



B2B Routing Service: SFTP Data Sheet

Technical information to configure your SFTP connection to the SEEBURGER Cloud

Company Details

Contact	Detai	ls

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

Name:SEEBURGER Cloud Service TeamE-mail:support@cloud.seeburger.dePhone:+49 (0)7252 96 1443

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. The last part contains information on how to **test** your connection.

<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
Server SSH-RSA Fingerprint:	82:fb:36:18:9d:eb:b1:3c:fe:83:93:ae:e0:62:aa:c0
Your SSH Public Key ¹ :	This authentication parameter is required for the connection to the SEEBURGER SFTP server.
	<u>Note</u> : 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: \cbr\outbox
	Note: the file content is used to determine to which recipient it 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.

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

3. SFTP – RECEIVING Data from 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 SSH-RSA Fingerprint:	82:fb:36:18:9d:eb:b1:3c:fe:83:93:ae:e0:62:aa:c0
Your SSH Public Key ¹ :	This authentication parameter is required for the connection to the SEEBURGER SFTP server. DSA/RSA type keys are allowed, minimum key length 2048 bit.
	Note: 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: \cbr\inbox
	Note: 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 belong 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\

4. SFTP – TESTING Your Connection

We are not using a separate test system for the SEEBURGER Cloud. After you have finished the configuration of your EDI system, you can start testing your configuration. The test works as follows:

- 1. Connect to the server and place a test file in /echo/outbox.
- 2. This file will appear automatically in /echo/inbox.

Note: You might need to refresh your SFTP Client to list all available directories, so that /echo is displayed.

If you do NOT receive the file 5 minutes after starting the test, please check your settings (e.g. firewall) or contact our SEEBURGER Cloud Service Team.

After successful testing, please contact our SEEBURGER Cloud Service Team to change from test to productive mode. Contact information can be found above on the first page of the data sheet.

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.	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 Conversions Help Key No key.
	Actions Generate a public/private key pair Load an existing private key file Load Save the generated key Parameters Type of key to generate: O RSA O DSA ECDSA Ed25519 SSH-1 (RSA) Number of bits in a generated key: 2048
PuTTY now creates the key.	
below the bar until the creation is complete.	File Key Conversions Help Key Please generate some randomness by moving the mouse over the blank area. Actions Generate a public (drivate key pair
	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 Parameters Save public key Number of bits in a generated key: 2048

Please use Key comment field with a meaningful description and Key passphrase to save your Private Key with password.	😴 PuTTY Key Generator ? × 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.	Public Key for pasting into UpenSSH authorized_keys file: ssh-rsa
Put the pair in a folder and make sure to give them meaningful file names.	AAAABJNzaC1yc2EAAAABJQAAAQEApqC2mQ1WSqpHR1gDgSFPgKAxLNIRS/4Fs OZ/2Qrzi0jD/wJU8rCQPzwR+VuOulkYbr49PQF/Eld9gFLgJjY +nyMNc1SNVYMswVXpzvfGPEnSYYDb0MftAuloz1QU/jQ +ZTqZWSIuCHjA4PKTCnnJEKtsvYi/IDNoWmYcC2h8JUE2sguPRbLMfZpp4BEjp3U0j V
You now have generated the key pair and can then use it	Key fingerprint: ssh-rsa 2048 7d:36:3b:2e:b8:e8:b5:ebfc:3f:e3:38fe:e1:22f1
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:
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>imakey-2020625 X</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/priva	te key pair				Genera	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 RSA	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 Generat	br	? ×						
File Key Conversion	is Help							
Key								
Public key for pasting in	to OpenSSH authorized_keys file:							
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEApqCZmQ1WSqpHRTgDgSFPgKAxLNIRS/4Fs OZ/2Qrzi0jDVwJU&CQPzwR+VuOulkYbr49PQF/Eld9gFLqJjY +nyMNc1SNVYMswVXpzvfGPEnSYVDb0MftAulozIQ0/jQ +ZTqZWSluCHjA4PKTCnnJEKsvYi/JDNoWmYcC2h8JUE2squPRbLMfZpp4BEjp3U0j								
Key fingerprint:	PuTTVgen: Enter Passphrase X	3:38.fe:e1:22.f1						
Key comment:								
Key passphrase:	Enter passphrase for key							
Confirm passphrase:	••••••							
Actions	OK Cancel							
Generate a public/priva	ite key pair	Generate						
Load an existing private	e key file	Load						
Save the generated key	Save public key	Save private key						
Parameters								
Type of key to generate RSA O D	e: ISA O ECDSA O Ed25519	O SSH-1 (RSA)						
Number or bits in a gen	cialeu key.	2040						

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.

2	PuTTY	Key Generato	or					?	×
File	Key	Conversion	s Help						
K	iey 👘	Impor	t key					-	
F	ublic ke ssh-rsa	Export	t O <mark>le</mark> nSSH	key					•
0	AAAAB3 DZ/2Qrz +nvMNc	Export	t OpenSSH t ssh.com k	key (force œy	new f	file format)		NIRS/4Fs	
ŀ	+ZTqZW	SIUCHJA4PK	CnnJEKtsv	17/1DNoVVn	1TCU2	h&JUEZsguPRbL	.мт∠рр	4BEjp3U0j	¥
K	(ey finger	print:	ssh-rsa 204	8 7d:36:3b:	2e:b8:	e8:b5:eb.fc:3f:e3	:38.fe:	e1:22.f1	
K	(ey comn	nent:	rsa-key-202	00625					
ĸ	(ey pass	ohrase:	•••••	•					
C	Confirm p	assphrase:	•••••	•					
A	ctions								
6	ienerate	a public/priva	te key pair				(Generate	
L	oad an e	existing private	key file					Load	
S	Save the generated key Save public key Save private key								
P	arameter	rs							
1	ype of k RSA	ey to generate	e: SA		A	O Ed25519	С) SSH-1 (RS	5A)
Ν	lumber o	f bits in a gene	erated key:				2	048	