co.met GmbH
Hohenzollernstraße 75
66117 Saarbrücken
www.co-met.info

Anleitung zur Erstellung eines Certificate Signing Requests

Version	1.1		
Geltungsbereich	Smart Energy Network (SEN)		
Klassifizierung	Intern		
Dokumenteneigner	Daniel Grob		
Genehmiger	Natalia Götz		
Verteiler	co.met und definierte Dritte		
Dokumentenstatus	Freigegeben		
Dokumententyp	Dokument (DOK)		
Autor/OE/FIRMA	Daniel Grob	C7	co.met
Gültig ab	21.02.2019		
Ersetzt Dokument			

Änderungshistorie

Versionsnummer	Datum der Änderung	Autor/OE/FIRMA	Beschreibung der Änderung
0.1	20.02.2019	DG/C7/co.met	Erstellung des Dokumentes
0.2	02.05.2019	DG/C7/co.met	Überarbeitungen Anträge
1.1	20.05.2019	DG/C7/co.met	Überarbeitung und Ergänzung

Prüfung- und Freigabe-Historie

Versionsnummer	Datum der Prüfung Datum der Freigabe	Prüfer Name/OE/Firma/Signatur	Genehmiger Name/OE/Firma/Signatur
1.0	20.02.2019	NG/co.met	NG/co.met
2.0	20.05.2019	NG/co.met	NG/co.met

Inhalt

1. Einleitung

Für die Schnittstellenanbindung an die SEN-Cloud wird ein Schnittstellenzertifikat benötigt. Entweder hält der Kunde ein von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat vor oder er beantragt ein Zertifikat bei der co.met GmbH. In dieser Anleitung wird beschrieben, wie das Zertifikat von der co.met beantragt wird. Der Generierungsprozess des Zertifikatsantrags wird einmal für Windows und einmal für Linux beschrieben.

Beachten Sie bitte das jeweils ein Antrag für das Produktiv- und einer für das Testsystem benötigt wird.

2. Certificate Signing Request (CSR) mit Linux erstellen

Den CSR erstellen Sie in **OpenSSL**. Um die Zertifikate übersichtlich speichern zu können, legen Sie einen **Ordner mit Namen *ssl*** im **Hauptordner */etc*** an, und arbeiten auch weiterhin in diesem neuen Ordner:

```
mkdir /etc/ssl/test.de && cd /etc/ssl/test.de
```

Nun befinden Sie sich in dem neu angelegten Ordner. Mithilfe der folgenden Befehlszeile starten Sie OpenSSL und erstellen Sie einen privaten Schlüssel von **2048 Bit**:

```
openssl genrsa -out test.de.key 2048
```

Der private Schlüssel dient zur Entschlüsselung der mit dem Zertifikat verschlüsselten Kommunikation und zur Signierung der Kommunikation. Deshalb darf zu ihm eine unbefugte Person **keinen Zugang** erhalten. Sie als Inhaber stellen den Webserver ein, der mit dem privaten Schlüssel arbeiten wird:

```
chmod 600 test.de.key
chown www-data test.de.key
```

2.1. Verwenden einer öffentlich erreichbaren Adresse

Den Zertifikatsantrag für eine öffentlich erreichbare Adresse erstellen Sie nun mithilfe der folgenden Befehlszeile:

```
openssl req -new -key test.de.key -out test.de.csr
```

Sie werden aufgefordert, die folgenden Angaben für den Schlüssel und das zukünftige Zertifikat einzutragen. Beachten Sie die folgenden Hinweise:

Benutzen Sie im Feld Common Name einen öffentlich validierbaren DNS-Eintrag, so tragen Sie diesen hier ein. Handelt es sich um eine private IP-Adresse, so ist eine DNS-Auflösung nicht möglich. Tragen Sie dann bitte die IP-Adresse ein.

Country Name (2 letter code) []: Name des Landes mit großen Buchstaben nach der ISO-Norm, z.B. DE
State or Province Name (full name) []:Name des Bundeslandes, z.B. SL für das Saarland
Locality Name (eg, city) []: Stadt des Firmensitzes. Zum Beispiel Saarbrücken
Organization Name (eg, company) []: Name der Organisation, welche das Zertifikat beantragt
Organizational Unit Name (eg, section) []: Name der Organisationseinheit oder Abteilung
Common Name (eg, YOUR name) []: Die wichtigste Angabe - die Domain, für welche das Zertifikat ausgestellt wird
Email Adresse []: Die E-Mailadresse - wird nicht zwingend benötigt

Es folgen noch zwei weitere Attribute, welche nur mit Enter bestätigt werden:
A challenge password []:
An optional company name []:

Um den nun erstellten CSR (Certificate Signing Request) an die co.met senden zu können, öffnen Sie den CSR in dem nano-Editor, wählen den kompletten Text aus und kopieren diesen:

```
nano test.de.csr
```

Mit dem Befehl „Strg+X“ kehren Sie in das Terminal zurück.

Den kopierten Text fügen Sie in Ihrer Mail zur Beantragung des SSL-Zertifikats ein und senden diese per S/MIME an sen@sen-cloud.de .

