

Common Upload Engine

User Guide

© 2021 by Deutsche Börse AG (“DBAG”). All rights reserved.

All intellectual property, proprietary and other rights and interests in this publication and the subject matter of this publication are owned by DBAG, other entities of Deutsche Börse Group or used under license from their respective owner. This includes, but is not limited to, registered designs and copyrights as well as trademark and service mark rights. Methods and devices described in this publication may be subject to patents or patent applications by entities of Deutsche Börse Group.

Specifically, the following trademarks and service marks are owned by entities of Deutsche Börse Group: Buxl[®], DAX[®], DivDAX[®], eb.rexx[®], Eurex[®], Eurex Repo[®], Eurex Strategy WizardSM, Euro GC Pooling[®], F7[®], FDAX[®], FWB[®], GC Pooling[®], GCPI[®], M7[®], MDAX[®], N7[®], ODAX[®], SDAX[®], T7[®], TecDAX[®], USD GC Pooling[®], VDAX[®], VDAX-NEW[®] and Xetra[®].

The following trademarks and service marks are used under license and are property of their respective owners:

- All MSCI indexes are service marks and the exclusive property of MSCI Barra.
- ATX[®], ATX[®] five, CECE[®] and RDX[®] are registered trademarks of Vienna Stock Exchange AG.
- IPD[®] UK Annual All Property Index is a registered trademark of Investment Property Databank Ltd. IPD and has been licensed for the use by Eurex for derivatives.
- SLI[®], SMI[®] and SMIM[®] are registered trademarks of SIX Swiss Exchange AG.
- The STOXX[®] indexes, the data included therein and the trademarks used in the index names are the intellectual property of STOXX Limited and/or its licensors. Eurex derivatives based on the STOXX[®] indexes are in no way sponsored, endorsed, sold or promoted by STOXX and its licensors and neither STOXX nor its licensors shall have any liability with respect thereto.
- Bloomberg Commodity IndexSM and any related sub-indexes are service marks of Bloomberg L.P.
- PCS[®] and Property Claim Services[®] are registered trademarks of ISO Services, Inc.
- Korea Exchange, KRX, KOSPI and KOSPI 200 are registered trademarks of Korea Exchange Inc.
- BSE and SENSEX are trademarks/service marks of Bombay Stock Exchange (“BSE”) and all rights accruing from the same, statutory or otherwise, wholly vest with BSE. Any violation of the above would constitute an offence under the law of India and international treaties governing the same.

Information contained in this publication may be erroneous and/or untimely. All descriptions, examples and calculations contained in this publication are for illustrative purposes only, and may be changed without further notice. Neither DBAG nor any entity of Deutsche Börse Group makes any express or implied representations or warranties regarding the information contained herein. This includes without limitation any implied warranty of the information’s merchantability or fitness for any particular purpose and any warranty with respect to the accuracy, correctness, quality, completeness or timeliness of the information. Neither DBAG nor any entity of Deutsche Börse Group shall be responsible or liable for any third party’s use of any information contained in this publication under any circumstances. The information contained in this publication is not offered as and does not constitute investment advice, legal or tax advice, an offer or solicitation to sell or purchase any type of financial instrument.

List of Abbreviations

CUE	Common Upload Engine
DBAG	Deutsche Börse AG
DSA	Digital Signature Algorithm
ECAG	Eurex Clearing AG
PuTTYgen	Putty Key Generator
RC	Registered Customer
RSA	Rivest, Shamir and Adleman (public-key cryptosystem)
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
VPN	Virtual Private Network

Table of Contents

1 General information 4

1.1 Intended audience 4

1.2 SSH File Transfer Protocol 4

2 Overview 5

2.1 Features and functionality 5

2.2 Security, Autorisation and Access 5

2.3 Hardware requirements 6

2.4 Software requirements 6

3 Setup process 7

3.1 How to generate and save SSH key pair 7

3.2 Example for key generation using PuTTYgen (Microsoft Windows) 7

3.3 CUE user administration 10

4 Connecting to the CUE 14

4.1 Microsoft Windows example using WinSCP 14

4.2 Uploading files 16

5 Report and file naming conventions 17

6 Appendix - Server Host Key for the CUE 18

6.1 Server Host Key DBAG CUE for Leased Line 18

7 Change Log 19

1 General information

The Common Upload Engine (CUE) allows admitted participants of the DBAG Group the upload of participant data to dedicated services provided by DBAG Group.

Participants are able to automate the upload of data files to the CUE via secure transfer protocol (SFTP). The participant has to provide the public part of a SSH key pair via the DBAG Member Section in order to participate. The public key is provided to the CUE infrastructure after the key upload and validation. Depending on the used service participant have to connect to the service in a given time window and upload files in a predefined format.

Participants are able to use their preferred hardware platform and operating system.

Communication with the CUE is based on OpenSSH. The OpenSSH server authenticates users using the standard methods supported by the SSH protocol (<https://www.openssh.com/specs.html>).

1.1 Intended audience

This document is intended for system developers, system and security administrators maintaining their systems to interact with the CUE service offered by DBAG. It is assumed that the reader is familiar with OpenSSH public/private key pair authentication methods (i.e. handling of public/private key pair) and the use of SFTP clients and/or scripts.

The purpose of this document is to provide an overview on how to obtain access to the CUE, how to deposit keys in the DBAG Member Section (User Administration) is documented separately.

1.2 SSH File Transfer Protocol

To avoid misunderstandings, "SFTP" stands for the SSH File Transfer Protocol as defined here: <https://www.sftp.net/>

2 Overview

2.1 Features and functionality

- Files can be uploaded to the admitted service environments (such as simulation & production).
- All uploads will be virus checked.
- All uploads will have a functional plausibility check, e.g if the naming convention is correct or whether the file is corrupt.
- Participants will receive an initial response if the uploaded file fulfils the initial upload requirements.
- Afterwards the CUE will perform the transmission to the admitted service automatically.

