DATA SHEET

SEEBURGER
BUSINESS INTEGRATION

SEEBURGER CLOUD

MBR Gateway Service: OFTP2 Data Sheet

Technical information to configure your OFTP2 connection to the SEEBURGER Cloud

Company Details

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

Contact Details

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 part is for your network administrator to open your **firewall** for successful communication. The second part contains the general settings to **send/receive** data to/from the SEEBURGER Cloud. The third part contains the configuration data required to **send** data to the SEEBURGER Cloud. The fourth part contains the configuration data required to **receive** data from the SEEBURGER Cloud.

Please be aware of these general comments:

- OFTP2 is based on TCP. OFTP over ISDN or X.31 or VPN is not supported.
- OFTP2 security settings are enabled, that means:
    - OFTP2 is "strict" using SSL/TLS. A transmission without SSL/TLS is not supported.
      Server certificate should be signed by a trusted certificate authority.
    - Session authentication via passwords.
    - Session authentication using certificates is supported. If this will be used, OFTP2 certificates need to be exchanged. Session authentication needs to be enabled on both sides (SEEBURGER Cloud and Partner).
    - File encryption (AES-256) is supported. If this will be used, OFTP2 certificates need to be exchanged.
    - File signature and EERP signature are supported. They can only be enabled or disabled together.
      If these will be used, OFTP2 certificates for file signature and EERP signature need to be exchanged.
      The signature algorithm RSA-SHA256 or RSA-SHA512 should be used. We strongly recommend **not** to use SHA-1 signature algorithm.
    - File compression is supported.
      Note: Compression on session level is not recommended as it is very ineffective for modern EDI formats. It is not used by the SEEBURGER Cloud to send data to customers.
- The SEEBURGER Cloud uses the same OFTP2 certificate for TLS/SSL, encryption, signature, session authentication and file level.
- OFTP2 **Change Direction** is not supported. Only the initiator of the OFTP2 session is allowed to send files. The partner is not allowed to send files. To receive files from your partner, they have to initiate the OFTP2 session with you.

1. OFTP2 – FIREWALL Configuration

To **SEND** data to the SEEBURGER Cloud, please open your firewall to allow outgoing OFTP2 traffic:

FROM: IP address of your OFTP2 system	**TO:**	IP ranges:	**85.115.5.64**	–	**85.115.5.95** and
			85.115.19.120	–	**85.115.19.127**
		Port:	**6619**		

To **RECEIVE** data from the SEEBURGER Cloud, please open your firewall to allow incoming OFTP2 traffic:

FROM:	IP ranges:	**85.115.5.64**	–	**85.115.5.95** and	**TO:** IP address and port of your OFTP2 system
		85.115.19.120	–	**85.115.19.127**	

Note: Our firewall is already open to receive messages from you.

2. OFTP2 – General settings for SENDING/RECEIVING Data

Our SSID:	O0013000031SEE30532CL03
Our password:	SEEBUR
Our TLS/SSL certificate:	oftp2.seeburger.cloud.cer[1]
Our session authentication certificate:	oftp2.seeburger.cloud.cer[1]
SFID:	Individual SFID of your communication partner on the SEEBURGER MBR Gateway
Our ENCRYPTION certificate (file encryption):	oftp2.seeburger.cloud.cer[1]
Our SIGNATURE certificate (file and EERP signature):	oftp2.seeburger.cloud.cer[1]

3. OFTP2 – SENDING Data to the SEEBURGER Cloud

URL:	oftp2.seeburger.cloud
Port:	6619
Compression:	File compression on sender side can be enabled. Note: Compression on session level is not recommended as it is very ineffective for modern EDI formats.
Certificate Authority (CA):	Odette CA
SIGNATURE Algorithm (file and EERP signature):	NONE, RSA-SHA256, RSA-SHA512, SHA-1 Note: We recommend using RSA-SHA256 or RSA-SHA512 to meet the highest standards of security. Note: File and EERP signature are jointly enabled / disabled.
ENCRYPTION Algorithm (file encryption):	NONE, AES-256, 3DES
EERP	Once the SEEBURGER Cloud successfully delivered a message to the recipient, an EERP is generated, **signed** by the SEEBURGER Cloud and returned to the sender. Note: The SEEBURGER Cloud supports sending EERP back immediately after receipt of the message. This is not recommended but might be required in some rare cases. Note: EERP signature can be disabled together with file signature.

4. OFTP2 – RECEIVING Data from the SEEBURGER Cloud

Compression:	None Note: File compression can be enabled, if required. Note: Compression on session level is not recommended as it is very ineffective for modern EDI formats.
Your TLS/SSL Certificate:	Note: An approved certificate authority (CA) should issue your SSL certificate. Please add the domain host name used in the URL as common name (CN) in the certificate request. Do not use a static IP as host name. Note: The option ”Certificate authority-based for TLS” can be used instead of configuring a specific certificate which has to be replaced regularly. The SEEBURGER Cloud will check the certificate presented by the server configured for this connection against a list of trusted root certificates. Also, the certificate presented by the server will be checked against the server name to ensure that the connection goes to the correct server.
ENCRYPTION Algorithm (file encryption):	NONE, AES-256, 3DES
SIGNATURE Algorithm (file and EERP signature):	SHA-1, RSA-SHA256 and RSA-SHA512 Note: We recommend using RSA-SHA256 or RSA-SHA512 to meet the highest standards of security. Note: File and EERP signature can be disabled together.
EERP	Normally the SEEBURGER Cloud waits for a signed partner's EERP before returning a positive acknowledgement to the original message sender. Note: Default timeout for the SEEBURGER Cloud waiting for the partner's EERP is 2 hours. The maximum value for this setting is 24 hours. Note: Disabling this standard behavior is not recommended but might be required in some rare cases.

[1] You can download our data sheets and certificates on the following URL: **www.seeburger.com/cloud/connect-the-cloud/**