



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

Name:	SEEBURGER Cloud Service Team
E-mail:	support@cloud.seeburger.de
Phone:	+49 (0)7252 96 1443

To configure your connection to the SEEBURGER Cloud, please use this data sheet we prepared for you. The first information 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 includes the configuration data required to **receive** data.

<u>Note</u>: 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	то:	IP ranges:	85.115.5.64 85.115.19.120	-	85.115.5.95 and 85.115.19.127
		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
SEEBURGER'S SSH Public Key:	sftp.seeburger.cloud.cer ¹
Your SSH Public Key ² :	This authentication parameter is required for the connection to the SEEBURGER SFTP server. DSA / RSA type keys allowed, minimum key length 2048 bit.
SFTP User:	The username is generated by the SEEBURGER Cloud, it usually has 6 alphabetic and 9 numeric characters, e.g. SEEGWE30000001
Password:	This password is used by your local system for authentication in file transfer with the SEEBURGER Cloud (in addition to the SSH Public Key). The password is required and cannot be empty.
Your outbox directory:	Put the data you want to send to the SEEBURGER Cloud in this path: \<short name="" of="" service="" the="">\outbox\[partner SEEID]</short> , e.g.:

Meta Based Routing: \mbr\outbox\SEEGWE3111111

(This directory name equals the Identification of the receiver to which the messages will be sent.)

3. SFTP – RECEIVING Data from the SEEBURGER Cloud

<u>Note</u>: 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			
SEEBURGER'S SSH Public Key:	sftp.seeburger.cloud.cer ¹			
Your SSH Public Key ² :	This authentication parameter is required for the connection to the SEEBURGER SFTP server. DSA / RSA type keys allowed, minimum key length 2048 bit.			
SFTP User:	The username is generated by the SEEBURGER Cloud, it usually has 6 alphabetic and 9 numeric characters, e.g. SEEGWE30000001			
Password:	This password is used by your local system for authentication in file transfer with the SEEBURGER Cloud (in addition to the SSH Public Key). The password is required and cannot be empty.			
Your inbox directory:	Find the data you receive from the SEEBURGER Cloud in this path: \<short name="" of="" service="" the="">\inbox\[partner SEEID]</short> , e.g.:			
	Meta Based Routing: \mbr\inbox\SEEGWE3111111			
	(This directory name equals the Identification of the sender who sent the data to you.)			

¹ You can download our data sheets and certificates on the following URL: **www.seeburger.com/cloud/connect-the-cloud/** ² If you have problems in creating the Public SSH 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.	Link: <u>https://www.puttygen.com/</u>
This free software is easily accessible on the internet.	
Now set the required parameters in the PuTTYgen interface.	PuTTY Key Generator ? X
To create a key, the following parameters are required: RSA or DSA and a bit length of at least 2048, then click on Generate.	File Key No key. Actions Generate Load an existing private key file Load Save the generated key Save public key
	Number of bits in a generated key: 2048
For the random generator, move the mouse over the area below the bar until the creation is complete.	PuTTY Key Generator ? × File Key Conversions Help Key Please generate some randomness by moving the mouse over the blank area.
	Actions Generate a public/private key pair Generate Load an existing private key file Load Save the generated key Save public key Parameters Type of key to generate: • RSA DSA • RSA DSA • ECDSA Ed25519 • SSH-1 (RSA) Number of bits in a generated key:

Please use Key comment field with a meaningful description and Key passphrase to save your Private Key with password.	😴 PuTTY Key Generator ? X File Key Conversions Help
Click on Save Public Key to save the public key.	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.	AAAABJIVaa IyozEAAAABJUAAAQEAPQL2mq IWSqpHK IgUgSFPgKAxLNiKS/4Fs OZ/2qrz0jDWJU8rCQPzwR+VuOukVpr49PQF/Eld9gFLqJ)Y +nyMNc1SNVYMswVXpzvfQPEnSYYDb0MftAulozIQ0/jQ +ZTqZWSIuCHjA4PKTCnnJEKtsvYi/IDNoWmYcC2h8JUE2sguPRbLMfZpp4BEjp3U0j
You now have generated the key pair and can then use it	Key fingerprint: ssh-rsa 2048 7d:36:3b:2e:b8:e8:b5:eb.fc:3f:e3:38.fe:e1:22.f1
for Seeburger SFTP Cloudlink.	Key comment: rsa-key-20200625
	Key passphrase:
	Confirm passphrase:
	Actions
	Generate a public/private key pair Generate
	Load an existing private key file Load
	Save the generated key Save public key Save private key
	Parameters Type of key to generate: ● RSA O DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA) Number of bits in a generated key: 2048
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.	<pre>nakey-2020625 1</pre>

<u>Note</u>:

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.

