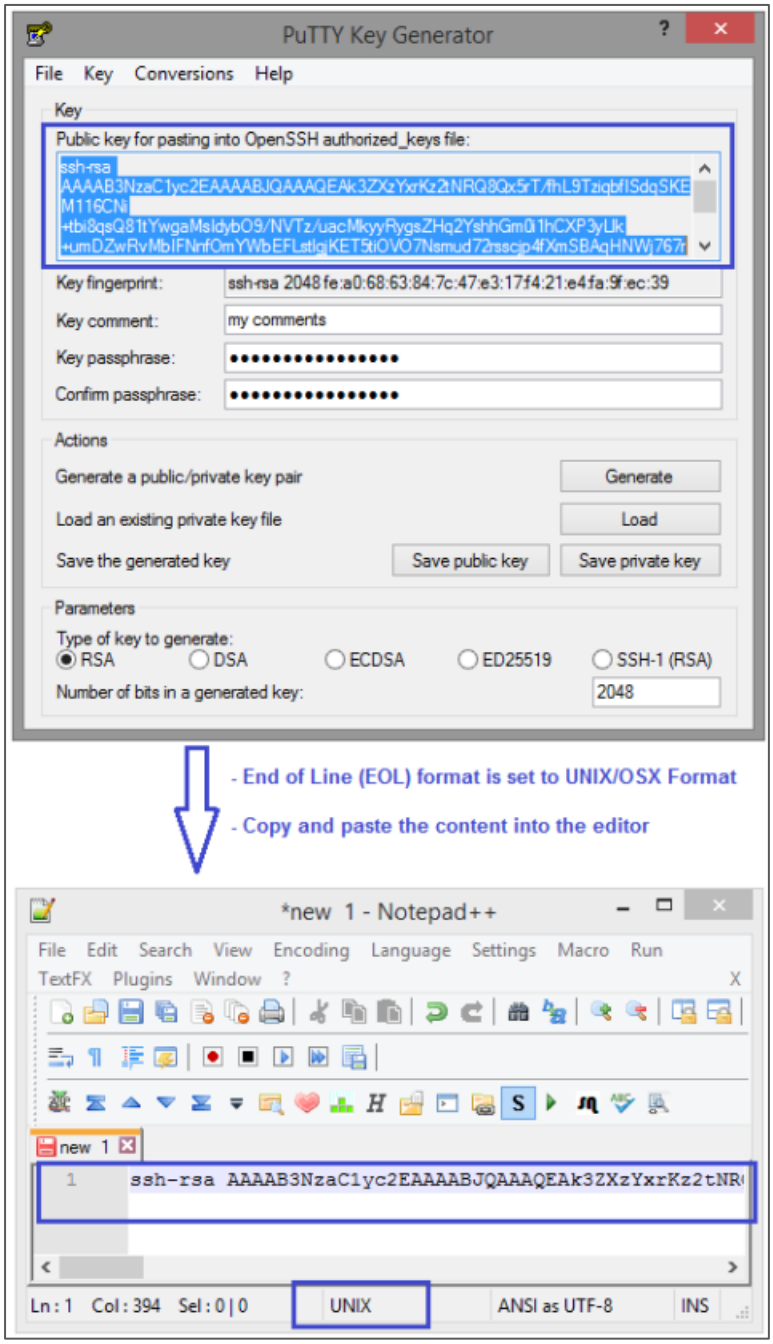


Figure 5 - Save the public key in the open SSH format via Copy & Paste

The public key file however should have the extension **".pub"** so that it will be readable by a regular text editor like Notepad++. The name of the public key must follow the rule (See Figure 6):

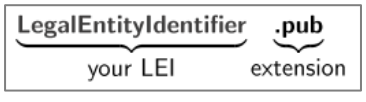


Figure 6: Naming convention for public keys

Example: 529900G3SW56SHYNPR95.pub

After generating the key pair, the user has to keep/store the private key in a safe place. The public key needs to be send via email to the customer.readiness@deutsche-boerse.com for validation and activation.

This key fingerprint is shown on the PuTTYGen window (Figure 8). In our example the hash value is equal to "fe:a0:68:63:84:7c:47:e3:17:f4:21:e4:fa:9f:ec:39".

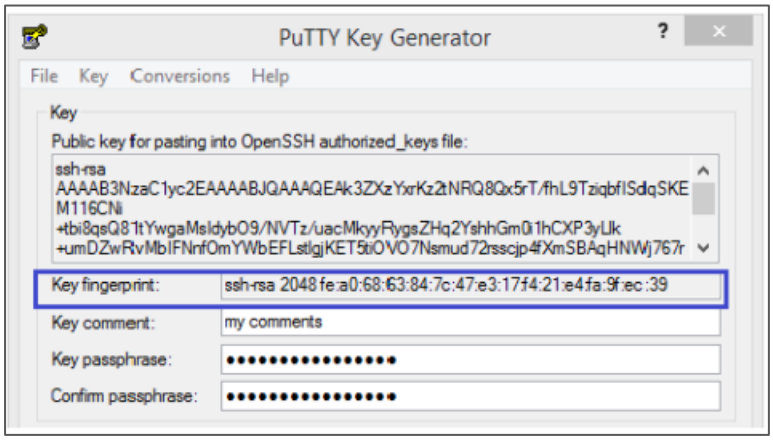


Figure 7: Hash value of the public key

4. How to connect to the SFTP server

To connect via SFTP there exist specialized and appropriate clients. In this document, only two clients are introduced: TurboFTP and WinSCP.

4.1. Using TurboFTP client

TurboFTP is an easy-to-use FTP client program with an Explorer-like interface that allows browsing remote directories, downloading or uploading files with drag and drop operation. Here are the steps needed to follow.

