SEEBURGER BUSINESS INTEGRATION

SEEBURGER CLOUD

MBR Gateway Service: SFTP Data Sheet

Technical information to configure your SFTP connection to the SEEBURGER Cloud

Company Details

Name:	SEEBURGER AG
Address:	Edisonstraße 1 DE-75015 Bretten

To configure your connection to the SEEBURGER Cloud, please use this data sheet we prepared for you. The first part is for your network administrator to open your **firewall** for successful communication. The second part contains the configuration data required to **send** data to the SEEBURGER Cloud. The third part contains the configuration data required to **receive** data from the SEEBURGER Cloud.

Note: The SEEBURGER Cloud provides an SFTP Server to send and receive data. SFTP uses the Secure Shell (SSH) to authenticate remote computers and allow remote computers to authenticate users. If your file transfer client does not support SSH, please contact our SEEBURGER Cloud Service Team.

1. SFTP – FIREWALL Configuration

For sending and receiving data, the following connection has to be allowed on your system / firewall:

FROM: IP address of your SFTP Client	**TO:** IP ranges: **85.115.5.64 – 85.115.5.95** (alternative representation) **85.115.5.64/27** and **85.115.19.120 – 85.115.19.127** (alternative representation) **85.115.19.120/29** Port: **1322**

Note: Our firewall is already open for you.

2. SFTP – SENDING Data to the SEEBURGER Cloud

SEEBURGER Hostname:	This hostname is used by your local system to send files to the SEEBURGER Cloud. sftp.seeburger.cloud
SFTP Server Fingerprints:	SSH-RSA 2048: 82:fb:36:18:9d:eb:b1:3c:fe:83:93:ae:e0:62:aa:c0 ECDSA-SHA2-NISTP 521: 5e:1b:80:fe:bc:f0:a8:bf:8c:c0:a7:97:44:e3:d0:b3
Your SSH Public Key[1]:	This authentication parameter is required for the connection to the SEEBURGER SFTP server. Allowed key types: DSA/RSA/ECDSA Minimum key length: 2048 bit for DSA/RSA, 256 NISTP for ECDSA

	Note: The SFTP server is using Public/Private Key authentication.
SFTP User:	The username is generated by the SEEBURGER Cloud, it usually has 6 alphabetic and 9 numeric characters, e.g. SEEGWE30000001
Your outbox directory:	Put the data you want to send to the SEEBURGER Cloud in this directory: **\mbr\outbox\[partner SEEID]**, e.g. **\mbr\outbox\SEEGWE31111111** Note: the directory name is used to determine to which recipient the file should be sent. We recommend always using the temporary file when sending. Many programs use this method automatically, but it may still need to be activated and configured in the software. Temporary files should have a specific format - for example: name.tmp, name.temp, name.filepart. Other temporary file names are not recognized as such. If the static file names are still sent, we will rename them and add an automatically generated suffix to the end of the file.

3. SFTP – RECEIVING Data from the SEEBURGER Cloud

Note: You may read any given file in the Inbox several times. In order to commit that you read the data, delete it. Otherwise it will remain sitting in the Inbox.

