MBR Gateway Service: SLMP Plus Data Sheet

Technical information to configure your SLMP Plus connection to the SEEBURGER Cloud

Company Details

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

SLMP (Secure Link Management Protocol) is a protocol used for data exchange between SEEBURGER components, for example the communication between SEEBURGER BIS and SEEBURGER Cloud.

A confirmation of delivery / error notification (the „end-to-end response") will be sent for every message that the SEEBURGER Cloud receives via the SLMP Plus (VAN/ASP-Add On) Cloud link as soon as one of the following final states is reached:

- Successful delivery
- Manual download (message receiver only)
- Expiration of the lifetime of the message
- Stop message (message sender only)
- Routing error
- Malicious message content found by Anti-Virus scan
- Other configuration errors (e.g. SLMP is configured on your system and SLMP Plus is configured at the SEEBURGER Cloud)

The activation of SLMP Plus requires a SEEBURGER BIS Solution supporting it.

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.

In general, we want to use TLS/SSL to secure the HTTP connection AND we want data always to be signed and encrypted on SLMP level.

1. SLMP Plus – FIREWALL Configuration

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

FROM: IP address of your SLMP system	**TO:** IP ranges:	85.115.5.64 – 85.115.5.95 and
		85.115.19.120 – 85.115.19.127
	Port:	**443**

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

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

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

2. SLMP Plus – SENDING Data to the SEEBURGER Cloud

Our SLMP Identifier:	SEECLOUDID_MBR
Individual SEEID of the communication partner	e.g. SEEGWE30000001
URL:	https://slmp.seeburger.cloud:443/mbr
Our TLS/SSL certificate:	slmp-ssl.seeburger.cloud.cer[1]
Security Mode:	SLMPv2.0
Certificate Authority (CA):	GlobalSign Root CA
Our ENCRYPTION Certificate:	slmp.seeburger.cloud.cer[1]

Depending on the Seeburger solution, the individual SEEID of the communication partner must be entered in the field provided. This parameter is called 'Receiver ID'.

3. SLMP Plus – RECEIVING Data from the SEEBURGER Cloud

Our SLMP Identifier:	SEECLOUDID_MBR
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 and do not use a static IP as host name.
Security Mode:	SLMPv2.0
Our SIGNATURE Certificate:	slmp.seeburger.cloud.cer[1]

4. SLMP Plus – 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. You send a test message from your system to the SEEBURGER Cloud.
2. The same message will be sent from the SEEBURGER Cloud to your system.
3. We will receive the EERP from your system.

If you do NOT receive our message 5 minutes after starting the test, please check your settings (e.g. firewall).

After successful testing, you will be switched from test to productive mode.

---

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