MaKo Cloud Service: SLMP Data Sheet

Technical information to configure your SLMP 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

SLMP (Secure Link Management Protocol) is a protocol used for data exchange between SEEBURGER components, for example the communication between BIS LINK and Cloud or SEEBURGER BIS and Cloud. To configure your connection to the SEEBURGER Cloud, please use this data sheet we prepared for you.

Depending on the selected operating mode, you need the following information for the configuration:

> SLMP in bidirectional mode:
>
> Your system has a static, public IP address and you open your firewall for this communication. You actively send data from your local system to the SEEBURGER Cloud and allow the SEEBURGER cloud to actively send data to you.
>
> SLMP in polling mode:
>
> Your system does not have a static, public IP address. You send data to the SEEBURGER Cloud and actively request (poll) data from the SEEBURGER Cloud. In polling mode your system will download the data rather than the SEEBURGER Cloud sending it actively.

SLMP – BIDIRECTIONAL Mode

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. The last one contains information you need to **test** your connection.

1. FIREWALL Configuration

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.

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 – SENDING Data to the SEEBURGER Cloud

Our SLMP Identifier:	**Standard identifier:**
	SEECLOUDID_MAKO
	Optimized identifier for Managed Service or iPaaS BIS:
	SEECLOUDID_MAKO_MS
URL:	https://slmp.seeburger.cloud:443/mako
Security Mode:	SLMPv2.0
TLS/SSL certificate:	slmp-ssl.seeburger.cloud.cer[1]
Certificate Authority (CA):	GlobalSign Root CA
ENCRYPTION Certificate:	slmp.seeburger.cloud.cer[1]

Optional: SLMP Plus

Is SLMP Plus (VAN/ASP-Add On) activated for your Cloud Link, a confirmation of delivery / error notification will be sent for every message that the SEEBURGER Cloud receives via that link as soon as one of the following final states is reached:

- Successful delivery
- Manual download
- Expiration of the lifetime of the message
- Routing error
- Malicious message content found by Anti-Virus scan
- Other configuration errors (e.g. if 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.

3. SLMP – RECEIVING Data from the SEEBURGER Cloud

Our SLMP Identifier:	**Standard identifier:**
	SEECLOUDID_MAKO
	Optimized identifier for Managed Service or iPaaS BIS:
	SEECLOUDID_MAKO_MS
Security Mode:	SLMPv2.0
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.
SIGNATURE Certificate:	slmp.seeburger.cloud.cer[1]

4. SLMP – 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.

If you do NOT receive our message 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.

SLMP – POLLING Mode

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 and poll** data to/from the SEEBURGER Cloud. The last one contains information you need to **test** your connection.

1. FIREWALL Configuration

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.

To **SEND and POLL** data to/from 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** |

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

2. SLMP – SENDING and POLLING Data to/from the SEEBURGER Cloud

Our SLMP Identifier:	**Standard identifier:**
	SEECLOUDID_MAKO
	Optimized identifier for Managed Service or iPaaS BIS:
	SEECLOUDID_MAKO_MS
URL:	https://slmp.seeburger.cloud:443/poll/mako
Security Mode:	SLMPv2.0
TLS/SSL certificate:	slmp-ssl.seeburger.cloud.cer[1]
Certificate Authority (CA):	GlobalSign Root CA
ENCRYPTION Certificate:	slmp.seeburger.cloud.cer[1]

3. SLMP – 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 polled by your system from the SEEBURGER Cloud.

If you do NOT receive our message 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.

---

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