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<br>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 configuration data required to **send** data to the SEEBURGER Cloud. The third part includes 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 TLS/SSL, plain OFTP is not supported.
  - Session Authentication via Passwords
  - Partner Authentication/File Encryption/File Signatures via Private/Public Key (Certificates)
- OFTP2 "Change Direction" is not yet 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, he has 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 address: **85.115.5.74**<br>Port: **6619** |

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

| | | | |
|---|---|---|---|
| **FROM:** | IP address: **85.115.5.74** | **TO:** | IP address and Port of your OFTP2 system |

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

## 2. OFTP2 – SENDING Data to the SEEBURGER Cloud

| | |
|---|---|
| Our SSID: | SEECLOUD_OFTP_SSID |
| Our Password: | 1 |
| SFID: | Individual ID of your communication partner on the SEEBURGER MBR Gateway |
| URL: | oftp2.seeburger.cloud |
| Port: | 6619 |

| | |
|---|---|
| TLS/SSL certificate: | oftp2-ssl.seeburger.cloud.cer[1] |
| Certificate Authority (CA): | GlobalSign Root CA |
| SIGNATURE Algorithm: | Note: We recommend using an SHA-2 algorithm to meet the highest standards of security. |
| ENCRYPTION Certificate (File Encryption): | oftp2.seeburger.cloud.cer[1] |
| ENCRYPTION Algorithm: | Note: We recommend using AES/256 to meet the highest standards of security. |
| 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.<br>In case the message could not be delivered before the message is expired a NERP (negative response) is generated and returned to the sender. |

## 3. OFTP2 – RECEIVING Data from the SEEBURGER Cloud

| | |
|---|---|
| Our SSID: | SEECLOUD_OFTP_SSID |
| Our Password: | 1 |
| SFID: | Individual ID of your communication partner on the SEEBURGER MBR Gateway |
| Compression: | None |
| Your TLS/SSL Certificate: | Note: An approved Certificate Authority (CA) should issue your SSL Certificate.<br>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. |
| ENCRYPTION Algorithm: | Note: We recommend using AES/256 to meet the highest standards of security. |
| SIGNATURE Certificate (File Signature): | oftp2.seeburger.cloud.cer[1] |
| SIGNATURE Certificate (Session Signature): | oftp2.seeburger.cloud.cer[1] |
| SIGNATURE Algorithm: | Note: We recommend using an SHA-2 algorithm to meet the highest standards of security. |
| EERP | SEEBURGER Cloud always requests **signed EERP** |

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