



MBR Gateway Service: SFTP Datenblatt

Konfigurationsdaten der SEEBURGER Cloud für die SFTP-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 Ihren Netzwerk-Administrator. Er muss Ihre **Firewall** konfigurieren, damit die Verbindung für SFTP 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: Für das Senden und Empfangen von Daten stellt die SEEBURGER Cloud einen SFTP-Server zur Verfügung. SFTP nutzt die Secure Shell (SSH) zur Authentifizierung. Sollte Ihr File-Transfer-Client SSH nicht unterstützen, wenden Sie sich bitte an unser SEEBURGER Cloud Service Team.

1. SFTP – Konfiguration der FIREWALL

Um Daten an die SEEBURGER Cloud zu **senden** und zu **empfangen**, öffnen Sie bitte Ihre Firewall für folgende Verbindungen:

VON: IP-Adresse Ihres SFTP-Clients	ZU: IP-Range: 85.115.5.64 – 85.115.5.95 und 85.115.19.120 – 85.115.19.127
	Port: 1322

Hinweis: Unsere Firewall ist bereits für Sie geöffnet.

2. SFTP – Daten an die SEEBURGER Cloud SENDEN

SEEBURGER Hostname:	Ihr eigenes System verwendet diesen Hostname, um Dateien an die SEEBURGER-Cloud zu senden. sftp.seeburger.cloud
SEEBURGERs öffentlicher SSH-Schlüssel:	sftp.seeburger.cloud.cer ¹
Ihr öffentlicher SSH-Schlüssel ² :	Dieser Parameter ist für die Authentifizierung der Verbindung mit dem SEEBURGER SFTP Server erforderlich. Der Schlüssel kann vom Typ DSA / RSA sein, seine minimale Schlüssellänge beträgt 2048 Bit.
SFTP Benutzer:	Der Benutzername wird von der SEEBURGER-Cloud generiert. Er besteht in der Regel aus 6 alphabetischen und 9 numerischen Zeichen, z.B. SEEGWE30000001
Passwort:	Dieses Passwort wird von Ihrem lokalen System zur Authentifizierung für die Dateiübertragung mit der SEEBURGER-Cloud verwendet (zusätzlich zum öffentlichen SSH-Schlüssel). Das Passwort darf nicht leer sein.

Ihr Verzeichnis für ausgehende Daten:

Legen Sie die Daten, die Sie senden möchten, in dieses Verzeichnis:
\< Kurzname des Services >\outbox\[SEEID des Partners], z.B.:
Meta Based Routing: | \mbr\outbox\SEEGWE31111111
(Dieser Verzeichnisname entspricht der Kennung des Empfängers, an den die Nachrichten gesendet werden.)

3. SFTP – Daten von der SEEBURGER Cloud EMPFANGEN

Hinweis: Sie können alle Dateien im Posteingang mehrfach lesen. Um das Lesen der Dateien zu bestätigen, löschen Sie sie. Andernfalls bleiben sie in Ihrem Eingangsverzeichnis liegen.

SEEBURGER Hostname:

Ihr eigenes System verwendet diesen Hostname, um Dateien an die SEEBURGER-Cloud zu senden.

sftp.seeburger.cloud

SEEBURGERs öffentlicher SSH-Schlüssel:

sftp.seeburger.cloud.cer¹

Ihr öffentlicher SSH-Schlüssel ²:

Dieser Parameter ist für die Authentifizierung der Verbindung mit dem SEEBURGER SFTP Server erforderlich. Der Schlüssel kann vom Typ DSA / RSA sein, seine minimale Schlüssellänge beträgt 2048 Bit.

SFTP Benutzer:

Der Benutzername wird von der SEEBURGER-Cloud generiert. Er besteht in der Regel aus 6 alphabetischen und 9 numerischen Zeichen, z.B. SEEGWE30000001

Passwort:

Dieses Passwort wird von Ihrem lokalen System zur Authentifizierung für die Dateiübertragung mit der SEEBURGER-Cloud verwendet (zusätzlich zum öffentlichen SSH-Schlüssel). Das Passwort darf nicht leer sein.