4.1.1 Collecting session details

Before connecting to the server, users first need to consider the following information:

- **Site Address**: this is the IP address of the SFTP server (environment). Ensure the valid IP address is inserted (see below).
- **Port:** this is the port number of the connection. Note that SFTP usually uses port 22 by default; you need to adapt it to 24.
- **User ID**: this should equal to the **LEI of your organisation**.

Native Internet IP addresses valid as of 15 October 2018:

Environment	IP Address	Port number
Simulation	194.36.239.242	24
Production	194.36.239.243	24

Leased Line IP addresses valid as of 15 October 2018:

Environment	IP Address	Port number
Simulation A-Side	193.29.90.72	2242
Simulation B-Side	193.29.90.104	2242
Production A-Side	193.29.90.71	2241
Production B-Side	193.29.90.103	2241

To use TurboFTP the following further information is also required:

- Site Name: a user will be asked to provide a name for a server connection. The Site Name will be saved to the FTP Address Book allowing for an easy selection of the server connection.
- Initial Local Directory: this is an optional directory. It is recommended to name the folder in which the user's test cases are available.

4.1.2 Connecting to the SFTP server

In order to connect via TurboFTP, users need to do the following:

Step 1: Start TurboFTP and a Login Dialog will appear.

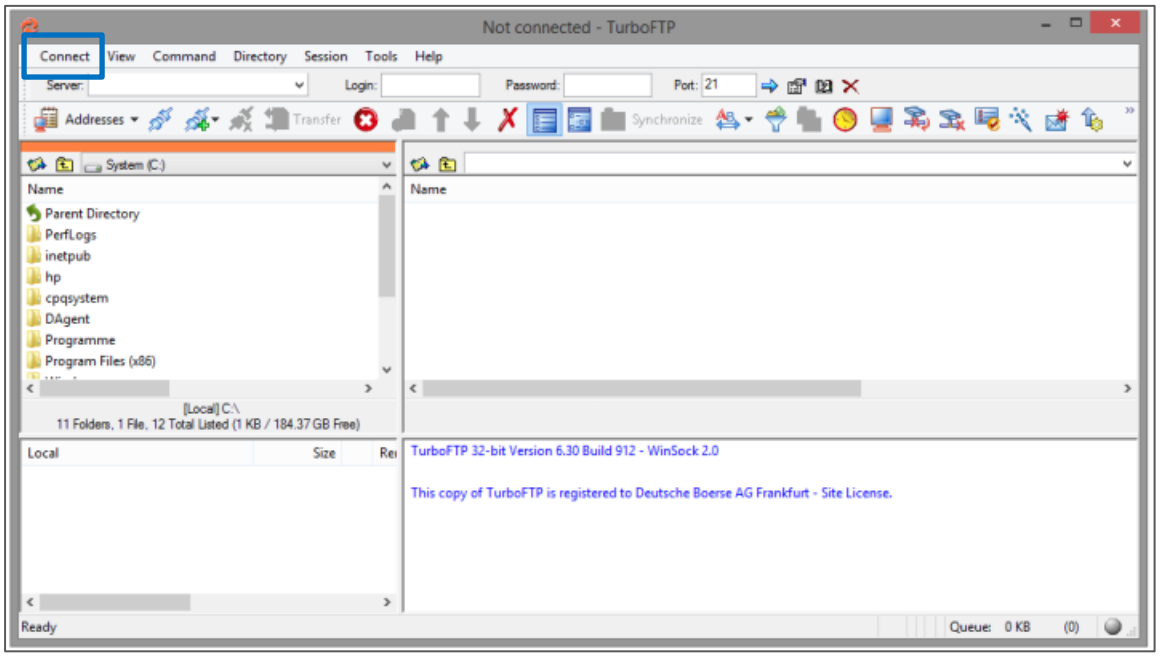


Figure 8 - TurboFTP login dialog

Step 2: Open menu-item "**Connect**" and click on "**Address Book**". The user should see the following screen:

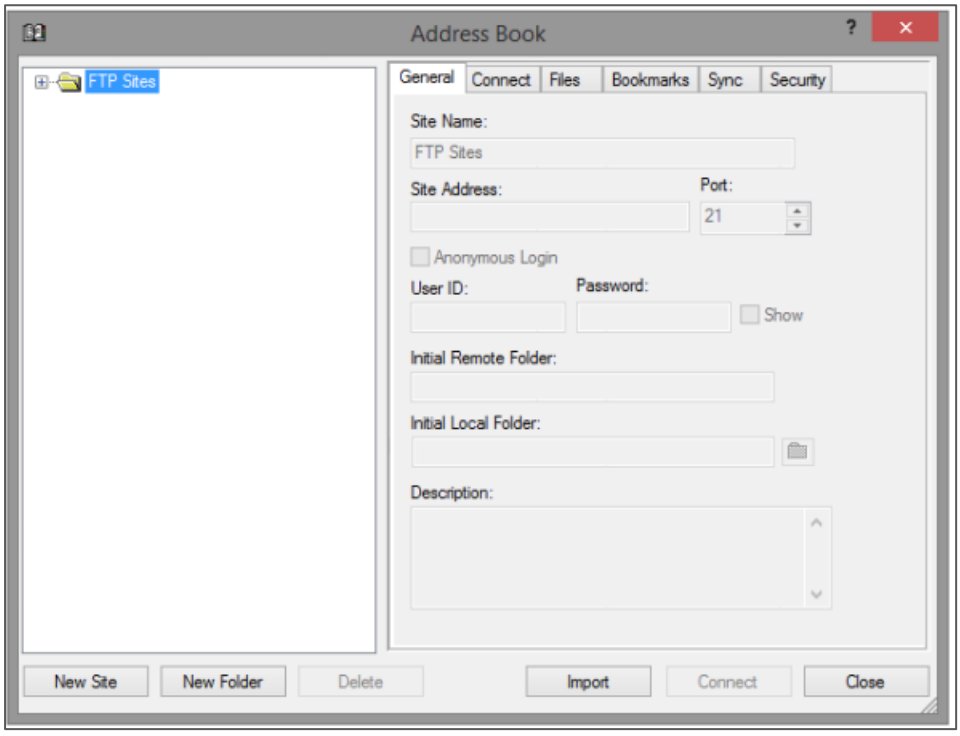


Figure 9 - Open Address Book

Step 3: Right-Click on **"New Site"** and key in your session details as described in Subsection 4.1.1 in the "**General"** tab:

