Lokale Zertifizierungsstelle (CA - certificate authority) erstellen

Wenn TLS verschlüsselte Webseiten ausschließlich in einer lokalen Netzwerkumgebung (Intranet) betrieben werden, können mit Hilfe einer lokalen Zertifizierungsstelle eigene Zertifikate erstellt werden.

Die Zertifizierungsstelle dient zum Erstellen des Stamm-Zertifikats welches die Gültigkeit der untergeordneten, selbst erstellten Serverzertifikate bestätigt.

Das Root-Zertifikat der Zertifizierungsstelle wird im Zertifikatsspeicher unter „***Vertrauenswürdige Stammzertifizierungsstellen***“ gespeichert.

Alle mit dem privaten Schlüssel dieses Stamm-Zertifikats signierten Zertifikate werden dann von den Browsern als vertrauenswürdig angesehen.

In diesem Beitrag geht es ausschließlich um das Erstellen der lokalen Zertifizierungsstelle unter Linux, des privaten Schlüssels und des Stamm-Zertifikats.

Das Signieren eines Zertifikats, für einen Webserver, mit Hilfe dieser Zertifizierungsstelle wird hier beschrieben.

Erstellen eines privaten Schlüssels

Ein Verzeichnis erstellen wo der private Schlüssel und das Zertifikat ablegt wird:

```
mkdir CA
```

Die Berechtigungen des Verzeichnisses ändern:

```
chmod 700 CA/
```

In das Verzeichnis wechseln:

```
cd CA
```

Den privaten Schlüssel, geschützt mit einem sicheren Passwort, generieren:

```
openssl genrsa -des3 -out ca-testfirma.key 4096
```

> Jeder, der den Schlüssel besitzt kann damit Zertifikate erstellen!

Die Berechtigung es Schlüssels ändern:

```
chmod 500 ca-testfirma.key
```

> Den privaten Schlüssel benötigt man zum Signieren von selbst erstellten Zertifikaten. Es wird daher dringend empfohlen ein externes Backup des privaten Schlüssels aufzubewahren und dieses natürlich vor unbefugtem Zugriff zu schützen!

Erstellen des Stamm-Zertifikats

Als nächstes wird das Stamm-Zertifikat (Root Certificate) erstellt, dass die Gültigkeit aller untergeordneten Serverzertifikate über einen langen Zeitraum bestätigen soll.

Daher wird ein Ablaufdatum weit in der Zukunft gewählt, in diesem Fall 7300 Tage also 20 Jahre.

Zum Erstellen des Zertifikats wird das Passwort des privaten Schlüssels und folgende Informationen für das Zertifikat benötigt:

– County Code – Ländercode nach ISO-3166-1 ALPHA-2
– State or Province Name – Bundesland
– Locality Name – Ortsnamen
– Organization Name – Firmenname / Organisationsbezeichnung
– Organizational Unit Name – Abteilungsname
– Common Name – Zertifikatsname
– Email Address

Der Zertifikatsname (Common Name) ist der Name des Zertifikats welcher später auch im Zertifikatsspeicher angezeigt wird.

Bis auf das Pflichtfeld „Country Code“ könnten alle Felder leer gelassen werden, auf Grund der Überprüfbarkeit des Zertifikats wird jedoch dringend empfohlen sie auszufüllen.

```
openssl req -new -x509 -days 7300 -key ca-testfirma.key -out ca-testfirma.pem
```

> Das Stamm-Zertifikat bestätigt die Gültigkeit aller selbst erstellten Zertifikate. Es wird daher dringend empfohlen ein externes Backup des Stamm-Zertifikates aufzubewahren und dieses

natürlich vor unbefugtem Zugriff zu schützen!

Installieren des Stamm-Zertifikats in den Zertifikatspeicher

Mozilla Firefox

Der Mozilla Firefox besitzt einen eigenen Zertifikatsspeicher. Das Stammzertifikat muss unter Einstellungen -> Datenschutz & Sicherheit -> Sicherheit -> Zertifikate anzeigen… -> Zertifizierungsstellen importiert werden.

Chrome, Edge, Opera, Vivaldi, etc…

Auf Chromium basierte Browser verwenden den Zertifikatsspeicher von Windows. Das Stammzertifikat kann über das Snap-In Zertifikate in der Microsoft Management Console (MMC) zu den Vertrauenswürdigen Stammzertifizierungsstellen hinzugefügt werden.

Revision #12
Created 2026-01-11 15:07:32 UTC by Admin
Updated 2026-01-11 19:33:00 UTC by Admin