2.2 Security, Autorisation and Access

In general, the setup process for the participant involves the following three steps:

1. *Generating an OpenSSH compliant public/private key pair*
2. *Creating a CUE user and uploading the public key in the DBAG Member Section*
3. *Logging into the CUE and upload data files via SFTP client*

To provide a secure service, the OpenSSH authentication method is used. This method requires an OpenSSH compliant public/private key pair, which the participant must generate. This process ensures that the participants authenticates themselves against the CUE. The public key must be generated and uploaded to the DBAG Member Section, while the participant will keep the private key. By using a key-based authentication method, no login passwords have to be transferred at any time.

- Participants need to generate a public/private key pair.
- It is recommended to limit access to the CUE using dedicated IP addresses.
- Security of data will be ensured by the usage of SSH2.

The illustration below provides an overview on how to access the CUE and how to set up the access process in order to download all necessary files.

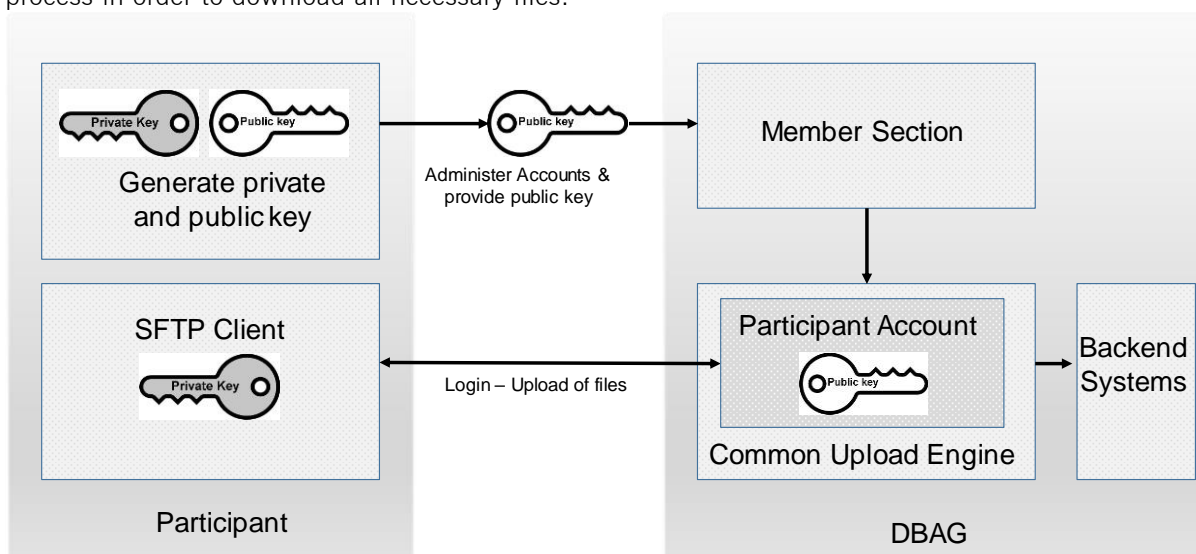


Fig. 1: Process overview to connect to the CUE

Note: The figure above provides a simplified functional overview.

- The public key will be provided to the CUE via the Member Section.
- The private key always remains by the participant.
- The user needs the private key when initiating a connection attempt.
- It is recommended to create a public/private key pair for every user connecting to the CUE.
- The private key has to be stored secure; it is in responsibility of the participant to ensure the security of the key.

2.3 Hardware requirements

There are no particular hardware requirements to access the CUE servers. The CUE server can be accessed from any computer running the SFTP client program.

2.4 Software requirements

To transfer files to the CUE a SFTP client compliant with a current SSH2 version is required.

- OpenSSH provides a large suite of secure tunnelling capabilities, several authentication methods, and sophisticated configuration options.
- DBAG has disabled all known insecure Ciphers, Key Exchange Algorithms and MAC Algorithms for the SSH server.

Known secure parameters for each method are listed below:

Key Exchange Algorithms:

- ✓ curve25519-sha256
- ✓ curve25519-sha256@libssh.org
- ✓ diffie-hellman-group18-sha512
- ✓ diffie-hellman-group14-sha256
- ✓ diffie-hellman-group16-sha512
- ✓ diffie-hellman-group-exchange-sha256
- ✓ ecdh-sha2-nistp256
- ✓ ecdh-sha2-nistp384
- ✓ ecdh-sha2-nistp521

Ciphers (encryption Algorithms):

- ✓ chacha20-poly1305@openssh.com
- ✓ aes256-gcm@openssh.com
- ✓ aes128-gcm@openssh.com
- ✓ aes256-ctr
- ✓ aes192-ctr
- ✓ aes128-ctr

MAC Algorithms:

- ✓ hmac-sha2-512-etm@openssh.com
- ✓ hmac-sha2-256-etm@openssh.com
- ✓ umac-128-etm@openssh.com
- ✓ hmac-sha2-512
- ✓ hmac-sha2-256

3 Setup process

3.1 How to generate and save SSH key pair

As mentioned in chapter 2, public/private keys are used for authentication by the CUE infrastructure. The participant must generate the pair of keys. Please note that we recommend separate SSH key pairs for Simulation and Production for security reasons.