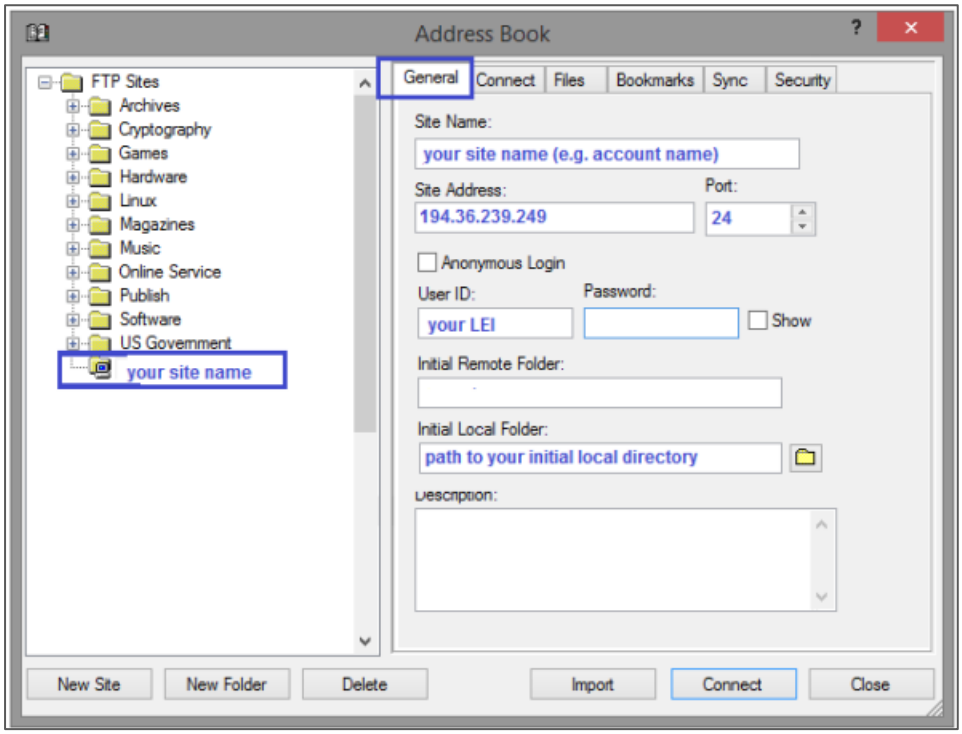


Figure 10 - Enter session details within General tab

Step 4: Switch to the **"Security"** tab and check the blue-framed boxes as Figure 11 shown below. After that, enter the following input parameters:

- **Password Encryption** is based on **SHA1** hash algorithm
- **Secure Connection Type** should be set to **SFTP over SSH2**
- **Port** number equals **24**
- **Public Key** is the path to the folder in which the public key is stored
- **Private key** is the path to the folder in which the private key is stored
- **Password** is the passphrase used to protect the private key

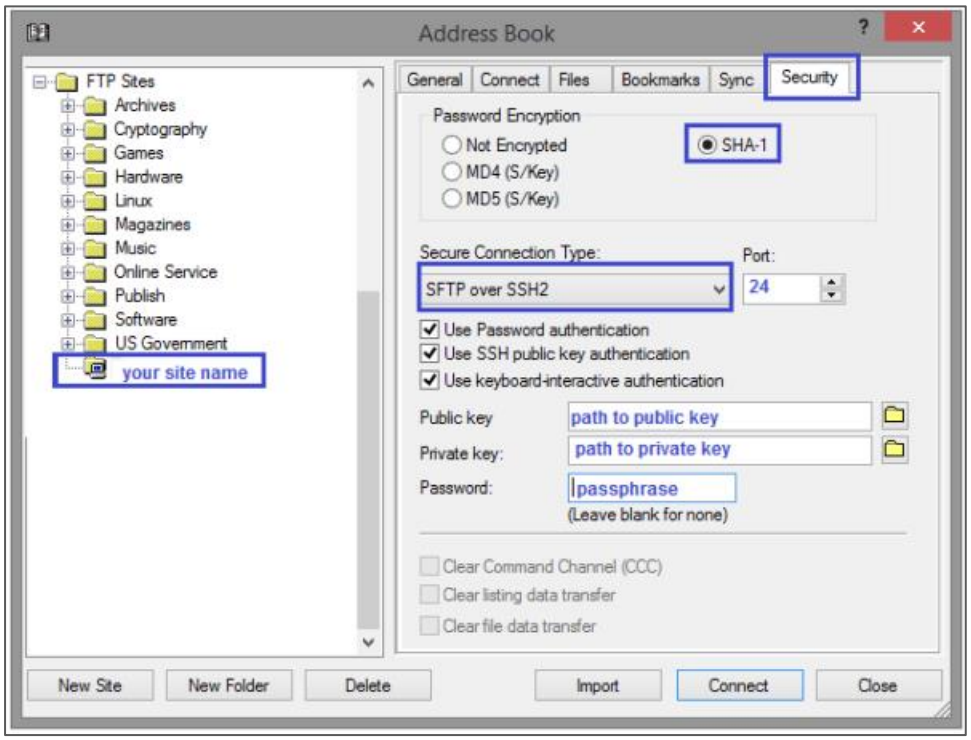


Figure 11 - Enter session details within Security tab

Step 5: Next, click on the "**Connect**" button to login. If the login was successful, the user should see a window like the following showing a "Login successful" message, the connection details (the user ID and the IP address of the server) as well as the remote directory which contains the relevant folders for submission (Figure 12). These folders are described as follows:

- The **Cash_Market_-_XETR_XFRA** folder: this is the location where the inbound files need to be uploaded by trading participants for processing Xetra (XETR) and Börse Frankfurt (XFRA) reference data.
- The **Eurex_Derivatives_-_XEUR** folder: this is the location where the inbound files need to be uploaded by trading participants for processing Eurex reference data.
- *Xetra/ Eurex reference data must not be placed in any other folder except the two mentioned above.*

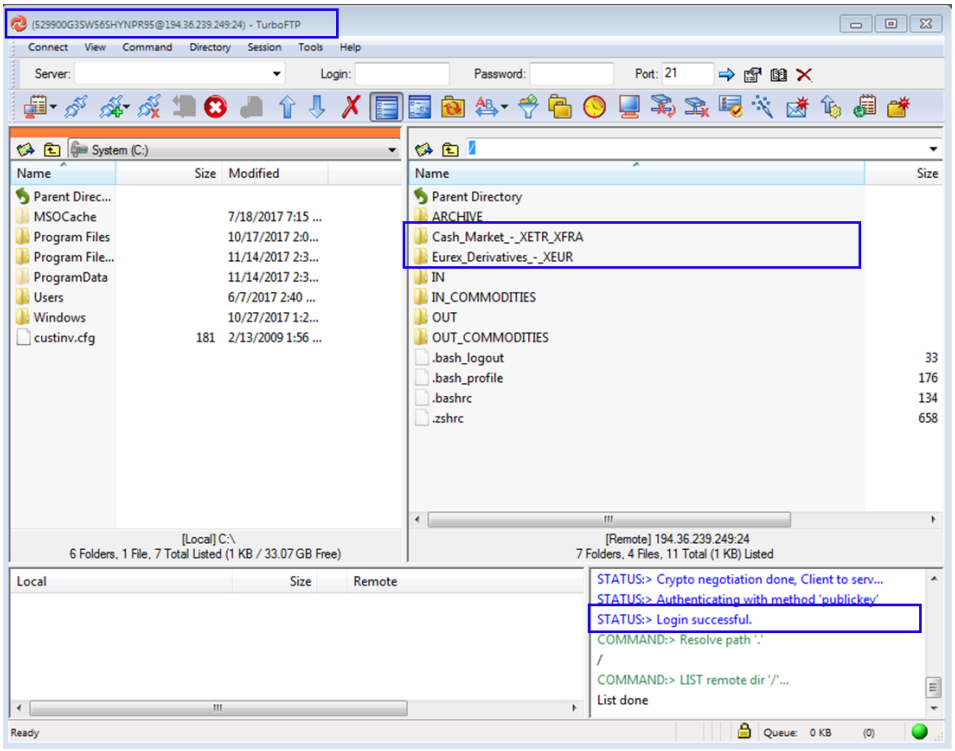


Figure 12 - Successful login via TurboFTP

The user is now connected and can upload files via TurboFTP.

4.1.3 How and where to upload files

After connecting to the server, users can upload files using the Drag & Drop function. Before starting with uploading any file, the user should take into account the file requirements listed in Section 5. Users should first adjust their files according these requirements, before uploading them via TurboSFTP as follows:

- Select the local files or directories to be transmitted from the local directory
- Drag selected files and drop them into the remote target folder named "**Cash_Market_-_XETR_XFRA**" or "**Eurex_Derivatives_-_XEUR**" depending on the market a file refers to.

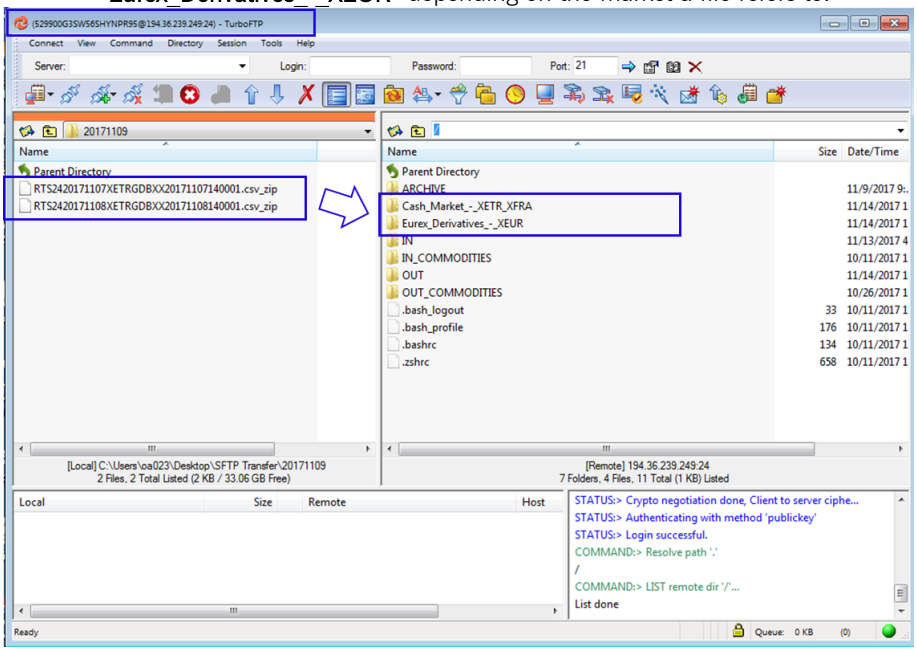


Figure 13 - Drag & drop the files into the input folder

If the files have been processed successfully, the trading participant receives a short message confirming that the data has been successfully transmitted. If not, the member receives an error message.