2.2. Verwenden einer internen IP-Adresse

Möchten Sie eine interne IP-Adresse verwenden, fügen Sie diese im Feld Subject Alternative Name des CSR ein. Hierzu ist ein anderes Vorgehen notwendig, wie hier beispielhaft dargestellt. Führen Sie den folgenden Befehl aus, um die Datei reg.conf zu erstellen:

```
touch req.conf
```

Öffnen Sie die erstellte Datei „reg.conf“ mit dem nano-Editor und tragen Sie hier folgenden Inhalt in die Datei ein (Erklärung der Parameter siehe oben, passen Sie die *kursiv* geschriebenen Teile an. Benötigen Sie mehr oder weniger alternative Namen, so fügen Sie diese fortlaufend als DNS.X ein bzw. entfernen diese. Benötigen Sie nur eine IP-Adresse, tragen Sie diese direkt im Feld „subjectAltName“ ein.):

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
```

C = DE
ST = *SL*
L = *Saarbrücken*
O = *Name der Organisation, welche das Zertifikat beantragt*
OU = *Name der Organisationseinheit oder Abteilung*
CN = *Die wichtigste Angabe - die Domain, für welche das Zertifikat ausgestellt wird*
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = *www.ihre-firma.de*
DNS.2 = *ihre-firma.de*
IP.1 = *192.168.1.1*

Mit dem Befehl „Strg+O“ speichern Sie die Datei und mit „Strg+X“ kehren Sie in das Terminal zurück.

Den Zertifikatsantrag erstellen Sie nun mithilfe der folgenden Befehlszeile:

```
openssl req -new -key test.de.key -out test.de.csr -config req.conf
```

Um den nun erstellten CSR (Certificate Signing Request) an die co.met senden zu können, öffnen Sie den CSR in dem nano-Editor, wählen den kompletten Text aus und kopieren diesen:

```
nano test.de.csr
```

Mit dem Befehl „Strg+X“ kehren Sie in das Terminal zurück.

Den kopierten Text fügen Sie in Ihrer Mail zur Beantragung des SSL-Zertifikats ein und senden diese per S/MIME an sen@sen-cloud.de .

3. CSR am Beispiel des IIS 7.0 mit Windows erstellen

1. Öffnen Sie **Internet Information Services** (IIS).

- Klicken Sie auf Start.
- Wählen Sie Verwaltung.
- Starten Sie den Internet Services Manager.

2. Klicken Sie auf **Server-Name.**

3. In dem mittleren Menü doppelklicken Sie auf die Schaltfläche **Server-Zertifikate** im Abschnitt **Sicherheit.**

4. Wählen Sie Menü "Aktionen" (rechts) und klicken Sie auf **Zertifikatsanforderung erstellen**.

5. Der Anfrage-Assistent wird geöffnet.

6. In dem **Distinguished Name-Fenster** geben Sie die Informationen wie folgt ein:

- Das Common Name Feld sollte die Web-Adresse, bzw. IP-Adresse für Ihr SSL-Zertifikat enthalten.
- Geben Sie den Namen Ihrer Firma und Abteilung in die dafür vorgesehenen Felder ein.
- Geben Sie Ihre Stadt/Filiale, Bundesland/Kanton und Land/Region Details ein.
- Und klicken Sie auf Weiter.

7. In dem "Cryptographic Service Provider Properties"-Fenster lassen Sie bei den Einstellungen die Standardwerte (Microsoft RSA SChannel und 2048) stehen und klicken Sie auf **Weiter.**

8. Geben Sie einen Dateinamen und Speicherort für Ihren CSR ein.

Die soeben erstellte Datei fügen Sie in Ihrer Mail zur Beantragung des SSL-Zertifikats ein und senden diese per S/MIME an sen@sen-cloud.de .

4. Folgezertifikat beantragen

Die bereitgestellten Zertifikate sind zwei Jahre gültig. Die Gültigkeitsdauer muss vom Zertifikatsinhaber selbst überwacht werden. Läuft das Zertifikat aus und wird ein neues Zertifikat benötigt, muss das neue Zertifikat, wie in den vorherigen Kapiteln beschrieben, erneut angefordert werden.

5. Zertifikat überprüfen

Um sicherzustellen, dass das unter Punkt 2 bzw. 3 erstellte Zertifikat korrekt erstellt wurde, empfiehlt sich dieses vor Versand zu überprüfen, um unnötige Wartezeit durch ein Ausstellen einer korrigierten Version zu vermeiden. Hierzu kann ein Prüftool wie z.B. https://ssl.de/csr-check.html genutzt werden. Dort wird der erstellte CSR hineinkopiert und mittels eines Klicks auf den Button „CSR Check“ überprüft. In der angezeigten Zusammenfassung bitte die Werte überprüfen und danach, wie oben beschrieben, an co.met senden.

6. Wie geht es weiter?

Nach der Ausstellung des Zertifikates senden wir dieses per Email an Sie als Einsender des CSR.

Hinweis: Im SEN-Support-Portal https://support.sen-cloud.de/SEN-PKI/SitePages/Homepage.aspx können Sie sich die offiziellen Zertifikate herunterladen, falls wegen Ihrer Netzkonfiguration kein Abruf per Internet möglich ist.

Sie importieren nun das ausgestellte Zertifikat auf Ihrer Seite und führen den Import der Serverzertifikate der Gegenstelle (=EMT-System in Saarbrücken) in Ihre Webserverkonfiguration durch.