SEEBURGER
BUSINESS INTEGRATION

SEEBURGER CLOUD

MBR Gateway Service: OFTP2 Datenblatt

Konfigurationsdaten der SEEBURGER Cloud für die OFTP2-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 OFTP2-Verbindung aufgebaut werden kann. Der zweite Abschnitt enthält die allgemeinen Einstellungen, die nötig sind, um Daten an die/von der SEEBURGER Cloud zu **senden/empfangen**. Der dritte Abschnitt enthält die Konfigurationsdaten, die nötig sind, um Daten an die SEEBURGER Cloud zu **senden**. Der vierte Abschnitt enthält die Konfigurationsdaten, die nötig sind, um Daten von der SEEBURGER Cloud zu **empfangen**.

Bitte beachten Sie folgende allgemeine Hinweise:

- Wir unterstützen nur OFTP2 über TCP. OFTP über ISDN, X.31 oder VPN unterstützen wir nicht.
- OFTP2-Sicherheitseinstellungen sind aktiviert, das bedeutet:
  - TLS/SSL wird verwendet. Eine Übertragung ohne TLS/SSL ist nicht möglich. Das Serverzertifikat sollte von einer vertrauenswürdigen Zertifizierungsstelle unterzeichnet sein.
  - Die Sitzungsauthentifizierung erfolgt mittels Passwörtern.
  - Die Session-Authentifizierung mit Zertifikaten wird unterstützt. Wenn dies genutzt werden soll, müssen die OFTP2-Zertifikate ausgetauscht werden.
    Die Session-Authentifizierung muss auf beiden Seiten (SEEBURGER Cloud und Partner) aktiviert sein.
  - Die Dateiverschlüsselung (AES-256) wird unterstützt. Wenn dies genutzt werden soll, müssen die OFTP2-Zertifikate ausgetauscht werden.
  - Die Dateisignatur und die EERP-Signatur werden unterstützt. Sie können nur gemeinsam aktiviert oder deaktiviert werden.
    Wenn diese genutzt werden sollen, müssen die OFTP2-Zertifikate für die Dateisignatur und die EERP-Signatur ausgetauscht werden.
    Es sollte der Signaturalgorithmus RSA-SHA256 oder RSA-SHA512 verwendet werden. Wir empfehlen dringend, den SHA-1-Signaturalgorithmus **nicht** zu verwenden.
  - Dateikomprimierung wird unterstützt.
    Hinweis: Eine Komprimierung auf Session-Ebene wird nicht empfohlen, da sie für moderne EDI-Formate sehr ineffektiv ist. Sie wird von der SEEBURGER Cloud nicht verwendet, um Daten an Kunden zu senden.
- Die SEEBURGER Cloud verwendet dasselbe OFTP2-Zertifikat für TLS/SSL, Verschlüsselung, Signatur, Session-Authentifizierung und Dateiebene.
- OFTP2 **Change Direction** wird nicht unterstützt. Nur Initiierende der OFTP2-Session dürfen Dateien versenden. Dem Partner ist es nicht erlaubt, Dateien in derselben Session zurückzusenden. Damit Sie Dateien von Ihrem Partner empfangen können, muss dieser eine eigene Session initiieren.

1. OFTP2– Konfiguration der FIREWALL

Um Daten an die SEEBURGER Cloud zu **senden**, öffnen Sie bitte Ihre Firewall für folgende ausgehende OFTP2-Verbindungen:

VON:	IP-Adresse Ihres OFTP2-Systems	**ZU:**	IP Range:	**85.115.5.64** – **85.115.5.95** und **85.115.19.120** – **85.115.19.127**	
			Port:	**6619**	

Um Daten von der SEEBURGER Cloud zu **empfangen**, öffnen Sie bitte Ihre Firewall für folgende eingehende OFTP2-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 OFTP2-Systems		

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

2. OFTP2 – Allgemeine Einstellungen für das SENDEN/EMPFANGEN von Daten

Unsere SSID:	O0013000031SEE30532CL03
Unser Passwort:	SEEBUR
Unser TLS/SSL-Zertifikat:	oftp2.seeburger.cloud.cer[1]
Unser Zertifikat für die Session-Authentifizierung:	oftp2.seeburger.cloud.cer[1]
SFID:	Individuelle SFID Ihres Kommunikationspartners auf dem SEEBURGER MBR Gateway
Unser Verschlüsselungszertifikat (Dateiverschlüsselung):	oftp2.seeburger.cloud.cer[1]
Unser Signaturzertifikat (Datei- und EERP-Signatur):	oftp2.seeburger.cloud.cer[1]