4.2. Using WinSCP client

WinSCP (Windows Secure Copy) is a free, open source file transfer tool for Windows. As with TurboFTP this client allows secure file transfers between the client's local computer and the remote server.

4.2.1 Collecting session details

The following connection information should be available for users in order to connect with WinSCP:

- **Host name** Host name: a user will be requested to provide the IP address of the SFTP server (environment). Ensure the valid IP address is inserted (see below).
- **Port number:** this is the port number of the connection.
- **User name**: this must be equal the **LEI** of your organisation.

Native Internet new IP addresses valid as of 15 October 2018:

Environment	IP Address	Port number
Simulation	194.36.239.242	24
Production	194.36.239.243	24

Leased Line IP addresses valid as of 15 October 2018:

Environment	IP Address	Port number
Simulation A-Side	193.29.90.72	2242
Simulation B-Side	193.29.90.104	2242
Production A-Side	193.29.90.71	2241
Production B-Side	193.29.90.103	2241

Private key file: a user has to specify the path to his/her private key.

4.2.2 Connecting to the SFTP server

To get access to the server, users need to do the following:

Step 1: Start WinSCP and a Login Dialog will appear.

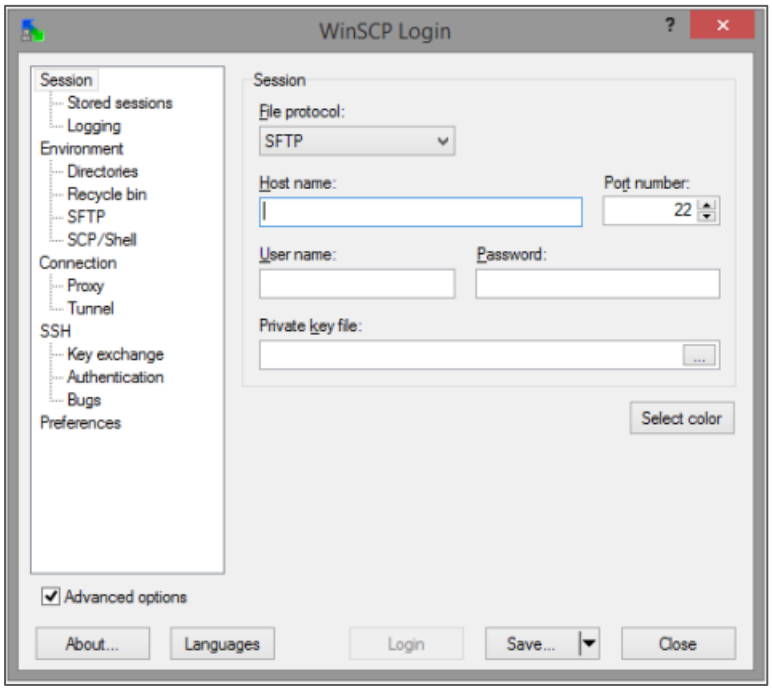


Figure 14 - WinSCP login dialog

Step 2: First set **the File Protocol** as **SFTP** and then enter the login credentials described in Subsection 4.2.1.

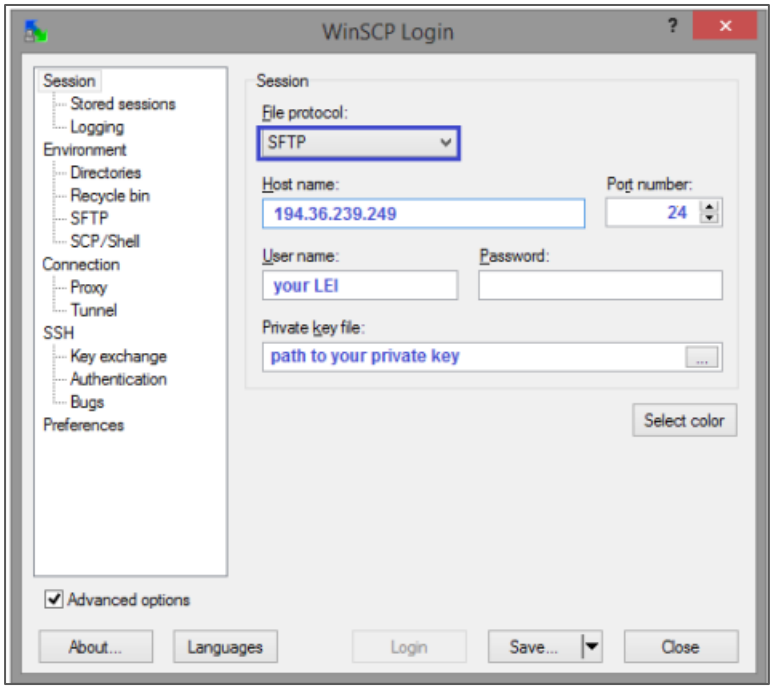


Figure 15 - Login credentials in WinSCP

Step 3: Choose **Directories** under **Environment** and click on **Browser** button to select the path to the local directory, in which the files for submission are located.