PuTTY Key Generate	or				?	×
le Key Conversion	s Help					
Load private key	H					
Save public key	3	SH authorize	d_keys	file:		
Save private key	e	AQEApqCZ	mQ1WS		gKAxLNIRS/	4Fs
Exit	ĥ	SYYDb0Mft	Aulozia	19gFLqJj Y 20/jQ		
+Z1qZWSIUCHJA4PK	CNNJEKts	vYi/IDNoWi	mYcC2h	8JUE2sguPRbL	.MfZpp4BEjp	3U0j 🗸
Key fingerprint:	ssh-rsa 20	48 7d:36:3b	:2e:b8:e	e8:b5:eb.fc:3f:e3	3:38.fe:e1:22.f	1
Key comment:	rsa-key-20	200625				
Key passphrase:						
Confirm passphrase:						
Actions						
Generate a public/private key pair Generate						te
Load an existing private	key file				Load	
Save the generated key	/		Save	e public key	Save priva	te key
Parameters						
Type of key to generate	sA		5A	O Ed25519	⊖ ssh-	1 (RSA)
N. 1. (1.9.)					2040	

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**.

😨 PuTTY Key Generato	or	?						
ile Key Conversion	s Help							
Key								
Public key for pasting in	to OpenSSH authorized_keys file:							
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEApqCZmQ1WSqpHRTgDgSFPgKAxLNIRS/4Fs OZ/20rzi0jDVwJU&CQPzwR+VuOulkYbr49PQF/Bd3gFLqJy +nyMNc1SNVYMswVXpzvfGPEnSYYDb0MftAuloz1Q0/jQ +ZTqZWSluCHijA4PKTCnnJEktsyYi/IDNoWmYcC2h8JUE2squPRbLMfZpp4BEp3U0j								
Key fingerprint:	PuTTYgen: Enter Passphrase $ imes$	3:38.fe:e1:22.f1						
Key comment:								
Key passphrase:	Enter passphrase for key rsa-key-20200625							
Confirm passphrase:	•••••							
Actions	OK Cancel							
Generate a public/priva	te key pair	Generate						
Load an existing private	key file	Load						
Save the generated key	Save public key	Save private key						
Parameters								
Type of key to generate	: SA OECDSA OEd25519	O SSH-1 (RSA)						
Number of bits in a gene	erated key:	2048						

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.

S	PuTTY	Key Generato	or					?	×
File	e Key	Conversion	s Help						
F	Key	Impor	t key					L	
	Public ke ssh-rsa	Export	t OlenSSH	key					^
	AAAAB3 OZ/2Qrz +nyMNc	Export	t OpenSSH key (force new file format) t ssh.com key					NIRS/4Fs	
	+21d2 vv StudenjA4+ K Tenniferstv Tr/TiDNo vvini redznos 062/sgur Robini zpp+bejp Kev fingemint: [ssh-tsa 2048 7d:36:3b:2e:b8:e8:b5:eb.fc:3f:e3:38.fe:e1:22]							чысрэоор e1:22.f1	<u> </u>
	Key comn	nent:	rsa-key-202	00625					
	Key passp	ohrase:	•••••	•					
	Confirm passphrase:								
-	Actions								
	Generate	a public/priva	te key pair				(Generate	
	Load an e	existing private	key file					Load	
	Save the generated key Save public key Save							e private ke	у
Parameters									
	Type of k RSA	ey to generate	s: SA	OECDS	A	O Ed25519	С	SSH-1 (RS	SA)
	Number o	f bits in a gene	erated key:				2	048	