Ihr Verzeichnis für eingehende Daten :

Die Daten, die Sie empfangen, finden Sie in diesem Verzeichnis:
\< Kurzname des Services >\inbox\[SEEID des Partners], z.B.:

Meta Based Routing: | \mbr\inbox\SEEGWE31111111

(Dieser Verzeichnisname entspricht der Kennung des Absenders, der die Nachrichten gesendet hat.)

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

² Wenn Sie Probleme bei der Erstellung des öffentlichen SSH-Schlüssels haben, finden Sie im Anhang Hilfe.

ANHANG – SSH PUBLIC KEY Erstellung mit PuTTYgen

Eines der Werkzeuge, mit denen Sie ein SSH-Schlüsselpaar für die Authentifizierung Ihres Benutzers erzeugen können, ist PuTTYgen. Es gibt weitere, Einzelheiten entnehmen Sie bitte deren Dokumentation. Der folgende Text skizziert am Beispiel von PuTTYgen den Prozess der Erstellung von

- Einem privaten Schlüssel (zur Verwendung in Ihrem SFTP-Client) und
- Einem öffentlichen Schlüssel (für den Upload in die SEEBURGER Cloud, zur Verwendung im SFTP-Server).

Zuerst müssen Sie das kostenlose Tool PuTTY installieren. Anschließend können Sie mit der Erstellung des öffentlichen Diese kostenlose Software ist im Internet leicht zugänglich:

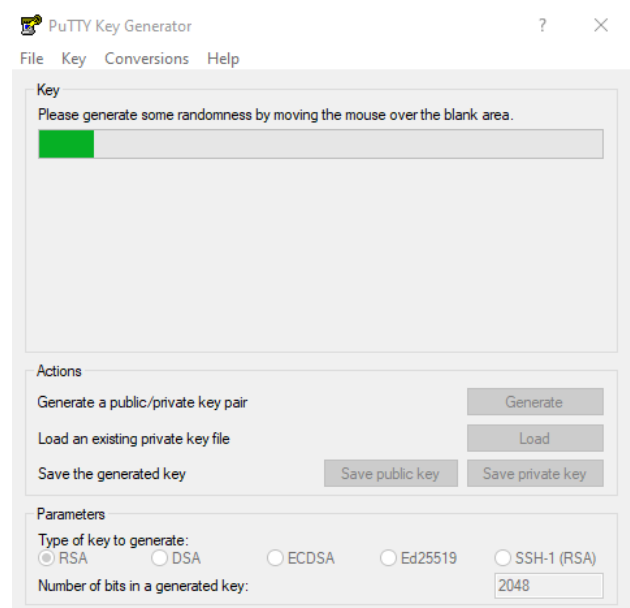
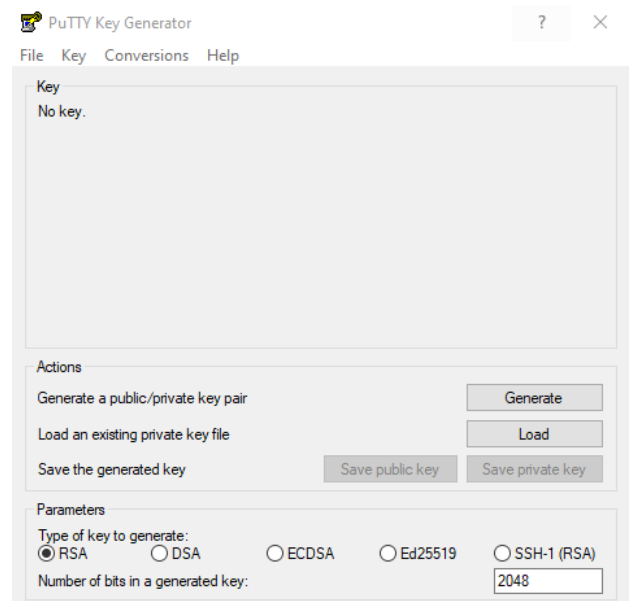
Stellen Sie nun die erforderlichen Parameter in der PuTTYgen-Oberfläche ein. Um einen Schlüssel zu erstellen, sind folgende Parameter erforderlich:

RSA oder DSA und eine minimale Schlüssellänge von 2048 bit, klicken Sie dann den **Generate** Button.