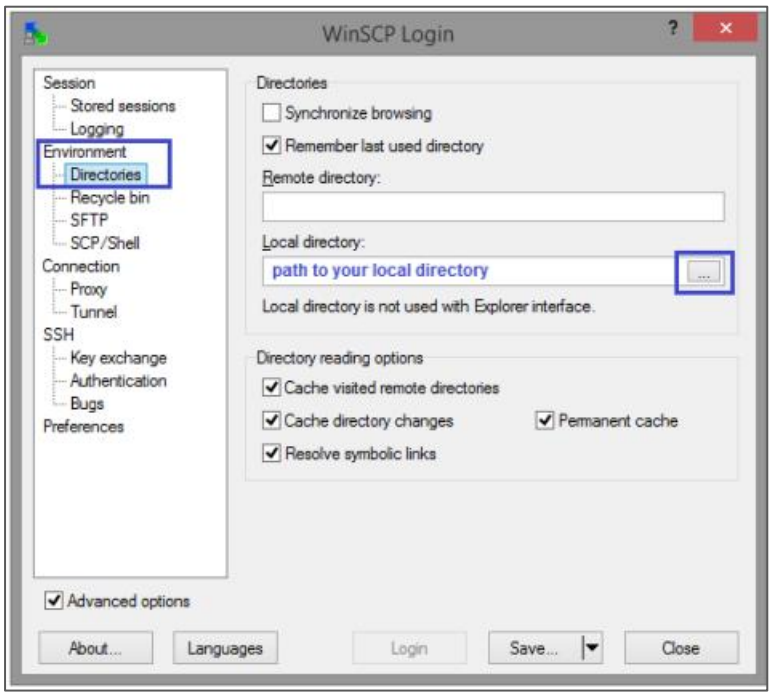


Figure 16 - Set the path to the local repository

Step 4: Press "**Login**" to connect

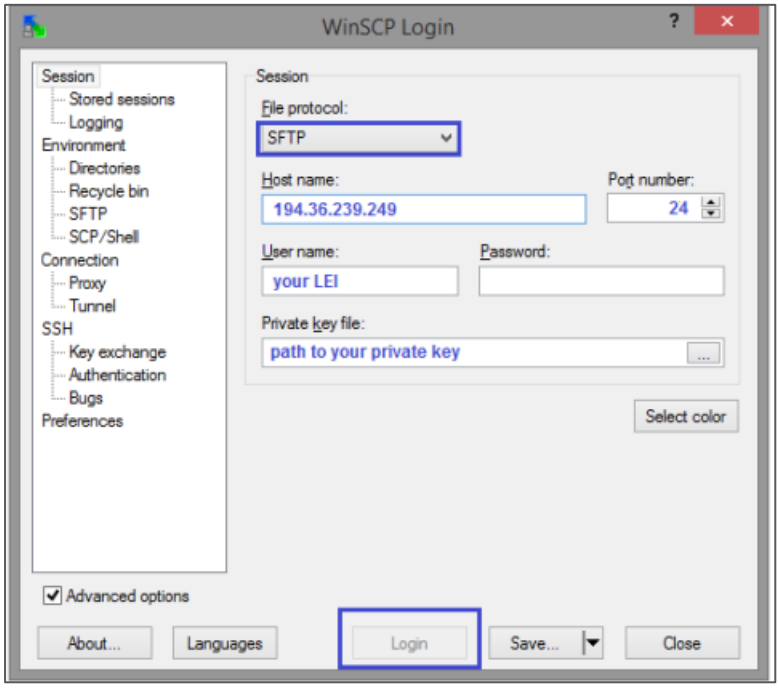


Figure 17 - Pressing "Login" to connect

Step 5: After clicking on "**Login**" a dialog screen will appear showing the personal data and will request to enter the corresponding "**Key passphrase**" set for the private key (if the private key has been protected):

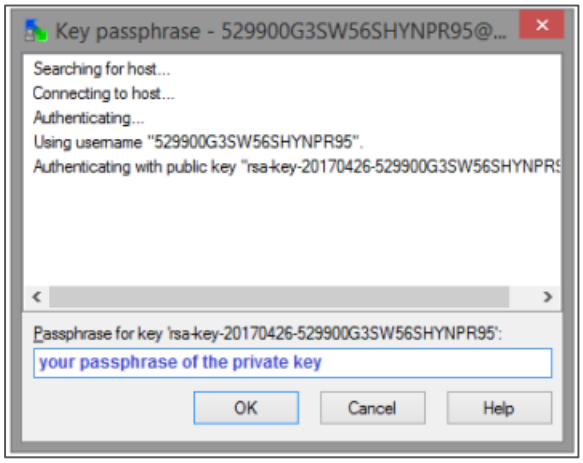


Figure 18 - Enter a passphrase

Step 6: If the connection was successful, users will see the content of the default remote directory as shown here

