part of eex group

ECC File Transfer Service

User-Guide

07.01.2025
Leipzig

Rel. 012

Table of Contents

1 GENERAL

ECC's File Transfer Service offers exchanges, clearing members and trading participants a secure access to data and reporting provided by ECC.

Access to the FTP server is provided on user level and is administrated by ECC. The username and password are identical with the access data for the ECC member area. These can be applied for from ECC using the form T10 for private data as well as the T10p for public data (ECCPUBLIC) which can be downloaded from www.ecc.de. Access to the FTP server can be established via

- SFTP (Privat-Public-Keypair or user/password)

To generate a directory on the FTP server the respective participant must subscribe reports via channel 'FTP' in the first step. Reports can be subscribed to within the ECC Member Area under the menu item Report Subscription (please refer for a more detailed description to the ECC member area User). After ECC generates a report via this channel for the first time, the directory for the respective company is created automatically. After that the appropriate users will be able to log on to the FTP server with their personal access data.

Trading participants could receive the following subdirectories:

\REPORTS\
\YYYY
\MM
\DD
\MISC

Additionally, clearing members will have these folders available

\CASCADING_FILE
\DEPOSIT RATE
\LIMITS

For the ECCPUBLIC FTP the following directories are available

\SPANFILES
\RISKPARAMETER
\PRODUCT_INFORMATION
\CONTRACTDETAIL
\OTCPRICERANGE
\CASCADINGFILES

The daily as well as the monthly reporting is saved immediately under the respective directive of the issue day upon their generation by ECC.

2 FILE TRANSFER SERVICE VIA SFTP

The SSH File Transfer Protocol (short: SFTP) is a possibility to transfer data via a secure and encrypted connection.

Access via SFTP is possible with user/password as well as with user/private&public-key pair. The keypair has to be generated by the participant; the public key must be provided to ECC and will be configured on our SFTP-server.

To access the ECC reporting via SFTP, a corresponding client is needed. For a Windows client system you can use e.g. “WinSCP” (https://winscp.net/eng/download.php) or “Filezilla” (https://filezilla-project.org/download.php?type=client); for a UNIX system e.g “scp” or “sftp” can be used. To respect your company compliance and regulations or you are not familiar with this, get in touch with your IT department to get and install a SFTP client tooling.

2.1 Technical Details

Server address:

production: ftps.ecc.de

simulation: ftpssimu.ecc.de

Protocol: SFTP (SSH-extension)

Port: 22

Accepted key-types & length:

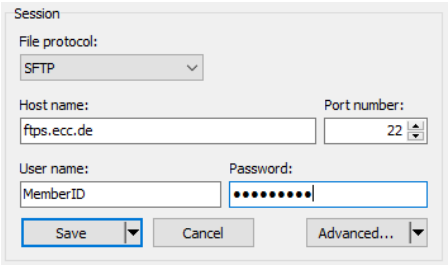
RSA with minimum 4096-bit

ECDSA with minimum 384-bit

2.2 Authentication with user & password

With the Member-Id that you received from our Member Readiness Team you will be able to login to our SFTP service in addition to the MemberArea GUI. The password for authentication is also the same as you use for the MemberArea.

An example configuration with WinSCP:

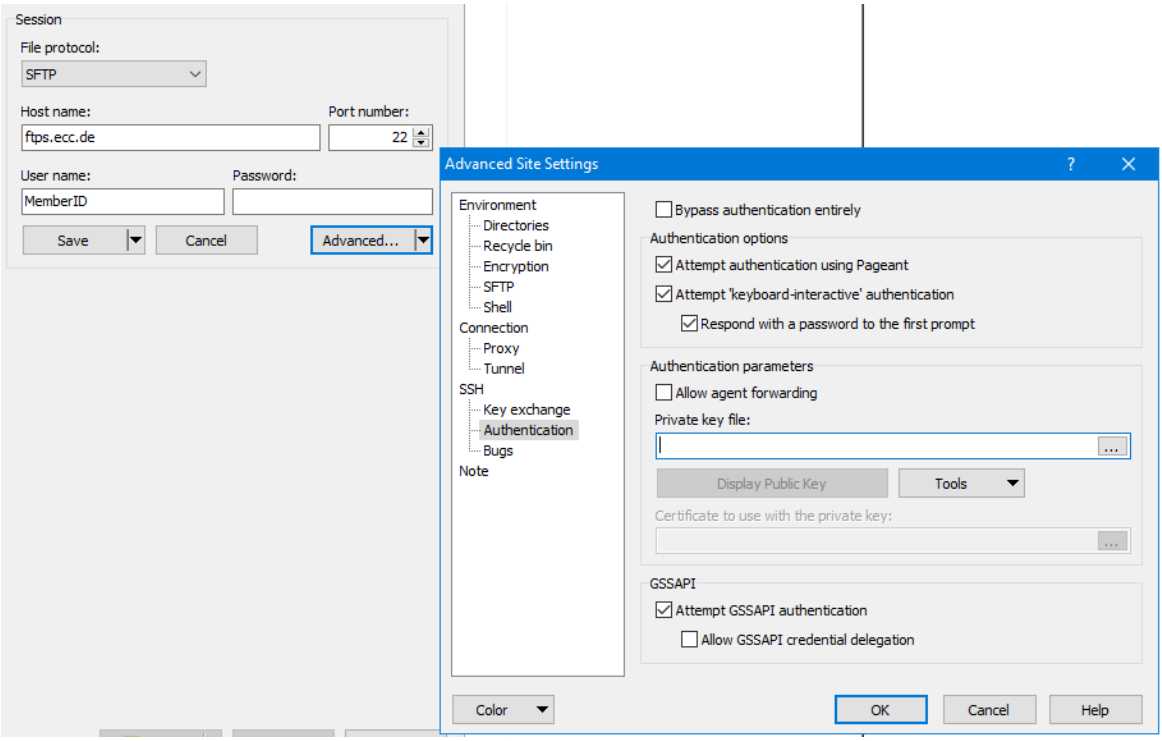


Other tools can of course also used and should have similar configuration possibilities.

2.3 Authentication with user & key pair

With the Member-Id that you received from our Member Readiness Team you will be able to login to our SFTP service in addition to the MemberArea GUI. For authentication you need to generate a keypair instead of using a password.

An example configuration with WinSCP:

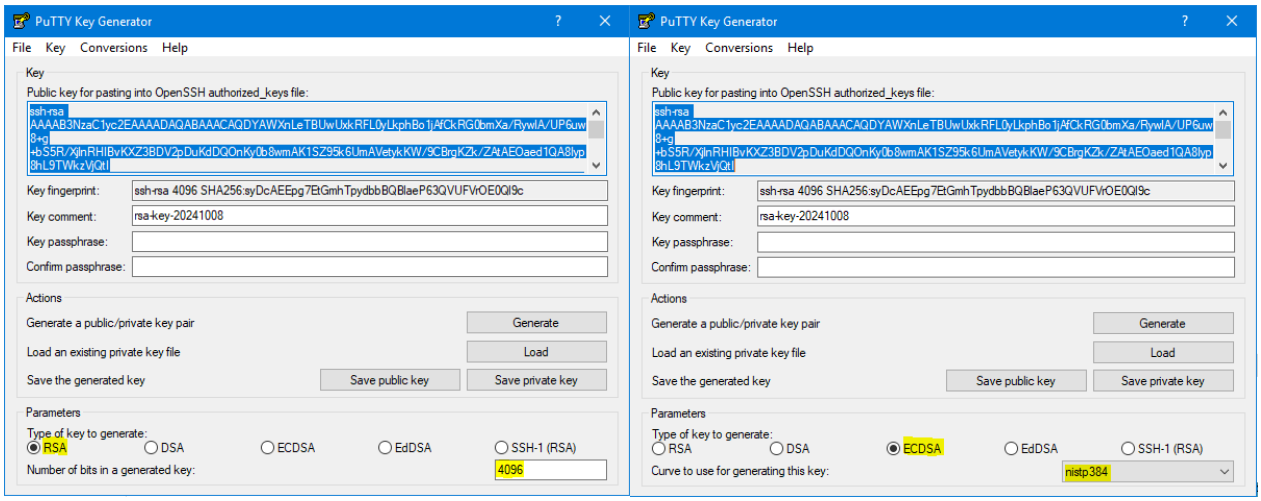


Other tools can of course also used and should have similar configuration possibilities.