PuTTY generiert jetzt den Schlüssel.

Für den Zufallsgenerator **bewegen Sie die Maus über den Bereich unter dem Balken, bis die Erstellung abgeschlossen ist.**

Link: <https://www.puttygen.com/>



Bitte nutzen Sie das Feld **Key comment** für eine aussagekräftige Beschreibung und das Feld **Key passphrase** um den privaten Schlüssel mit Passwort zu speichern.

Klicken Sie **Save Public Key** um den öffentlichen Schlüssel zu speichern.

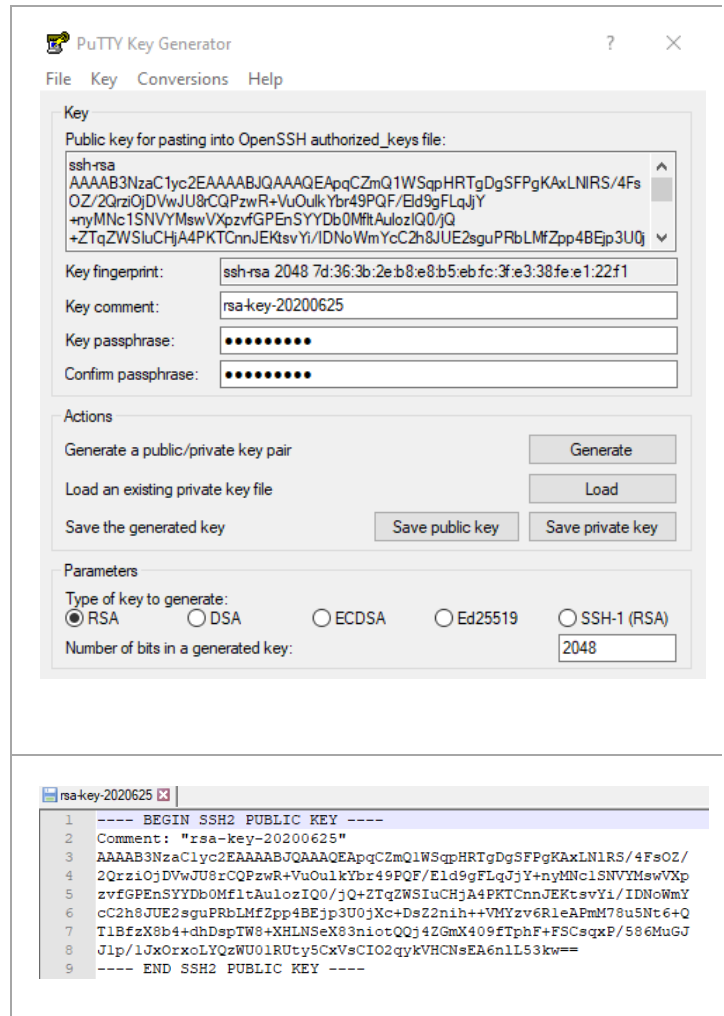
Klicken Sie **Save Private Key** um auch den privaten Schlüssel zu speichern.

Legen Sie das Schlüsselpaar in einem Ordner ab und achten Sie darauf, beiden Schlüsseln aussagekräftige Dateinamen zu geben.

Sie haben nun ein Schlüsselpaar generiert und können es für den Seeburger SFTP Cloudlink verwenden.

Den gespeicherten öffentlichen Schlüssel können Sie mit jedem beliebigen Windows-Editor öffnen.

Kopieren Sie den gesamten Inhalt in das Textfeld "SSH Public Key" in der Seeburger SFTP-Cloudlink-Konfiguration.