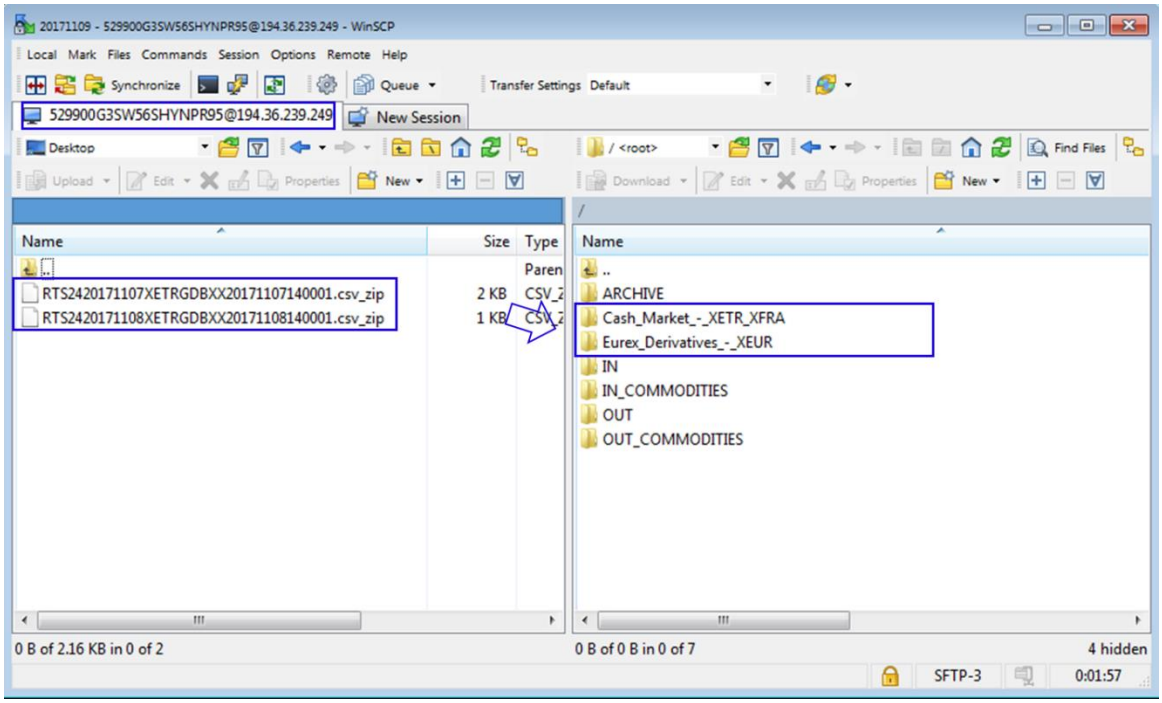


Figure 19 - Successful login via WinSCP

4.2.3 How and where to upload files

After connecting to the server users can upload files (for details about file requirements refer to Section 5) using Drag & Drop function. This works as follows:

- First select the local file to be transmitted from the local directory
- Then drag selected file and drop it into the remote target folder for the respective market

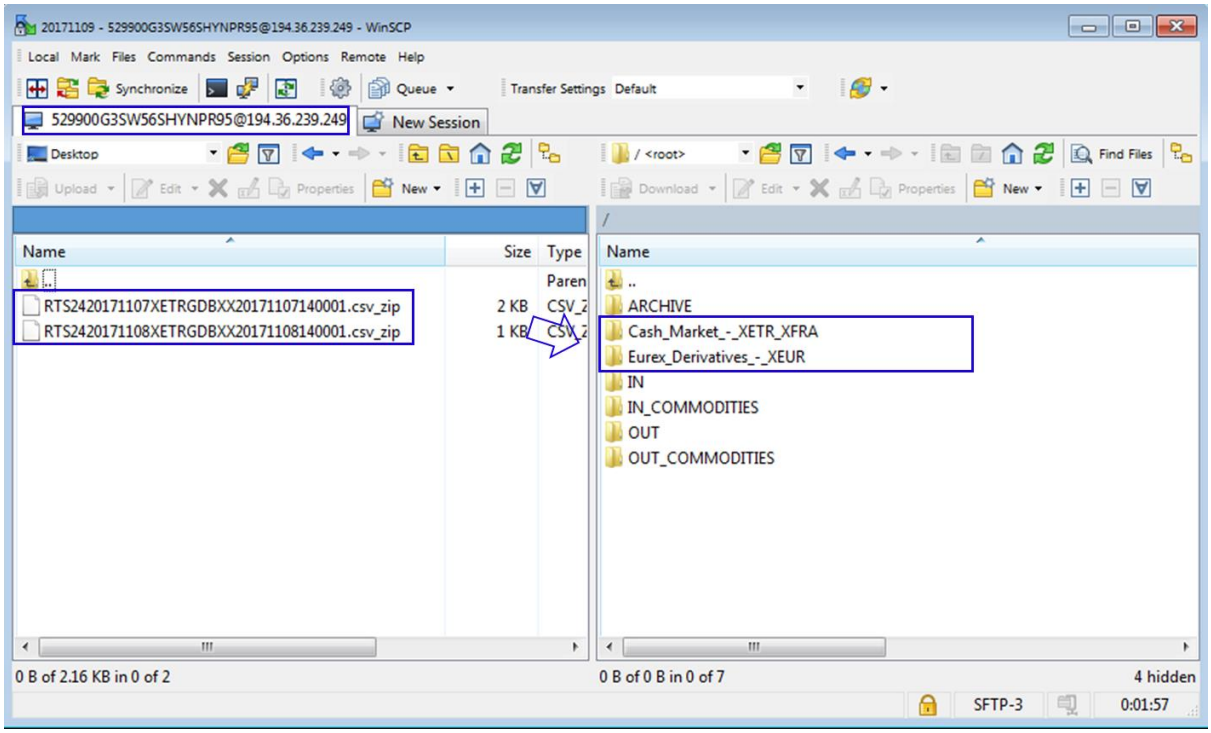


Figure 250 - Drag & drop the files into the folder within WinSCP

If the files have been processed successfully, the trading participant receives a short message confirming that the data has been successfully transmitted. If not, the member receives an error message.

5. File submission guidelines

Before starting to upload any files to the server the submitters/users are kindly asked to consider some requirements regarding the file naming and formats. The purpose of these requirements is to

- provide guidance to users in the preparation of inbound files and
- ensure that uploaded files meet the technical specifications. Any file not meeting these specifications will be rejected and not processed - requiring corrective action.

5.1. General requirements

The following preconditions need to be satisfied before any upload:

The naming must follow the chronological sequence: Reporting reason (service identifier), Date (valid for), Market Identifier Code (MIC), MemberID, timestamp, data format incl. zip. Please find the examples including coloured file naming blocks below:

- Short-/ long code: RTS2420171011XEURGDBXX20171012103159.csv_zip.
- Algo certificates: ALGO20171011XEURGDBXX20171012103159.csv_zip.