- It is required to use a minimum of 2048 bits for the generated key. The key type must be SSH2 RSA or DSA (RSA is faster in authentication). Once the parameters above are set the key can be generated.
- The key generation process will produce public and private keys. See details about key handling and usage in sections below.
- Save the public key files and private key files for future use.
- In no case should the **private key** be transferred over an insecure network, e.g. via e-mail, and it should always be kept only by the participant.
- It is highly recommended to protect the key file with a passphrase. This will encrypt the private key when it is saved in a secure location on the local machine. Using passphrases for batch SSH-keys requires familiarity with the SSH-agent authentication subsystem. Participants should be aware that the use of strong encryption methods and encrypted SSH-keys is advisable but will raise administration efforts and system complexity.
- To generate an SSH public/private key various freeware tools are available for download from the Internet, such as PuTTY or OpenSSH.

3.2 Example for key generation using PuTTYgen (Microsoft Windows)

See the following example of key pair generation.

- Make sure to have the latest stable version of PuTTYgen.
- Set key parameters type and bit number as shown below.
- Follow the instructions on the screen and move the mouse over the blank area for a while.

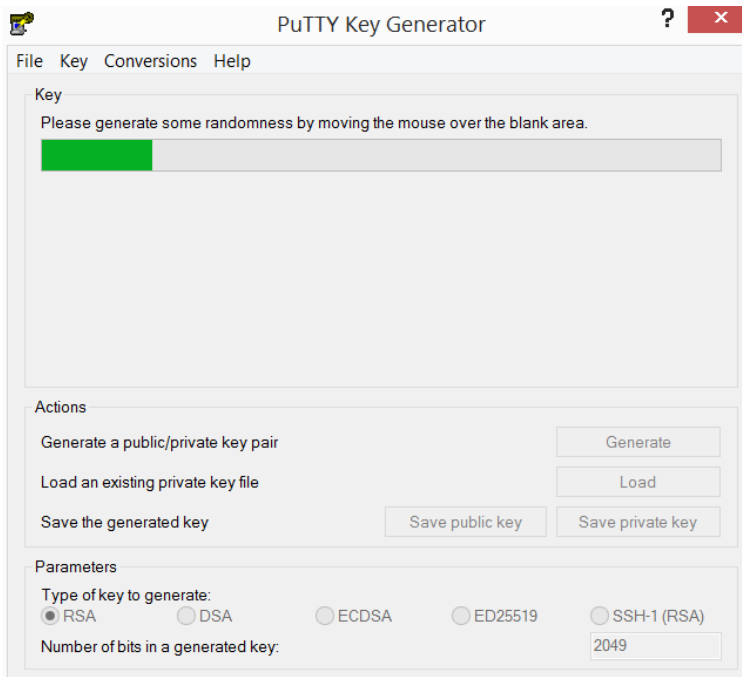


Fig. 2: Generate key (screenshot of PuTTYgen)

- Please note: When using Putty in some rare cases, one key bit can get lost, therefore it is recommended to generate and upload a key with 2049 bits or more.
- The private key must be accessible for the participant’s SFTP client in order to login successfully. By clicking the buttons highlighted in Figure 3, participants can save their private and public keys in the PuTTY format for further use with the PuTTY tools or WinSCP.

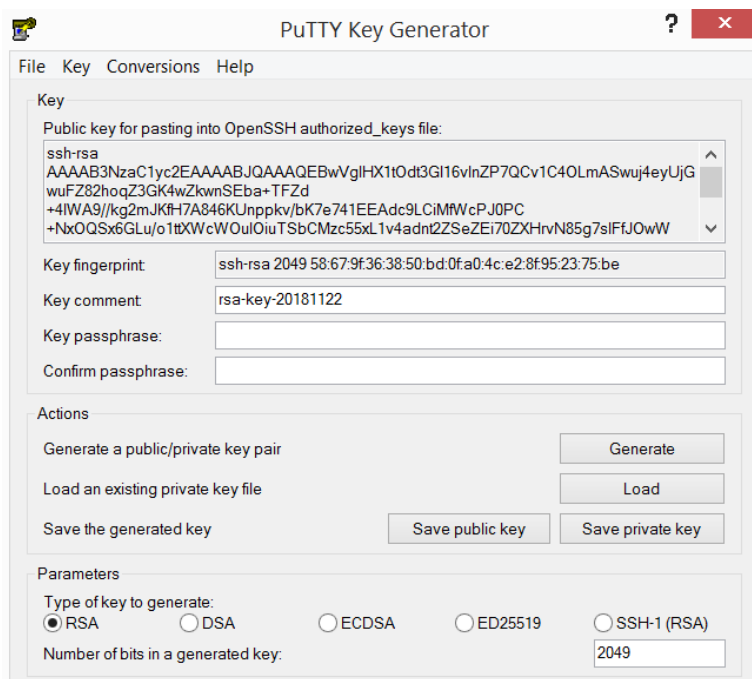


Fig. 3: Saving the generated public and private keys in the PuTTY format (screenshot from tool PuTTYgen)

The OpenSSH private key can also be exported in the OpenSSH format for use with other software working with OpenSSH keys (such as Unix SFTP).