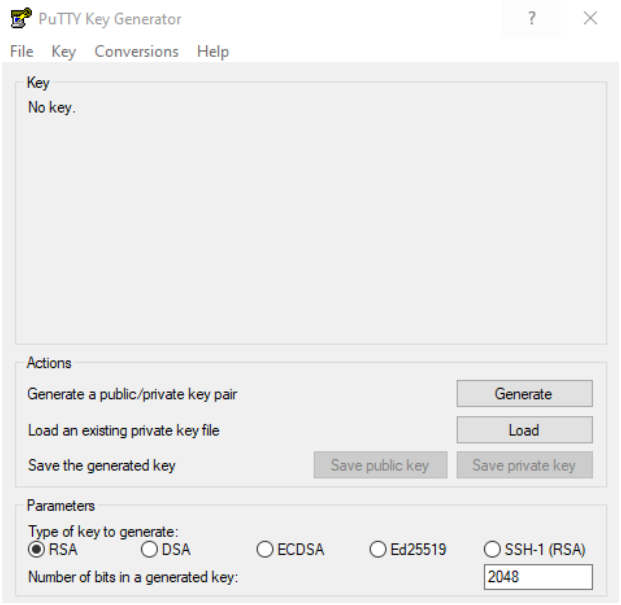
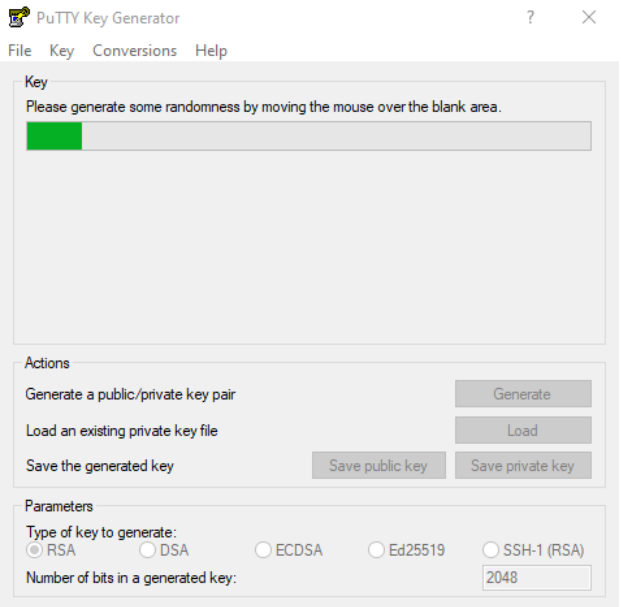
SEEBURGER Hostname:	This hostname is used by your local system to send files to the SEEBURGER Cloud. sftp.seeburger.cloud
SFTP Server Fingerprints:	SSH-RSA 2048: 82:fb:36:18:9d:eb:b1:3c:fe:83:93:ae:e0:62:aa:c0 ECDSA-SHA2-NISTP 521: 5e:1b:80:fe:bc:f0:a8:bf:8c:c0:a7:97:44:e3:d0:b3
Your SSH Public Key[1]:	This authentication parameter is required for the connection to the SEEBURGER SFTP server. Allowed key types: DSA/RSA/ECDSA Minimum key length: 2048 bit for DSA/RSA, 256 NISTP for ECDSA Note: The SFTP server is using Public/Private Key authentication.
SFTP User:	The username is generated by the SEEBURGER Cloud, it usually has 6 alphabetic and 9 numeric characters, e.g. SEEGWE30000001
Your inbox directory:	Find the data you receive from the SEEBURGER Cloud in this directory: **\mbr\inbox\[partner SEEID]**, e.g. **\mbr\inbox\SEEGWE31111111** Note: The directory name contains the SEEID of the corresponding sender. Please do not rename or move files in the SFTP folders that we provide to you in the Cloudlink. Changing the files will lead to problems in status transmission to the company that sends data to you. In addition, no new folder structures shall be created and polled files must be deleted directly. The SFTP folders are not intended to be a permanent storage section. In this context, we also want to inform that files not being deleted have a specific TTL (time to live) after which the files will be deleted without any additional warning. The inbox only allows you to receive files from the cloud - it is not allowed to be used to upload data yourself in order to download it afterwards. Data sending to the cloud goes via outbox\... .

[1] If you have problems creating the SSH Public Key, you can find help in the annex.

ANNEX – SSH PUBLIC KEY CREATION using PuTTYgen

One of the tools you can use to generate an SSH keypair for authentication of your user is PuTTYgen. Others exist, please see their documentation for details. The text below uses PuTTYgen as an example to outline the process of creating

- a private key (for use with your SFTP Client) and
- a public key (to be uploaded on the SEEBURGER Cloud Communication service where the SFTP Server will use it).

First you have to install the free tool PuTTY. Then you can start with the SSH Public Key creation. This free software is easily accessible on the internet.	Link: https://www.puttygen.com/
Now set the required parameters in the PuTTYgen interface. To create a key, the following parameters are required: **RSA or DSA and a bit length of at least 2048**, then click on **Generate**.	
PuTTY now creates the key. For the random generator, **move the mouse over the area below the bar until the creation is complete**.	