On the SFTP platform we do enforce the following checks:

- Main “format”: (RTS24|ALGO)([0-9]+)([A-Z]{9})([0-9]+).(csv|csv_zip).

- Reporting reason (service identifier), should begin with either RTS24 or ALGO.
- Check Date format.
- Market Identifier Code (MIC), MemberID check is basically a charset check (A-Z characters in uppercase), combination of both should be 9 characters long.
- Check Timestamp format.
- Data format should be either csv_zip or csv.

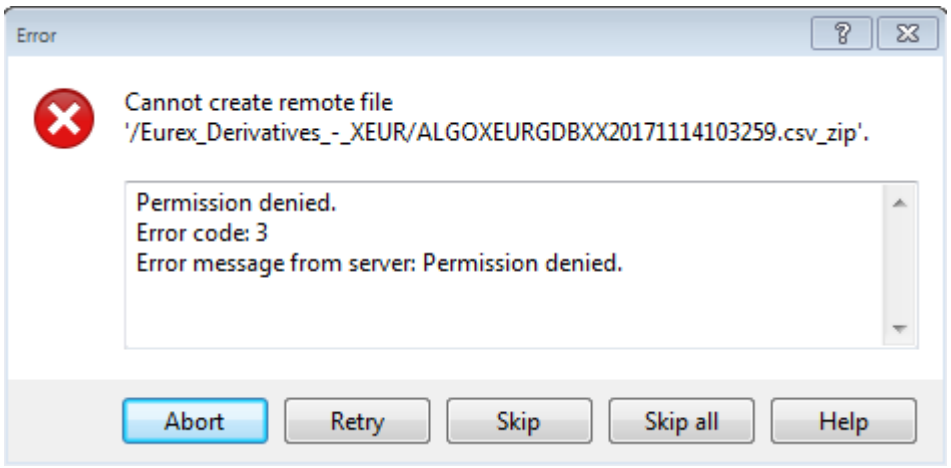
RTS 24/ ALGO file naming rule set:

Attributes	Attribute levels
Reporting reason (service identifier)	RTS24; ALGO
Date (valid for)	YYYYMMDD
Market Identifier Code (MIC)	4 characters (alphabetic) ("XEUR" for Eurex; "XETR" for Xetra, "XFRA" for Frankfurter Wertpapierbörse)
MemberID	5 characters (alphabetic)
Timestamp	YYYYMMDDhhmmss
Data format incl. zip indicator	.csv_zip; .csv

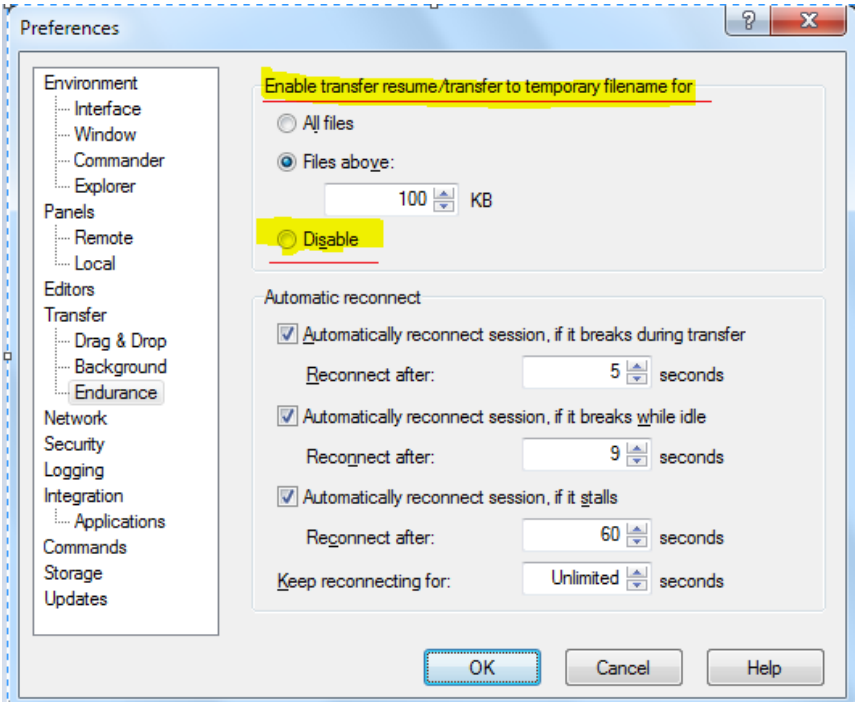
Only files delivered by 11:50 PM can be considered for data mapping for the business day T. The mapping will be done during the End of Day (EoD) process. The results will be published on T+1 in the respective reports available via the Common Report Engine.

5.2. Error Message

In case a submitted file does not match with the file naming rules described in section 5.1. the following error message will appear:



If you use WinSCP and your files are greater than 100KB, please disable the "temporary filename" option otherwise you will receive an error message.



6. Known Limitations & Best Practice

i) For the time being, no validation of the file content takes place, only for the file names as described in the section 5 (implementation of validation rules in progress).

ii) All submitted files that do not match the data format as described above (.csv_zip) will be deleted.

iii) Please be aware that should you decide to use both upload methods (SFTP and the Webservice) on the same day (not recommended) that a sequencing of the files, by you, will be required.

7. Support Contacts

For technical queries related to the SFTP certificate creation and upload please contact your Technical Key Account Manager via your VIP number or send an email to: cts@deutsche-boerse.com.

For queries related to reference data for MiFIDII or the Legal Entity Identifier (LEI), please contact your Key Account Manager or send an email to: customer.readiness@deutsche-boerse.com.