Serverzertifikat beantragen

Der folgende Abschnitt ist gedacht als Anleitung für Server-Administratoren, die eine abgesicherte Verbindung zu Ihrem Server einrichten wollen und dafür ein SSL-Zertifikat benötigen.

Zertifikatsrequest erstellen

Voraussetzung für ein Serverzertifikat ist ein Zertifikatsrequest. Im ersten Schritt wird also eine Datei für den Request und ein privater Schlüssel erzeugt.

In allen Beispiel-Kommandos können/sollen die hervorgehobenen Teile durch eigene Namen sinnvoll ersetzt werden!

Methode 1: openssl

Verwenden Sie diese Methode, wenn Sie

- selten Serverzertifikate benötigen
- nicht mehrere DNS-Namen im Zertifikate benötigen
- Voraussetzung ist das open-source-tool openssl und eine Kommandozeile

Erzeugen Sie einen Zertifizierungs-Request (**web.pem**) und den dazugehörigen privaten Schlüssel (**web.key**):

```
openssl req -newkey rsa:4096 -out web.pem -keyout web.key
```

Geben Sie, wenn Sie danach gefragt werden, die folgenden Daten ein (Beispiel! alles ändern, wo die Zeichenkette "ihr" drin vorkommt):

```
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Sachsen-Anhalt
Locality Name (eg, city) []:Magdeburg bzw. Stendal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hochschule Magdeburg-Stendal
Organizational Unit Name (eg, section) []:Ihr Fachbereich
Common Name (eg, YOUR name) []:ihr.server.h2.de
Email Address []:ihre.adresse@h2.de
```

Verwenden Sie für Server- und Email-Adressen bitte nur Kleinbuchstaben.

Der erzeugte private Schlüssel ist mit der von Ihnen eingegebenen Passphrase verschlüsselt. Dieser Schlüssel ist bei jeder Verwendung des privaten Schlüssels anzugeben. Wenn man dies vermeiden will (z.B. sollen Webserver automatisch starten ohne die Notwendigkeit, ein Passwort einzugeben), dann kann die Verschlüsselung des privaten Schlüssels aufgehoben werden:

```
openssl rsa -in web.key -out server.key
```

Der private Schlüssel **server.key** kann jetzt ohne Passwort benutzt werden.

Methode 2: openssl mit Konfigurationsdatei

Verwenden Sie diese Methode, wenn Sie

- häufig Zertifikatsanträge stellen müssen mit gleichen Angaben bei der Generierung des Requests
- Zertifikate mit mehreren DNS-Namen benötigen
- Voraussetzung ist das open-source-tool openssl und eine Kommandozeile.

Erstellen Sie eine Datei req.conf mit folgendem Inhalt (Beispiel! alles ändern, wo die Zeichenkette "ihr" drin vorkommt):

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

[req_distinguished_name]
C = DE
ST = Sachsen-Anhalt
L = Magdeburg
O = Hochschule Magdeburg-Stendal
OU = Ihr Bereich
CN = ihr.server.h2.de
emailAddress =ihre.adresse@h2.de

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = ihr.server.h2.de
DNS.2 = ihr.server.hs-magdeburg.de
DNS.3 = www.ihr.server.h2.de
...
```

Verwenden Sie für Server- und Email-Adressen bitte nur Kleinbuchstaben.

Erzeugen Sie einen Zertifizierungs-Request (**web.pem**) und den dazugehörigen privaten Schlüssel (**web.key**):

```
openssl req -newkey rsa:4096 -out web.pem -keyout web.key -config ./req.conf
```

Der erzeugte private Schlüssel ist mit der von Ihnen eingegebenen Passphrase verschlüsselt. Dieser Schlüssel ist bei jeder Verwendung des privaten Schlüssels anzugeben. Wenn man dies vermeiden will (z.B. sollen Webserver automatisch starten ohne die Notwendigkeit, ein Passwort einzugeben), dann kann die Verschlüsselung des privaten Schlüssels aufgehoben werden:

```
openssl rsa -in web.key -out server.key
```

Der private Schlüssel **server.key** kann jetzt ohne Passwort benutzt werden.

Der private Schlüssel verbleibt bei Ihnen, der Zertifizierungsrequest (im Beispiel oben die Datei web.pem) wird im nächsten Schritt für den Antrag benötigt.

Zertifikatsrequest einreichen

- Öffnen Sie die Webseite https://cert-manager.com/customer/DFN/ssl/sslsaml
- Wählen Sie den Identity-Provider "Your Instituion" und dort die Hochschule Magdeburg-Stendal (Magdeburg-Stendal University of Applied Sience) (Tipp: wenn Sie suchen, suchen Sie nach "Magdeburg-Stendal")
- Authentifizieren Sie sich mit Ihren Hochschul-Accountdaten
- Bestätigen Sie die zu übermittelnden Daten. Sie gelangen direkt zur Eingabe des Zertifikatrequest (wenn Sie Ihr erstes Zertifikat beantragen) oder erhalten eine Übersicht aller von Ihnen im "sectigo certificate manager" verwalteten Zertifikate.
- Wählen Sie die Schaltfläche "Enrol Certificate" (nur nötig, wenn Sie in der Liste der verwalteten Zertifikate sind)
- Wählen Sie unter "Select Enrollment Account" "Serverzertifizierung Hochschule Magdeburg-Stendal" und bestätigen Sie mit "Next"
- Zertifikatsprofil und Gültigkeitsdauer können nicht geändert werden. Laut Sectigo brauchen keine spezielleren Profile ("Webserver", "Radius", ...) gewählt werden.
- Laden Sie mit "Upload CSR" ihren im ersten Schritt erstellten Zertifikatsrequest (im Beispiel oben die Datei web.pem) hoch.
- Ihre im CSR angegebenen Daten werden angezeigt. Wenn weitere "Altenative Names" benötigt werden, können diese mit Komma getrennt im Feld "Subject Alternative Names" angegeben werden.
- Im Feld "External Requester" können mit Komma getrennt E-Mail-Adressen angegeben werden, die über die Beantragung per E-Mail unterrichtet werden sollen (z.B. "ra@hs-magdeburg.de")
- Mit "Auto renew" legen Sie fest, ob und wieviele Tage im Voraus Sie über den Ablauf des Zertifikates per E-Mail informiert werden wollen.
- Formular abschicken!

Im Anschluss erhalten Sie eine E-Mail, sobald Ihr Request von einem Administrator bestätigt wurde und eine weitere mit Downloadlinks, wo Sie sich das Zertifikat in dem von Ihnen benötigten Format herunterladen können.

Und wenn Sie sich fragen: War das jetzt schon alles? Kein Papierkram?

Ja, es sind hiermit keine Formulare mehr notwendig!