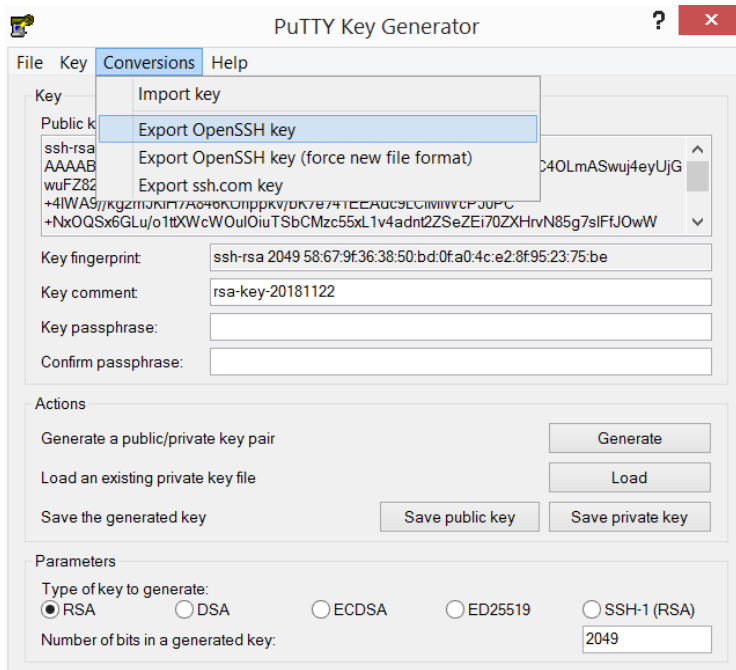


Fig. 4: Saving the OpenSSH private key for future use (screenshot from tool PuTTYgen)

- The public key **must** be saved in OpenSSH format to be uploaded to DBAG Member Section..
- Copy the marked text from PuTTYgen to a text editor, such as notepad and save it with the extension .pub.
- Make sure that this line has no “End Of Line” character (EOL) at the end!

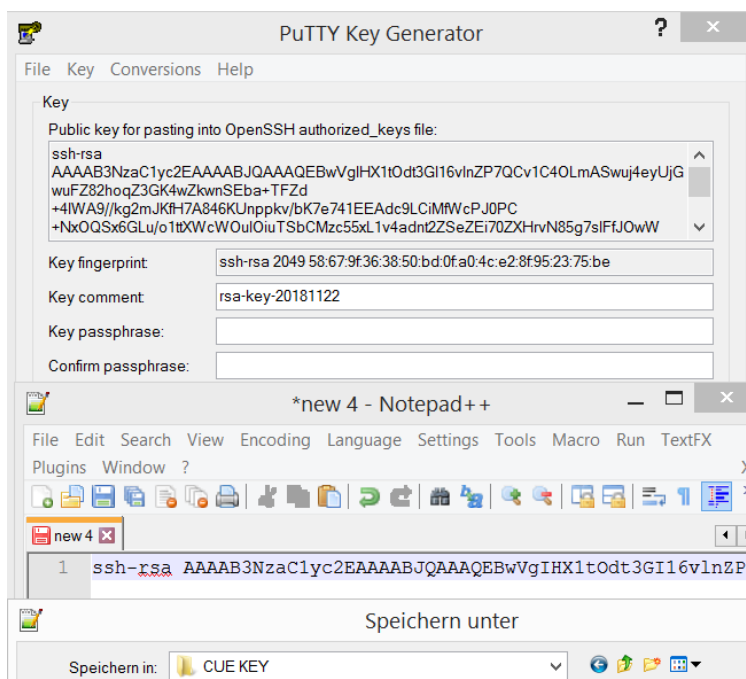


Fig. 5: Saving the public key for DBAG Member Section upload (screenshot from tool PuTTYgen and Notepad++)

- Public keys must consist of one line only. Only public OpenSSH keys in this format can be used with the CUE and can be successfully uploaded in the DBAG Member Section.
- After uploading, the participant must wait for the configuration data (users, keys, markets, etc.) to be transferred to the CUE database. Usually this processing takes place in the late evenings.
- In general, the access to the CUE will be ready after 2 business days. (After the first business day you have access and see empty folders, after the second business day upload of reports and files is possible.)
- Changes to existing users will take effect on the next day.

Please note that the public key does NOT have to be signed by a certification authority of the participant for the use with the CUE

3.3 CUE user administration

Before the CUE can be accessed, a CUE user account has to be set up and the OpenSSH public key has to be uploaded in the DBAG Member Section. This task can be performed by the “Technical User Administrator”.

“DBAG Member Section” <https://member.deutsche-boerse.com> -> “Technical Connection”-> “/Requests & Configuration ”-> “Self Service Certificates ” ->”Upload Engine User”

Administration rights to become a “Technical User Administrator” may be requested using the DBAG Member Section.

