



## MaKo Cloud AS4 Service: REST Datenblatt

Konfigurationsdaten der SEEBURGER Cloud für die REST-Anbindung

### Firma

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

### Kontakt

Name:	SEEBURGER Cloud-Service-Team
E-Mail:	support@cloud.seeburger.de
Telefon:	+49 (0)7252 96 1443

Dieses Datenblatt soll Sie bei der Anbindung an die SEEBURGER Cloud unterstützen. Der erste Abschnitt enthält Informationen für Ihre Netzwerk-Administration. Diese Abteilung muss Ihre **Firewall** konfigurieren, damit die HTTPS-Verbindung aufgebaut werden kann.

Der zweite Abschnitt enthält die Konfigurationsdaten, die nötig sind, um Daten an die SEEBURGER Cloud zu **senden**. Der dritte Abschnitt enthält die Konfigurationsdaten, die nötig sind, um Daten von der SEEBURGER Cloud zu **empfangen**. Der letzte Abschnitt beinhaltet Informationen dazu, wie Sie Ihre HTTPS-Verbindung **testen** können.

Bitte beachten Sie: Der REST-Service der SEEBURGER Cloud wird über HTTP/S realisiert. Die Services werden über URL/URI angesprochen. Die HTTP-Methoden geben an, welche Operation ein Dienst ausführen soll. Die HTTP-Methode für die Nachrichtenzustellung ist POST, andere Methoden sind für die zukünftige Verwendung reserviert. HTTP ist eine Verbindung über das Internet. Die SEEBURGER Cloud unterstützt nur HTTP über TLS/SSL. Wir empfehlen die Verwendung von TLS V1.2. Sollte Ihr System TLS/SSL nicht unterstützen, wenden Sie sich bitte an unser SEEBURGER Cloud-Service-Team.

## 1. REST – Konfiguration der FIREWALL

Um Daten an die SEEBURGER Cloud zu **senden**, öffnen Sie bitte Ihre Firewall für folgende ausgehende HTTPS-Verbindungen:

<b>VON:</b> IP-Adresse Ihres HTTPS-Systems	<b>ZU:</b> IP-Range: <b>85.115.5.64</b> – <b>85.115.5.95</b> und <b>85.115.19.120</b> <b>85.115.19.127</b>
	Port: <b>443</b>

Um Daten von der SEEBURGER Cloud zu **empfangen**, öffnen Sie bitte Ihre Firewall für folgende eingehende HTTPS-Verbindungen:

<b>VON:</b> IP-Range: <b>85.115.5.64</b> – <b>85.115.5.95</b> und <b>85.115.19.120</b> <b>85.115.19.127</b>	<b>ZU:</b> IP-Adresse und Port Ihres HTTPS-Systems
--	--

Hinweis: Unsere Firewall ist bereits für den Empfang Ihrer Daten geöffnet.

## 2. REST – Daten an die SEEBURGER Cloud SENDEN

Unsere URL:	<a href="https://rest.makgw.seeburger.cloud/msg">https://rest.makgw.seeburger.cloud/msg</a> mTLS (Two way SSL): <a href="https://rest-ism.makgw.seeburger.cloud/1/msg/routing">https://rest-ism.makgw.seeburger.cloud/1/msg/routing</a>
TLS/SSL-Zertifikat:	rest.makgw.seeburger.cloud.crt <sup>1</sup> rest-ism.makgw.seeburger.cloud.crt <sup>1</sup>