2.3.1 Example for Generating a key pair with Windows

To create a key pair with windows as client software you can use for example the program ‚PuTTYgen' of the PuTTY package. It generates pairs of public and private keys.

- Select the 'Type of keys to generate' and key length aligned with our and your security requirements
- click '*Generate*', to generate a new public/private key pair
- choice a '*Key comment*' and '*Key passphrase*' align with our own requirements
- copy the public key by copying it out of the `*Public key for pasting into authorised keys file*' box and send it via e-mail to ECC.
- The `*Key fingerprint*' box shows you a fingerprint value for the generated key. This needs to be checked with ECC by a different communication channel.
- `*Save private key*` output to a secure place on our side and provide it to our client program or IT department for further usage



2.3.2 Generating a key pair with UNIX

It is possible to generate a key pair as described above not only with Windows, but also with UNIX. Please find a short description about that below.

```
ssh-keygen -t ecdsa -b 384 -f <FILE>
Generating public/private ecdsa key pair.
Enter passphrase (empty for no passphrase): ***
Enter same passphrase again: ***
Your identification has been saved in <FILE>.
Your public key has been saved in <FILE>.pub.
The key fingerprint is:
SHA256:oZVyQuwFLJ9RN4zwzzI21NfW+VE90eZCqImSrPih
SuI
The key's randomart image is:
+---[ECDSA 384]---+
|     o++.oo  . .=|
|    ..+.o+.....o*|
|     =o=B..o..o=o|
|      BB.+o. .. +|
|   . ...S o    ..|
|  . o  . +       |
|.. o .           |
|+ . .            |
|.E               |
+----[SHA256]-----+
```

```
ssh-keygen -t rsa -b 4096 -f <FILE>
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase): ***
Enter same passphrase again: ***
Your identification has been saved in <FILE>.
Your public key has been saved in <FILE>.pub.
The key fingerprint is:
SHA256:MLWd5lfBy4h2+Zvs0bzSiolK/qil1wCSE2wQD/7D
8/0
The key's randomart image is:
+---[RSA 4096]----+
| ++     .    ..  |
|. o+   . o .  .. |
| ...o o . +. +.. |
|  o+ . o oo +.o  |
|   =o . S.....   |
|    + ..   .  .o |
|     . +o    .ooo|
|      =.o.. o.+o.|
|     oo+oE o o+. |
+----[SHA256]-----+
```

The private and public key are stored in the given filenames. You need to be ensured that the private key are stored on a secure location and not accessible from unauthorized persons. Only the public file must be send via e-mail to ECC, furthermore tell us the key fingerprint of the public key by a different communication channel. You can recover the fingerprint via

```
ssh-keygen -l -f <FILE>.pub
```

As the ECC needs the public key in ssh2-format, you can already transform it using ssh-keygen. For this you use the generated private key myfile and send us the file myfile_rfc4716.pub

```
ssh-keygen -e -m RFC4716 -f <FILE>.pub><FILE>_rfc4716.pub
```

2.4 Firewall

Please ensure that your firewall allows contacting our FTP-server:

Protocol	IP	Ports
SFTP	ftps.ecc.de	22 or 2222

3 CONTACT DETAILS

As your contacts for setting up access data and establishing ECC's File Transfer Service the team of Clearing & Settlement is on your disposal under the well-known hotline or e-mail address (if needed specialists from the IT departments of the involved companies will be called in).
The public key should be sent via e-mail to ECC, the check of the ‚key fingerprint' should be carried out by phone or via fax with an immediate confirmation by telephone.

European Commodity Clearing AG
Clearing & Settlement

Hotline: +49 341 24680 444

Fax: +49 341 24680 409

E-Mail: clearing@ecc.de