Elliptische-Kurven-Kryptografie (ECC) secp256k1

SSL-Zerfikate erstellen mit XCA

☐ 1. XCA installieren (https://hohnstaedt.de/xca/index.php)

☐ 2. XCA starten (XCA-Menü: Zubehör-XCA,http://blog.wenzlaff.de/?p=20761)

☐ 3. Erstellen Sie eine neue PKI-Datenbank, falls noch nicht geschehen (XCA-Menü: Datei > Neue Datenbank), geben Sie den Namen der Datenbank: **ecc.xdb** und **Speichern** und ein selbst ausgedachtes Passwort zweimal ein

☐ 4. Erstellen Sie einen neuen Privaten Key. Klicken Sie auf den Tab **Private Schlüssel** dann **Neue Schlüssel.** Dort eingeben:
Name: **ecc-priv-key**
Schlüsseltyp: **EC**
Schlüssellänge: **secp256k1: SECG curve over a 256 bit prime field**
und auf **Erstellen** klicken.

☐ 5. Erstellen Sie ein neues selbstsigniertes Zertifikat. Klicken Sie auf **Zertifikate** und auf **Neues Zertifikat**. Auf dem 1. Tab **Herkunft** muss bei Unterschreiben: **Selbstsigniertes Zertifikat erstellen** ausgewählt sein und als Signatur algorithmus: **SHA256**. Dann auf Vorlage für das neue Zertifikat: **default CA** auswählen und auf **Alles übernehmen** klicken. Auf den 2. Tab, als Inhaber folgende Eingaben (Beispiel anpassen)
Interner Name: **ecc-zertifikat** und unter Distinguished name:
countryName: **DE**
stateOrProvinceName: **Germany**
localityName: **Niedersachsen**
organizationName: **TWSoft**
organizationalUnitName: **TWSoft**
commonName: **pi-vier** (dieser Name (CN) ist Wichtig, und muss genau dem Rechnername entsprechen!)
emailAddress:**info-anfrage@wenzlaff.de**

nun unten im Feld: Privater Schlüssel den oben erstellten **ecc-priv-key (EC:256 bit)** auswählen.

Auf dem 3. Tab Erweiterungen auch noch den Key identifier: **X509v3 Authority Key Identifier** und X509v3Subject Key Identifier auswählen. Die X509v3 Basis Constraints bleiben auf Typ: **Zertifikats Authorität** und auf **Critical**. Evl. Noch die Gültigkeit anpassen oder auf 10 Jahre lassen. Evl. Noch X509v3 Subject Alternative Namen um alle Namen bzw. IP-Adressen ergänzen unter der das Zertifikat gültig sein soll.

Auf dem 4. Tab. Schlüsselverwendung X509v3 Key Usage **Digital Signature** und **Key Encipherment** wählen und unter X509v3 Extended Key Usage den **TLS Web Server Authentication** und **TLS Web Client Authentication** auswählen.

Auf den 5. Tab. Netscape unter Netscape Cert Typ den **SSL Server** auswählen. Dann auf OK klicken und das Zertifikat wurde erstellt.

☐ 6. Nun das Zertifikat als Datei exportieren. Im 3. Tab Zertifikate das erstellte **ecc-zertifikat** selektieren und auf Export klicken und das Exportformat: **PEM (*.crt)** auswählen und als **ecc-zertifikat.crt** speichern.

☐ 7. Nun noch den privaten Schlüssel als Datei exportieren. Im 1. Tab Private Schlüssel den ecc-priv-key selektieren und auf Export klicken. Dann das Exportformat: **PEM private (*.pem)** auswählen und als **ecc-priv-key.pem** speichern

Wir haben nun den Privaten Schlüssel **ecc-priv-key.pem** und das Zertifikat **ecc-zertifikat.crt** in einer Datei.

www.wenzlaff.info