Zertifizierungsstelle (CA):	GlobalSign Root CA				
Authentifizierungsart:	<p>Client-Zertifikat benutzen (Two-way-SSL)</p> <p>Bitte teilen Sie uns ihr Zertifikat über Ihrem SEEBURGER Consultant mit. Two-way-SSL nutzt zusätzlich auch Basic Authentication.</p> <p>Benutzername und Passwort benutzen (Basic Authentication)</p> <table border="1"> <tr> <td>Benutzername:</td> <td><u>Hinweis:</u> Der Benutzer wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.</td> </tr> <tr> <td>Passwort:</td> <td><u>Hinweis:</u> Das Passwort wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.</td> </tr> </table>	Benutzername:	<u>Hinweis:</u> Der Benutzer wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.	Passwort:	<u>Hinweis:</u> Das Passwort wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.
Benutzername:	<u>Hinweis:</u> Der Benutzer wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.				
Passwort:	<u>Hinweis:</u> Das Passwort wird aktuell von ihrem SEEBURGER Consultant zur Verfügung gestellt.				
HTTP-Methode:	POST				
HTTP-Header-Parameter:	<p>Die folgenden HTTP-Header-Parameter sind zu unterstützen: Beim <b>Senden von Nachrichten</b> an die SEEBURGER Cloud:</p> <table border="1"> <tr> <td>Erforderlich:</td> <td><b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication</td> </tr> </table>	Erforderlich:	<b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication		
Erforderlich:	<b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication				

### 3. REST – Daten von der SEEBURGER Cloud EMPFANGEN

Ihre URL:	<p><u>Hinweis:</u> Ihre URL muss mit HTTPS beginnen, die Nutzung von TLS/SSL ist zwingend vorgeschrieben. Bitte geben Sie die vollständige URL an (ggf. einschließlich des SAP-Clients).</p>
Komprimierung:	Keine
Ihr TLS/SSL-Zertifikat:	<p><u>Hinweis:</u> Eine zugelassene Zertifizierungsstelle (CA) sollte Ihr SSL-Zertifikat ausstellen. Nutzen Sie bei der Zertifikatsanforderung bitte den Domännennamen Ihrer URL wie einen gewöhnlichen Namen (CN). Verwenden Sie bitte keine statischen IP-Adressen als Hostnamen.</p>
Unser Zertifikat für die Authentifizierung:	see.mako.cloud.cer <sup>1</sup>
Zertifizierungsstelle (CA):	GlobalSign Root CA

Authentifizierungsart:	<p>- Client-Zertifikat benutzen (Two-way-SSL)  <u>Hinweis:</u> Bitte laden Sie das für die Authentifizierung bestimmte Zertifikat msg-api.authentication.seeburger.cloud.cer in den Zertifikatsspeicher für akzeptierte Client-Zertifikate Ihrer Software.</p> <p>- Benutzername und Passwort benutzen (Basic Authentication)  <u>Hinweis:</u> Bitte achten Sie darauf, dass Sie sichere Benutzernamen und Passwörter verwenden.</p> <table border="1" data-bbox="883 373 1403 449"> <tr> <td>Benutzername:</td> <td>Benutzer Ihres HTTPS-Systems</td> </tr> <tr> <td>Passwort:</td> <td>Passwort Ihres HTTPS-Systems</td> </tr> </table>	Benutzername:	Benutzer Ihres HTTPS-Systems	Passwort:	Passwort Ihres HTTPS-Systems
Benutzername:	Benutzer Ihres HTTPS-Systems				
Passwort:	Passwort Ihres HTTPS-Systems				
HTTP-Methode:	POST				
HTTP-Header-Parameter:	<p>Die folgenden HTTP-Header-Parameter sind zu unterstützen:          Beim <b>Empfangen von Nachrichten</b> aus der SEEBURGER Cloud:</p> <table border="1" data-bbox="883 571 1500 693"> <tr> <td>Erforderlich:</td> <td><b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication (nicht bei Two-way-SSL)</td> </tr> </table>	Erforderlich:	<b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication (nicht bei Two-way-SSL)		
Erforderlich:	<b>Username</b> (Benutzername) und <b>Password</b> (Passwort) im Kopfbereich der Basic Authentication (nicht bei Two-way-SSL)				

Optional: Response-Dokument

Ein Response-Dokument (JSON-Objekt), aus dem hervorgeht, dass der Empfangsstatus vorliegt, sollte hinzugefügt werden. Dafür muss auf Kundenseite eine Schnittstelle bereitgestellt werden. Es gelten die gleichen Verbindungsdetails wie oben beschrieben.

<sup>1</sup>Sie können die Datenblätter und Zertifikate hier herunterladen: <https://www.seeburger.com/de/cloud/connect-the-cloud/>