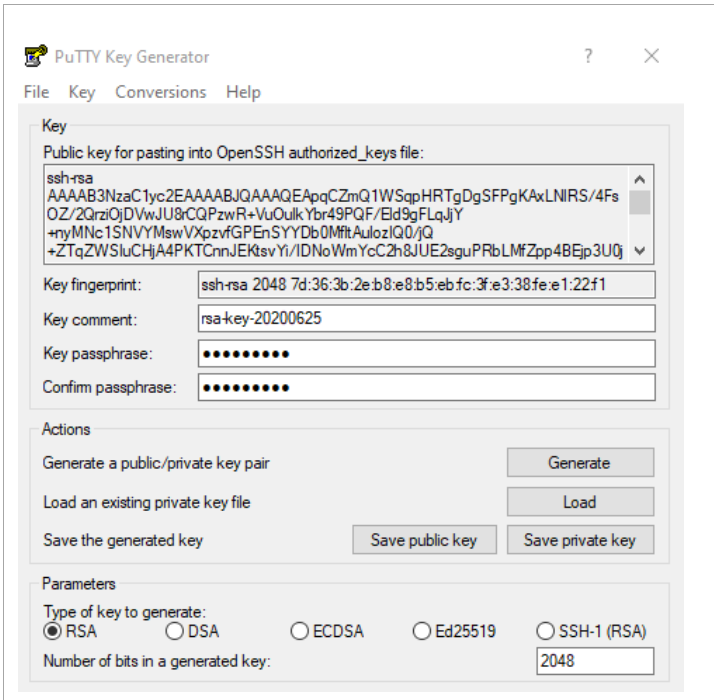
Please use **Key comment** field with a meaningful description and **Key passphrase** to save your Private Key with password.

Click on **Save Public Key** to save the public key.

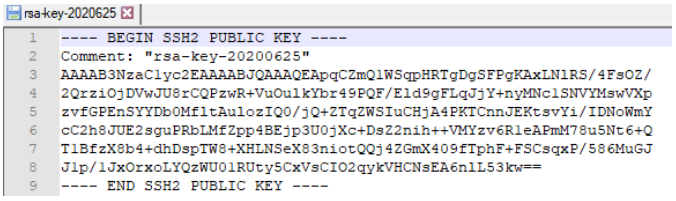
Click on **Save Private Key** to save the private key as well.

Put the pair in a folder and make sure to give them meaningful file names.

You now have generated the key pair and can then use it for Seeburger SFTP Cloudlink.



Finally, you can open the saved public key with any Windows editor and copy and paste the whole content into the text „SSH Public Key“ field in the Seeburger SFTP Cloudlink configuration.



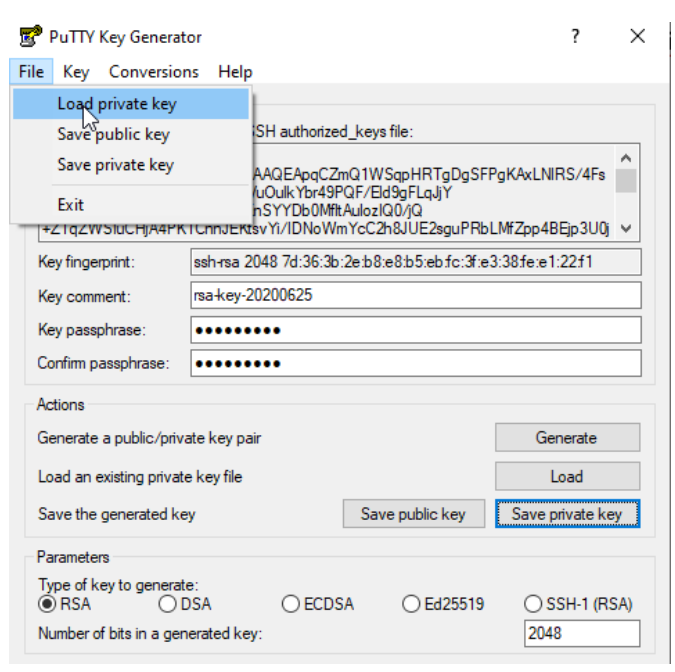
Note:

Not all Business Interface Systems natively support the Private Key format .ppk generated by PuTTYgen. You can convert your private key into format (.pem) file before you import it in your Business Interface Systems. You can use the PuTTYgen tool for this conversion too.