3. OFTP2 – Daten an die SEEBURGER Cloud SENDEN

URL:	oftp2.seeburger.cloud
Port:	6619
Komprimierung:	Die Dateikomprimierung auf Senderseite kann aktiviert werden. Hinweis: Die Komprimierung auf Session-Ebene wird nicht empfohlen, da sie für moderne EDI-Formate sehr ineffektiv ist.
Zertifizierungsstelle (CA):	Odette CA
Signaturalgorithmus (Datei- und EERP-Signatur):	Keine, RSA-SHA256, RSA-SHA512, SHA-1 Hinweis: Wir empfehlen RSA-SHA256 oder RSA-SHA512 zu verwenden, um den höchsten Sicherheitsstandard erfüllen zu können. Hinweis: Datei- und EERP-Signatur werden gemeinsam aktiviert / deaktiviert.
Verschlüsselungsalgorithmus (Dateiverschlüsselung):	Keine, AES-256, 3DES
EERP	Sobald die SEEBURGER Cloud eine Nachricht erfolgreich an den Empfänger zugestellt werden konnte, wird eine EERP generiert und **signiert** an den Sender verschickt. Hinweis: Die SEEBURGER Cloud unterstützt das Zurücksenden von EERP unmittelbar nach Erhalt der Nachricht. Dies wird nicht empfohlen, kann aber in einigen seltenen Fällen erforderlich sein.

4. OFTP2 – Daten von der SEEBURGER Cloud EMPFANGEN

	Hinweis: Die EERP-Signatur kann zusammen mit der Dateisignatur deaktiviert werden.
Komprimierung:	Keine Hinweis: Die Dateikomprimierung kann bei Bedarf aktiviert werden. Hinweis: Eine Komprimierung auf Session-Ebene wird nicht empfohlen, da sie für moderne EDI-Formate sehr ineffektiv ist.
Ihr TLS/SSL-Zertifikat:	Hinweis: Eine zugelassene Zertifizierungsstelle (CA) sollte Ihr SSL-Zertifikat ausstellen. Nutzen Sie bei der Zertifikatsanforderung bitte den Domänennamen Ihrer URL wie einen gewöhnlichen Namen (CN). Verwenden Sie bitte keine statischen IP-Adressen als Hostnamen. Hinweis: Die Option „Zertifizierungsstellenbasiert für TLS“ kann verwendet werden, anstatt ein spezielles Zertifikat zu konfigurieren, welches regelmäßig ersetzt werden muss. Die SEEBURGER Cloud wird das Zertifikat, welches von dem für diese Verbindung konfigurierten Server vorgelegt wurde, mit einer Liste vertrauenswürdiger Stammzertifikate verglichen. Des Weiteren wird dieses vom Server vorgelegte Zertifikat mit dem Servernamen abgeglichen, um sicherzustellen, dass die Verbindung zum richtigen Server hergestellt wird.
Verschlüsselungsalgorithmus (Dateiverschlüsselung):	Keine, AES-256, 3DES
Signaturalgorithmus (Datei- und EERP-Signatur):	SHA-1, RSA-SHA256 and RSA-SHA512 Hinweis: Wir empfehlen RSA-SHA256 oder RSA-SHA512 zu verwenden, um den höchsten Sicherheitsstandard erfüllen zu können. Hinweis: Datei- und EERP-Signatur können gemeinsam deaktiviert werden.
EERP	Normalerweise wartet die SEEBURGER Cloud auf die EERP eines signierten Partners, bevor sie eine positive Bestätigung an den Sender der ursprünglichen Nachricht zurückschickt. Hinweis: Die Standarddauer für die Wartezeit, während die SEEBURGER Cloud auf die EERP des Partners wartet, beträgt 2 Stunden. Der Maximalwert für diese Einstellung beträgt 24 Stunden. Hinweis: Die Deaktivierung dieses Standardverhaltens wird nicht empfohlen, kann aber in einigen seltenen Fällen erforderlich sein.

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