



PEPPOL Access Service: REST Datenblatt

Konfigurationsdaten der SEEBURGER Cloud für die REST-Anbindung

Company Details

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

Contact Details

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 Ihren Netzwerk-Administrator. Er muss Ihre **Firewall** konfigurieren, damit die HTTPS-Verbindung aufgebaut werden kann.

Der zweite Teil enthält Einstellungen, die Sie konfigurieren müssen, um Daten an die SEEBURGER Cloud zu **senden**. Der dritte Abschnitt enthält die Konfiguration, mit der Sie Daten von der SEEBURGER Cloud **empfangen** 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:

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

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

VON: IP Range: 85.115.5.64 – 85.115.5.95 und 85.115.19.120 – 85.115.19.127	ZU: 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:	https://msg-api.seeburger.cloud:443/peppol/msgs
TLS/SSL-Zertifikat:	http.seeburger.cloud.cer ¹
Zertifizierungsstelle (CA):	GlobalSign Root CA
Authentifizierungsart:	Basic (Benutzername/Passwort)
	Benutzername: <u>Hinweis:</u> In der SEEBURGER Cloud können Sie den Benutzernamen selbst festlegen. Er muss eindeutig sein.

	<p>Neben alphanumerischen Zeichen unterstützen wir Unterstriche.</p> <p><u>Hinweis</u>: Das Passwort wird automatisch generiert, sobald Sie den entsprechenden Button geklickt haben.</p>						
HTTP-Methode:	POST						
HTTP Header Parameter:	<p>Die folgenden HTTP-Header-Parameter sind zu unterstützen: Beim Senden von Nachrichten an die SEEBURGER Cloud</p> <table border="1"> <tr> <td>Erforderlich:</td> <td> <p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication</p> <p>TXID ist die Transaktions-ID für die Duplikatsprüfung (zur eindeutigen Identifizierung der Transaktion)</p> </td> </tr> <tr> <td>Optional:</td> <td> <p>Filename (Dateiname)</p> <p>Subject (Betreff)</p> <p>TTL ist die Message Time to Live in Minuten (für automatischen Ablauf, ersetzt den im B2B Directory definierten Wert für REST Cloudlink)</p> </td> </tr> </table> <p>Für den Empfang eines Response-Dokuments aus der SEEBURGER Cloud (XML (Standardeinstellung) oder JSON-Objekt).</p> <table border="1"> <tr> <td>Erforderlich:</td> <td> <p>HTTP Status mit Statuscodes: 200 OK, 400 Bad Request, 401 Unauthorized, 403 Forbidden,...</p> <p>GMID für die von der SEEBURGER Cloud generierte globale Nachrichten-ID</p> </td> </tr> </table>	Erforderlich:	<p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication</p> <p>TXID ist die Transaktions-ID für die Duplikatsprüfung (zur eindeutigen Identifizierung der Transaktion)</p>	Optional:	<p>Filename (Dateiname)</p> <p>Subject (Betreff)</p> <p>TTL ist die Message Time to Live in Minuten (für automatischen Ablauf, ersetzt den im B2B Directory definierten Wert für REST Cloudlink)</p>	Erforderlich:	<p>HTTP Status mit Statuscodes: 200 OK, 400 Bad Request, 401 Unauthorized, 403 Forbidden,...</p> <p>GMID für die von der SEEBURGER Cloud generierte globale Nachrichten-ID</p>
Erforderlich:	<p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication</p> <p>TXID ist die Transaktions-ID für die Duplikatsprüfung (zur eindeutigen Identifizierung der Transaktion)</p>						
Optional:	<p>Filename (Dateiname)</p> <p>Subject (Betreff)</p> <p>TTL ist die Message Time to Live in Minuten (für automatischen Ablauf, ersetzt den im B2B Directory definierten Wert für REST Cloudlink)</p>						
Erforderlich:	<p>HTTP Status mit Statuscodes: 200 OK, 400 Bad Request, 401 Unauthorized, 403 Forbidden,...</p> <p>GMID für die von der SEEBURGER Cloud generierte globale Nachrichten-ID</p>						

3. REST – Daten von der SEEBURGER Cloud EMPFANGEN

Ihre URL:	<p><u>Hinweis</u>: Ihr URL muss mit HTTPS beginnen, die Nutzung von TLS/SSL ist zwingend.</p> <p>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 als Common Name (CN). Verwenden Sie bitte keine statischen IP-Adressen als Hostnamen.</p>				
Authentifizierungsart:	<p>Basic (Benutzername/Passwort)</p> <p><u>Hinweis</u>: Bitte achten Sie darauf, dass Sie sichere Benutzernamen und Passwörter verwenden.</p> <table border="1"> <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 Empfangen von Nachrichten aus der SEEBURGER Cloud</p> <table border="1"> <tr> <td>Erforderlich:</td> <td> <p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication (nicht bei 2-way-SSL)</p> </td> </tr> </table>	Erforderlich:	<p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication (nicht bei 2-way-SSL)</p>		
Erforderlich:	<p>Username (Benutzername) und Password (Passwort) im Kopfbereich der Basic Authentication (nicht bei 2-way-SSL)</p>				

		<p>TXID ist die vom Sender generierte Transaktions-ID (gibt der Sender keine TXID an, generiert die SEEBURGER Cloud eine globale Nachrichten-ID)</p> <p>GMID ist die globaler Nachrichten-ID, die von der SEEBURGER Cloud generiert wird.</p> <p>Priority (Priorität) mit den Werten Hoch / 1, Mittel / 2, Niedrig / 3, Standardwert ist Mittel / 2.</p> <p>Filename (Dateiname)</p> <p>Subject (Betreff)</p>
	Optional:	
	Für das Senden eines Response-Dokuments an die SEEBURGER Cloud (XML (Standardeinstellung) oder JSON-Objekt).	
	Erforderlich:	<p>HTTP Status mit Statuscode: 200 OK, 400 Bad Request, 401 Unauthorized, 403 Forbidden,...</p> <p>Status mit kurzem Status (ERFOLGREICH, EXPIRED, RECALLED, DATA ERROR,)</p> <p>Status Text enthält Text, der auf Fehler oder Erfolg hinweist.</p>

Optional: Response-Dokument

Ein Response-Dokument (XML (Standardeinstellung) oder JSON-Objekt), aus dem hervorgeht, dass der Empfangsstatus vorliegt, sollte hinzugefügt werden (redundant zum Header).

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