Start PuTTYgen again.

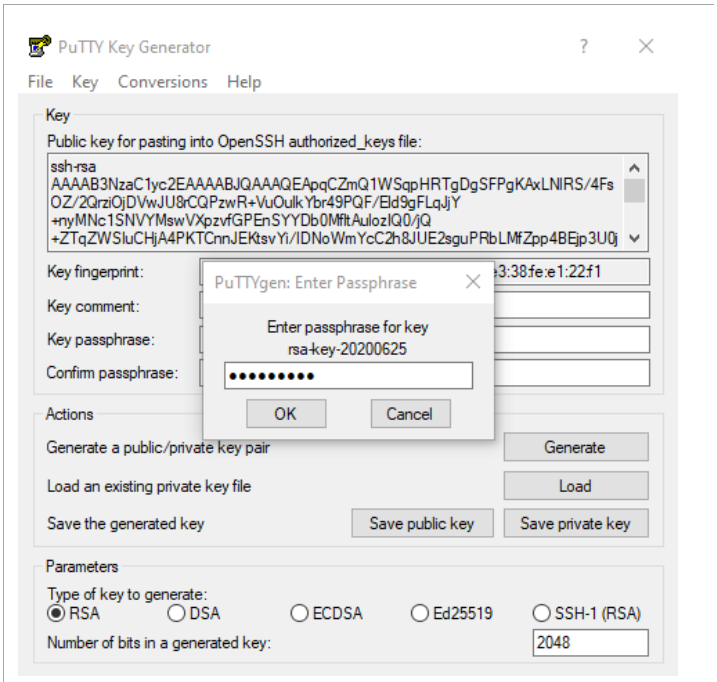
Click **File** and **Load private key.**

Navigate to your .ppk file, select and open it.



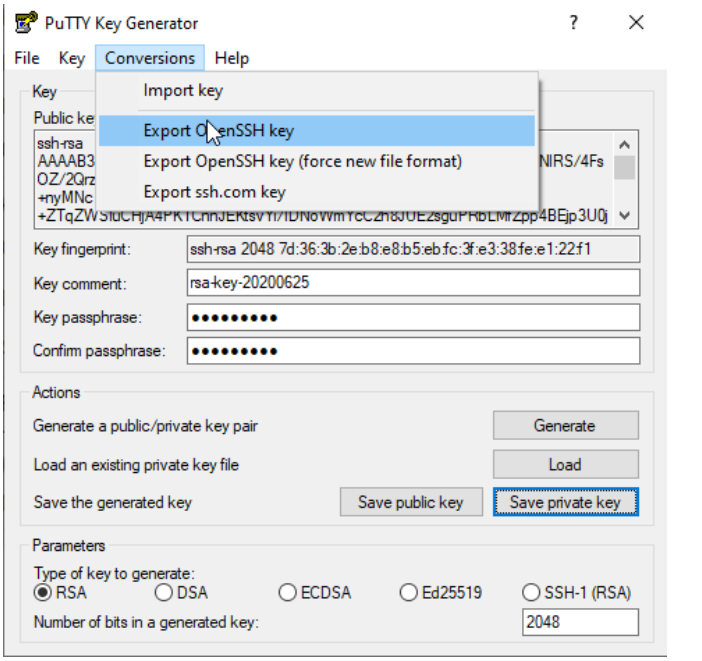
A dialog will be opened now. The expected **passphrase for key** is the one you entered during the creation of your private key.

Enter your passphrase and click **OK**.



Your private key is opened now.

Go to **Conversion** and choose **Export OpenSSH Key**.

Enter the name of file, e.g. „rsa-key-2020625**.pem**“. Ensure that .pem is the ending of your filename.

Click **Save**. Now you can use this *.pem- file for the import in your Business Integration System.