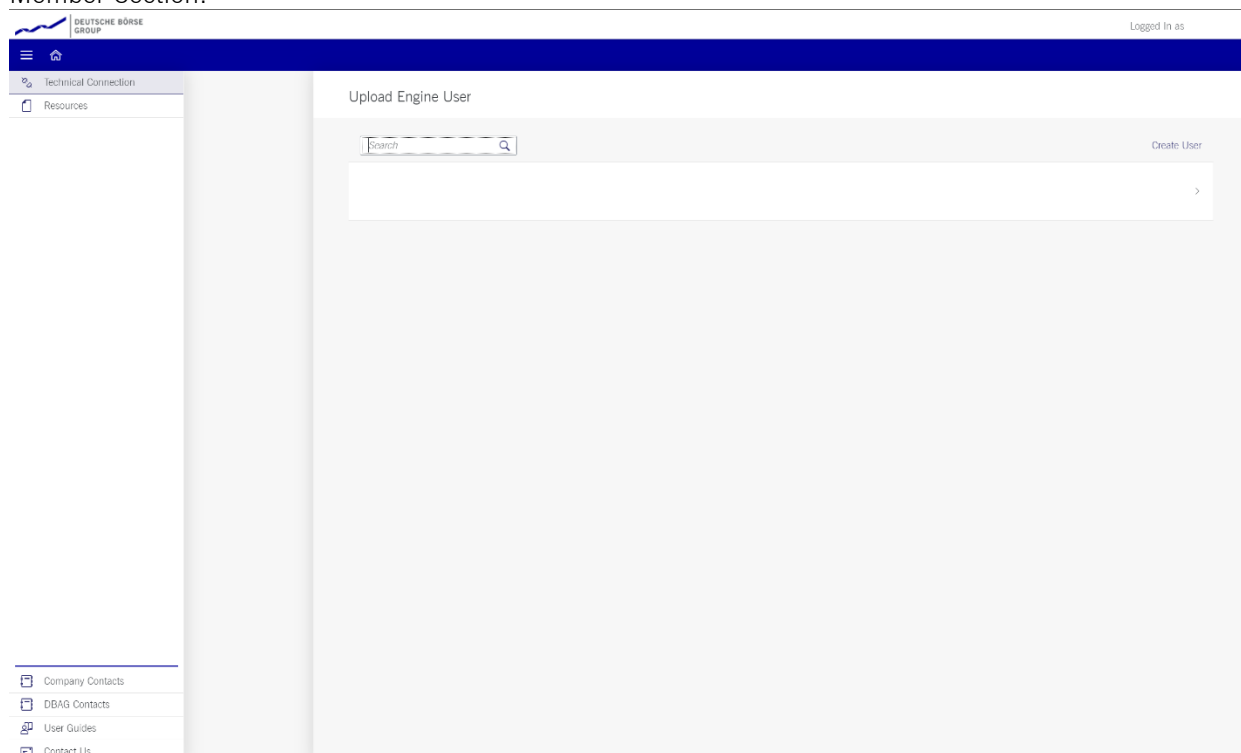


Fig.6: CUE users must be maintained in the DBAG Member Section

An overview of all existing and already created CUE users will be displayed. It is possible to edit, modify or delete existing CUE users by simply selecting them from the list.

All CUE users can be identified by their UserID, which is generated during the account setup process. A UserID looks like this example: 1027709_000002

- The first part, 1027709 is the so-called DBAG business partner ID which is used in the DBAG Member Section for identification of a participant of Deutsche Börse AG. A business partner may have different memberships on Eurex and Xetra; each membership is represented by a Member ID.
- The second part, 0000002 is a sequential number, automatically assigned by the system.

In addition, new CUE users can be created in the DBAG Member Section:

The new input screen will be opened by clicking on “Create User” where all necessary user information needs to be entered.

Fig. 7: Input screen in the DBAG Member Section to create a new CUE user

- **User Information (Optional):**
In the field “Description” a short description of the user should be given. Please note that the description is not the UserID. Any description of the user may be entered here.
The UserID field itself will be filled by the system automatically.
- **Engine Configuration:**
“Engine configuration” needs to be clicked to enter the “MemberID”, a “Market” and an “Environment”. A selection of all applicable combinations for this specific user will be displayed from which he can choose.
- **Network Data (Optional):**
Access for a user can be restricted to a single or multiple IP-addresses or an IP-range. An additional IP address will be added by clicking on “Add Row”. This is optional, but highly recommended by DBAG. Select an IP address and click on “Remove Row” to remove it.
The address pattern entered here will be included in the configuration file for this user account. A wildcard (*) can be used in the pattern to represent zero or more characters. In order to combine multiple patterns, a pattern list can be used; each pattern must be on a new line. To prevent mistakes a logical check of the IP address is provided.
- **Certificates:**
The certificate refers to the public key created as described in chapter 3.1. The certificate/public key is

only used to authenticate a user/role. The user/role permissions (i.e. access to member/market/etc.) are assigned at a later stage in the setup process (please refer to step 2 in this chapter).


It is recommended to create a private/public key pair for every CUE user that may connect to the CUE.

A public key needs to be uploaded by clicking on "Add Certificate". Next a popup window will appear where the OpenSSH public key has to be uploaded. Browse to the location of the key and click "Upload".

Add Certificate

Upload CertificateGenerate Certificate

Certificate Data: `ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCHly5fq8Znl79I/dG
MgQlmfAbsJv05Z2fCWGOkbmRz0i+7vg9p+aAYSQ91pHgqI
OegjW10UyZptkYShctz581mij9s8h+I9O9103PDQ8X5Z08+
pbkcPTFgGogGykuUVDyE2/fd9Y4LX++JBWToZ5lZNLAcUd`

Valid From: 02.08.2021 

Always valid:

Comment:

Add Cancel

Fig.8: Popup screen to upload the public key

A validity period of 90 days is used by default. The certificate/public key is added by clicking "Add".

Key expiration:

CUE users will be notified by email in due time about upcoming expiration. Latest one day before a certificate/public key will expire, the existing key needs to be prolonged (upload the existing key once more and define a new expiration date) or a new private/public key pair must be generated and the newly generated public key needs to be uploaded.

- The final step is to save the changes: Click on "Save" to automatically create the User ID.