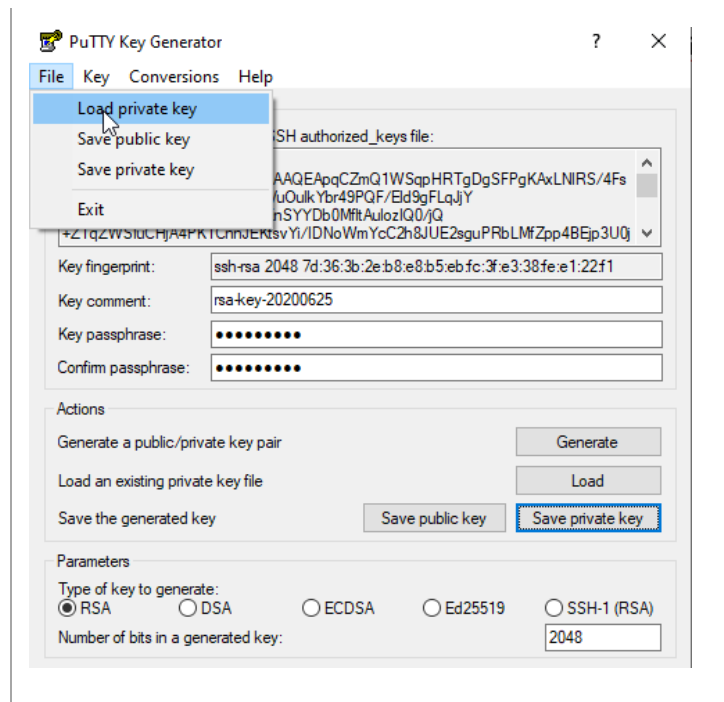
Hinweis:

Nicht alle Schnittstellen-Management-Systeme unterstützen das von PuTTYgen generierte private Schlüsselformat .ppk. Sie haben jedoch die Möglichkeit, Ihren privaten Schlüssel in ein anderes Format (.pem) zu konvertieren. Auch für diese Konvertierung können Sie PuTTYgen verwenden.

Starten Sie PuTTYgen.

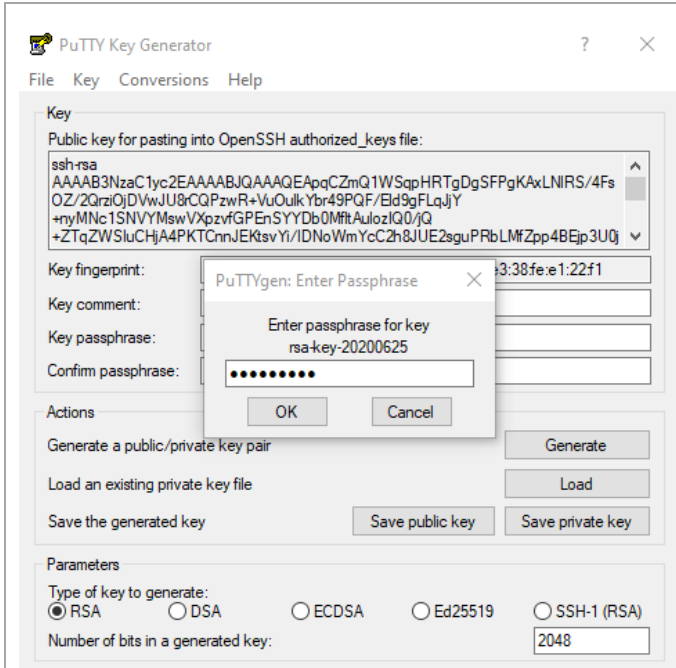
Wählen Sie zuerst **File** und dann **Load private key** aus.

Navigieren Sie zu Ihrer .ppk-Datei, wählen Sie sie aus und öffnen Sie sie.



Es wird ein Dialog geöffnet. Das erwartete **passphrase for key** ist derjenige, den Sie bei der Erstellung Ihres privaten Schlüssels eingegeben haben.

Geben Sie Ihre Passphrase ein und klicken Sie auf **OK**.



Ihr privater Schlüssel wird jetzt geöffnet.

Gehen Sie zu **Conversion** und wählen Sie **Export OpenSSH Key**.

Geben Sie den Namen der Datei ein, z.B. "rsa-key-2020625.pem". Stellen Sie sicher, dass .pem die Endung Ihres Dateinamens ist.

Klicken Sie auf **Save**. Nun können Sie diese *.pem-Datei für den Import in Ihr Schnittstellen-Management-System verwenden.