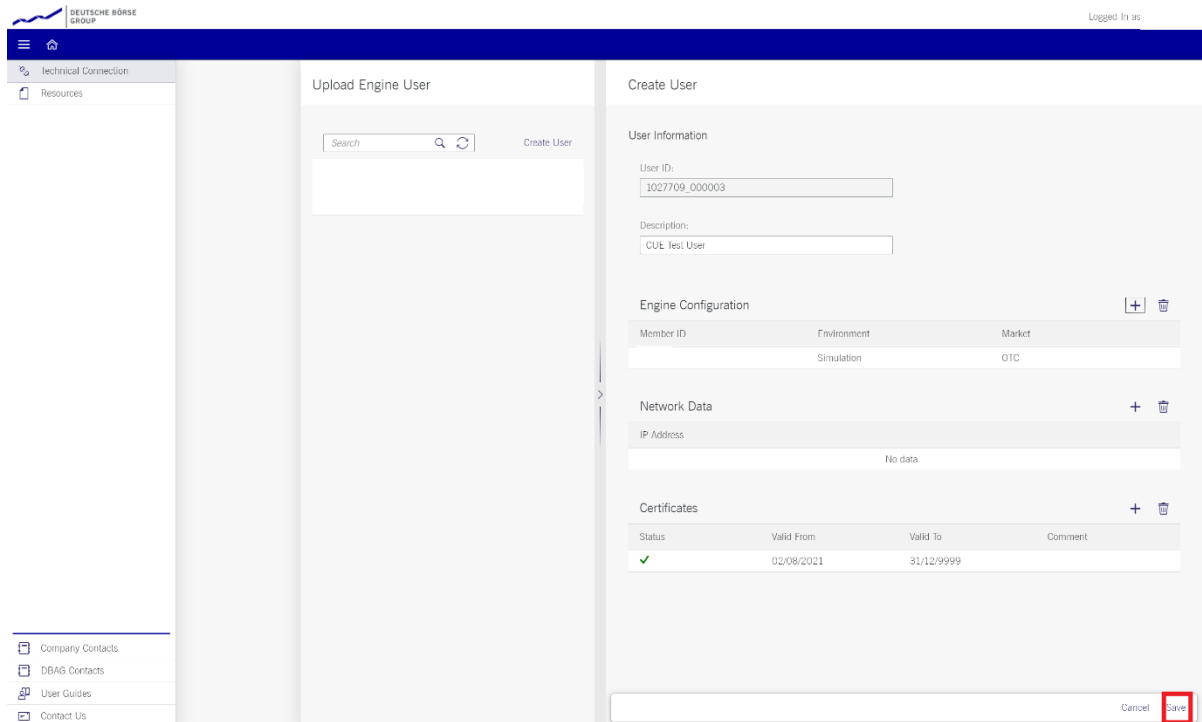


Fig.9: Exemplary CUE user information after the successful creation of a CUE user

The generated UserID is displayed in Common Upload Engine User Overview table, as well as in the field UserID when selecting a user in the table on the main screen.

All Central Coordinators and their deputies are informed via e-mail whenever a new CUE user has been successfully setup, modified or deleted.

When initially creating a CUE user, the information will be available after two business days. All subsequent changes to a CUE user become active after the next business day.

4 Connecting to the CUE

Participants may use an SFTP client of their choice to access the CUE server and upload their files. The following information is required to log into the CUE:

- User ID which has been generated by successfully setting up a new user in the DBAG Member Section.
- The IP address (host name) of DBAG/CUE.
- The private SSH key fitting to the public key uploaded in the DBAG Member Section.
- The IP's used for access to the CUE are shown in the table below.

The CUE is divided into areas.

Area A gives upload access to files of the following service:

- LSOC

Common Upload Engine			
Leased line		Internet	Port
A	B		
193.29.90.70	193.29.90.102	t.b.a.	2251

Area B gives upload access to files of the following service:

- Regulatory Reporting Eurex and FWB (non-MIFIR reporting, short code and algoID upload)

Common Upload Engine			
Leased line		Internet	Port
A	B		
193.29.90.88	193.29.90.119	193.29.90.158	2261

If you are using a client to connect to the CUE, the client will ask you once to accept the DBAG CUE Server Host Key, The Server Host Key will be remembered for future logins by the client. If you use a customized script to access the CUE, the Server Host Key has to be integrated where appropriate. The DBAG Server Host Key for the CUE can be found in the Appendix of this document.

Connectivity to the CUE can be tested via Telnet.

4.1 Microsoft Windows example using WinSCP

WinSCP is an open source free SFTP client, SCP client, FTPS client and FTP client for Microsoft Windows.

Its main function is file transfer between a local and a remote computer. Beyond this, WinSCP offers scripting and basic file manager functionality.

Source: <http://winscp.net/eng/index.php>

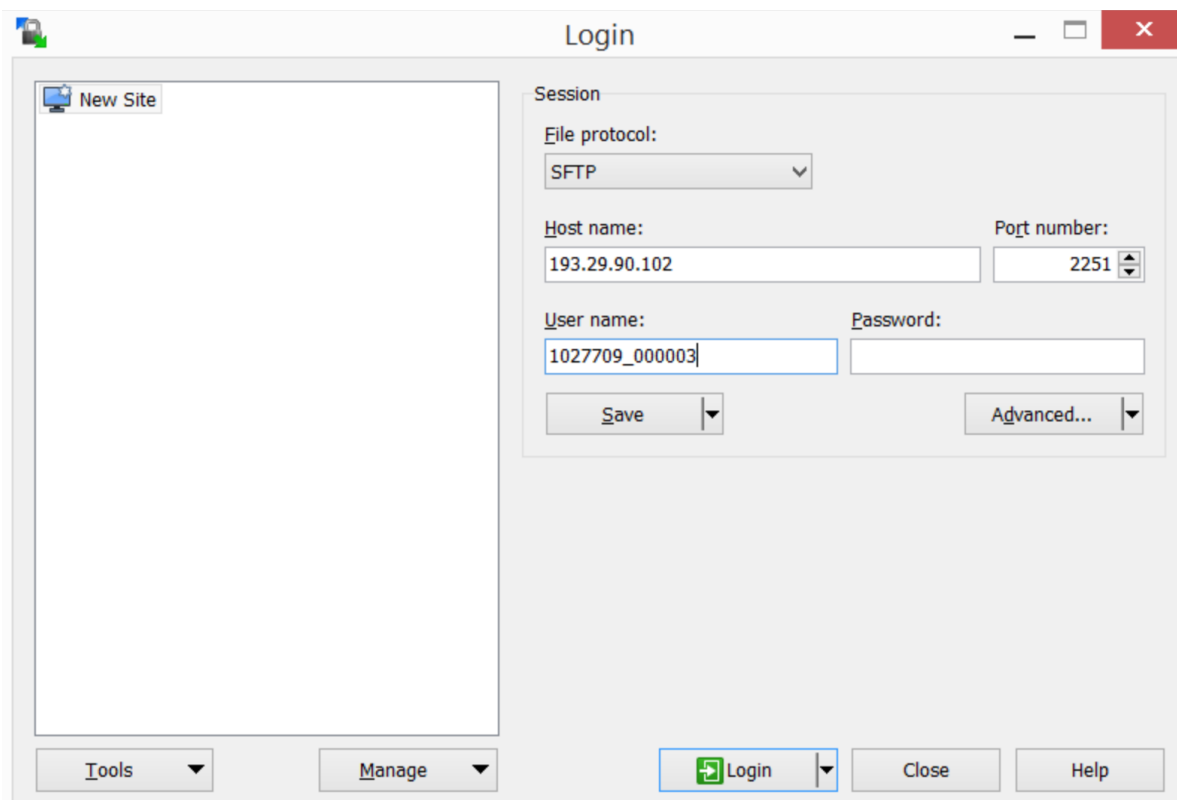


Fig. 10: Input screen required in order to log in to the CUE

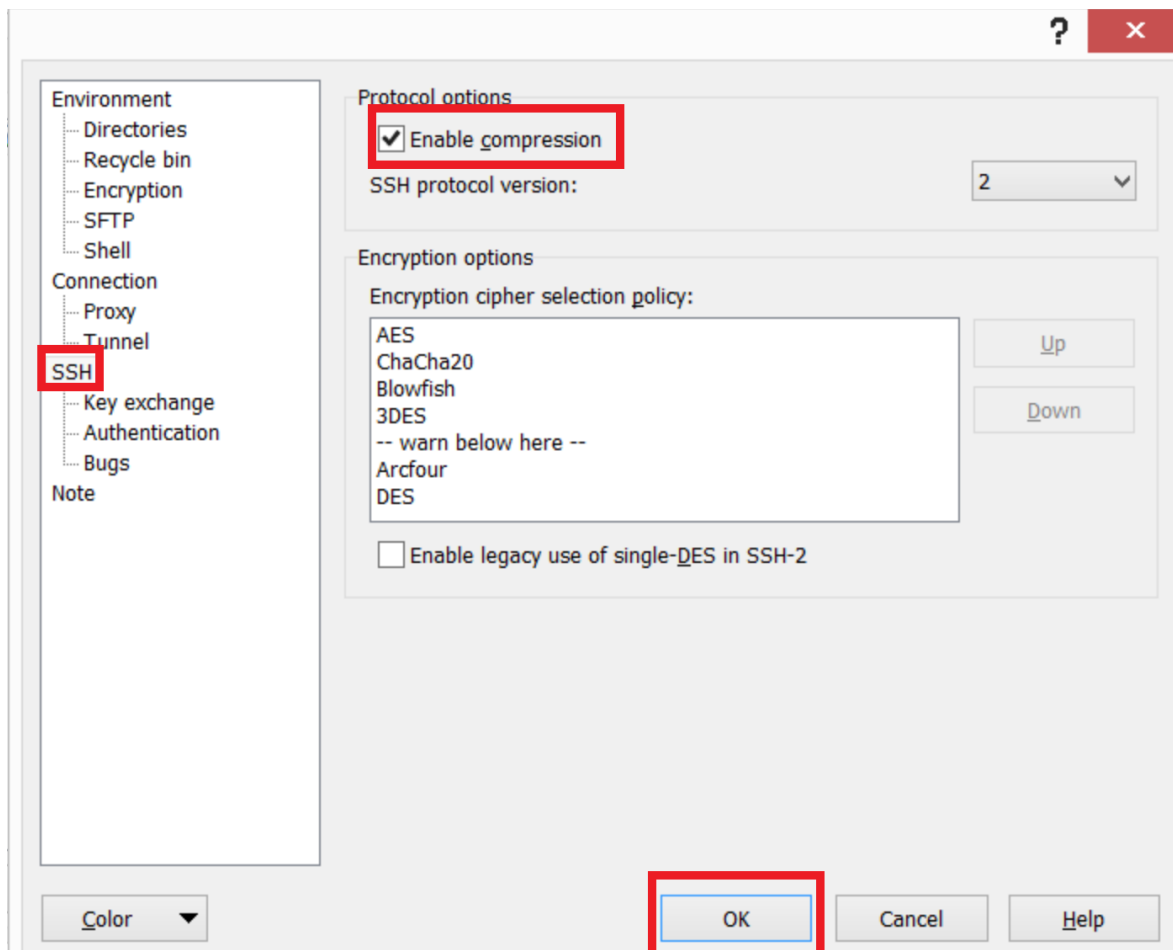


Fig. 11: Enable compression for SSH transfer.

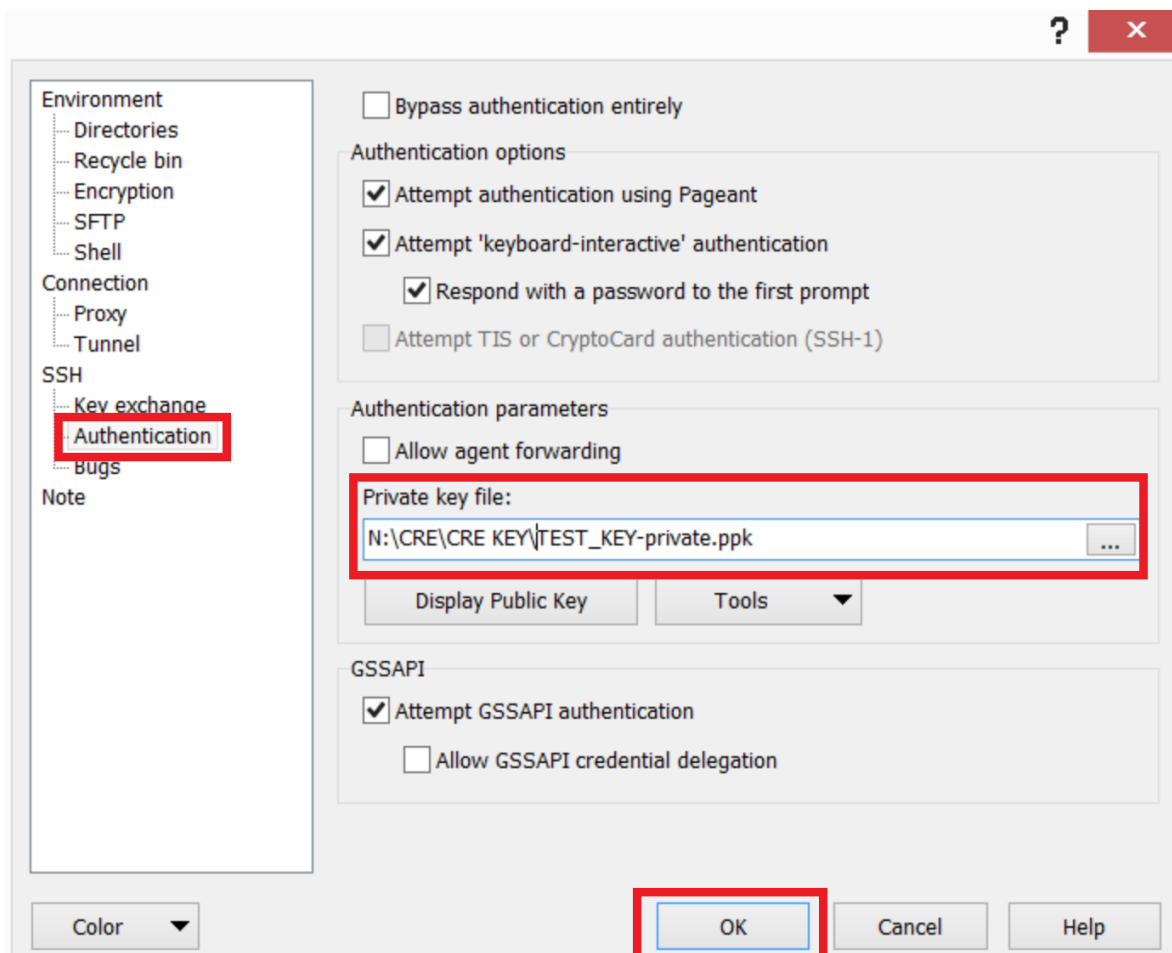


Fig. 12: Upload private Key

After a successful login participant can use the full range of functionality of the CUE.

4.2 Uploading files

Participants may use the SFTP client of their choice to access the CUE’s server. After successful login, participants will be able to upload their files.

In case a connection to the CUE is not possible or an existing connectivity got broken please do not try to login again in very short time intervals (i.e. several tries every few seconds) but rather wait a little while (a minute or more) and then try again. If you tried this for a few times and still no connection can be established, please contact DBAG Technical Support.

5 Report and file naming conventions

Report and file naming conventions and further procedures will be described in a separate documentation issued by the respective service.

6 Appendix - Server Host Key for the CUE

6.1 Server Host Key DBAG CUE for Leased Line

ssh-rsa

```
AAAAB3NzaC1yc2EAAAADAQABAAQCAQD84GrfCr8mb8KXcm4AAYVw2EdYbp0zITHnt5hj6opuh  
COIXKvpoHMMgDd2I6tk+FQI6VpDHEV7HHg2SsKo21oaNsTB+YHJSrF5RKzt1o24eq1NTrwQZH  
g0vhjR1b2le6QVcy5fdmCymWTLq4NAB5I6YAy4WjhSwJr4CzfZI7bZ6BmgfR+DQyzKlgl6mD0+  
Q3wuCDkysLA/rKrXMfCRpH2ly1VOWCeGb0ZdxWM/exK195+5xyDjFw1pDGSVpzGr2cE5V5B7bk  
xdOtb7Buj8oINUQjLk85co5iG7iA0/9yDTJrbX++m9FvFnlGmpet+j6EG09aypZBEHo//u/wK3+IQ  
Sql9Elwsf0Ssq89sOw65+GOckw7pShArHDTpeJTbabMPrHbi7d86bPulv74mctfaN2wU+Uo3CdI  
AjJigP8cVrw7OTLRh9Rb2j6/IDk7z/tUF+ATRMht6S/f11g/450LRjY6fy9pQtRU7rpCTuqwgm9F7Y  
SJOGwxZuDCccpWyvShugflGY3X0aW16dgqkWv5BHXgDr+4RYimiGBD31J9BSbTYA6epXRvNW  
PyBqMYkKhBA9WLMs3pnR53dlce+IC5pycg0g6/MrqhY3VF1rtOca8UoB9734dTYLybVkc4ixJ7u  
R3wh2K+LyR6JWgVHMj6hAtAN/Go+92vzPNJH9yi18/Q==
```

7 Change Log

Date	Chapter	Change
16.08.2021	4	New Screenshots and IP Address overview
27.09.2021	1.3 / 7	Moved the change log from 1.3 to the end of the document as chapter 7
	4	Adapted assignment of IP addresses for CUE area A
	4	Corrected the IP address for CUE area B, leased line A