Digitales Zertifikat

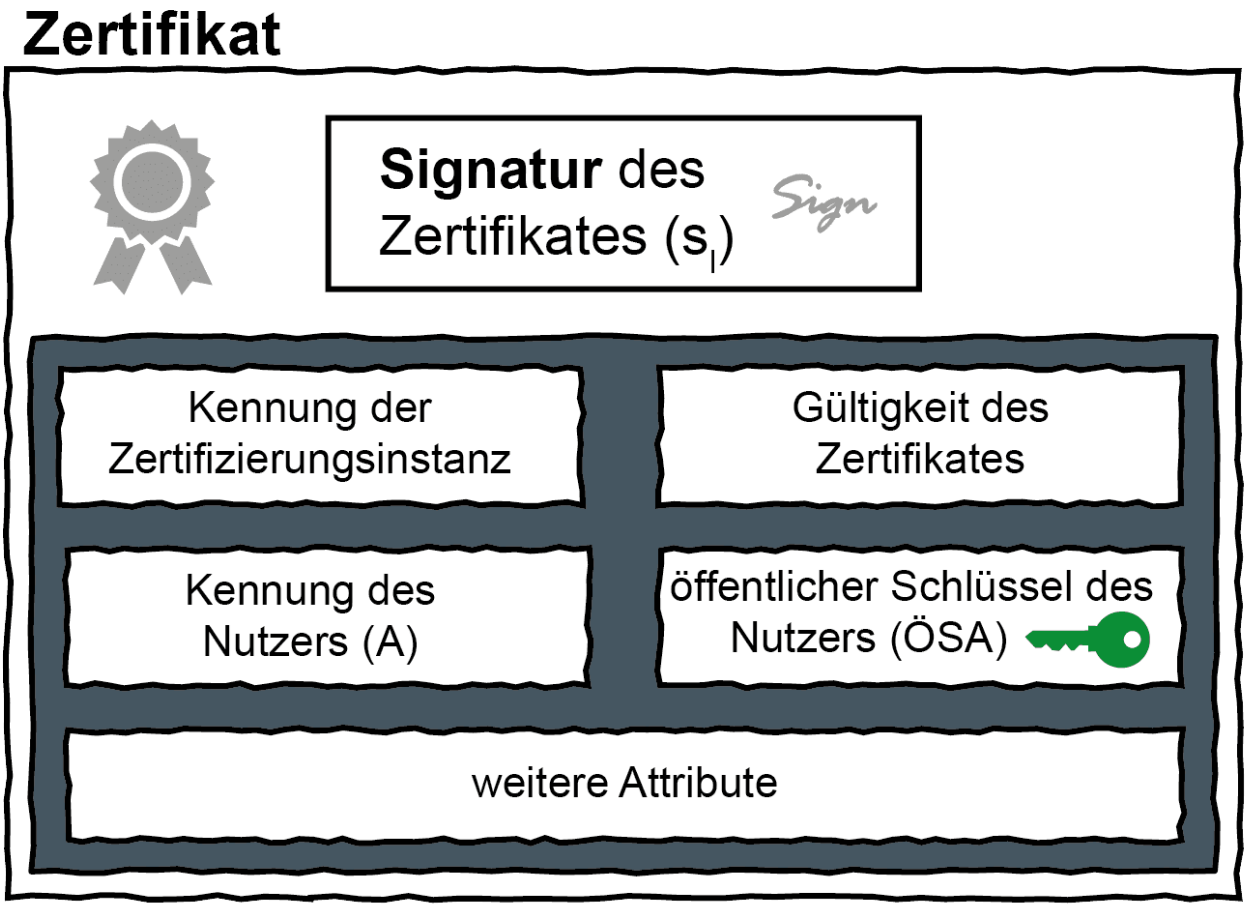
Was ist ein Zertifikat?

Ein digitales Zertifikat (auch Zertifikat oder Public-Key-Zertifikat) dient als Echtheitsnachweis für eine Website, Mailserver oder Signatur.

Durch ein Zertifikat kann geprüft werden, ob der Inhaber einer Webseite oder Versender einer E-Mail auch die Rechte hat diese Webseite / E-Mail-Adresse zu betreiben und gewährleistet somit auch die Vertraulichkeit und Authentizität.

Da im Zertifikat der Public Key des Hosts enthalten ist, kann durch ein Zertifikat auch verschlüsselte Kommunikation stattfinden.

Im Zertifikat sind einige Verwaltungsinformationen enthalten, wie Name des Inhabers, Name der CA (Certificate Authority), Gültigkeit des Zertifikats, Public Key des Inhabers, Seriennummer des Zertifikats, digitale Signatur der CA.



Zweck von Zertifikaten:

Die Zertifikate dienen dem Zweck, einen Identitätsnachweis des Inhabers einer Webseite von einer vertrauenswürdigen Stelle zu haben, auf die man sich verlassen kann.

Funktionsweise:

Der Inhaber erstellt zuerst ein Schlüsselpaar.

Mit dem Öffentlichen Schlüssel und weiteren Verwaltungsinformationen beantragt man ein Zertifikat bei einer CA.

Die CA signiert ein Zertifikat und stellt es für eure Domain aus, nachdem Sie bestätigt hat, das ihr auch der tatsächliche Inhaber der Domain seid. (Dazu wird einfach die Domain aufgelöst und die IP mit der des Antragstellers verglichen)

Das Zertifikat wird über eine "Site" im Webserver hinterlegt.

Beim Aufruf wird das Zertifikat geprüft und die Signatur der CA kann über die bereits bei Installation hinterlegten Public Keys der Root-CAs geprüft werden.

Über den im Zertifikat hinterlegten Public Key kann dann auch eine verschlüsselte Verbindung mit dem Webserver hergestellt werden.

Erstellen eines Selbst-Signierten Zertifikats:

Grundsätzlicher Ablauf:

1. Eigenen FQDN (Fully Qualified Domain Name) ermitteln
2. Apache2 installieren und SSL Module aktivieren -> Port 80 und 443 sollten jetzt offen sein
3. Schlüsselpaar generieren / Zertifikat erstellen
4. Virtuellen Server (VirtualHost) konfigurieren
5. Testen und Zertifikat prüfen

```
#1 FQDN (Fully Qualified Domain Name) herausfinden
ip -c a #x.x.x.x
host x.x.x.x #host.domain.lokal

#2 Apache2 installieren
apt install apache2 -y
lsof -i -P #Port 80 muss jz offen sein
#Im Browser http://localhost -> geht
#           https://localhost -> nope

#3 SSL Modul aktivieren:
a2enmod ssl
```

```
systemctl restart apache2

lsof -i -P #Port 443 jz offen
#Im Browser https://localhost -> Fehler "sichere" Verbindung fehlgeschlagen

#4. Schlüsselpaar generieren
apt install openssl -y
mkdir /etc/apache2/ssl
cd /etc/apache2/ssl
openssl req -new -x509 -days 365 -nodes -out apache.pem -keyout apache.pem #Hier Als Common
Name den FQDN eintragen
chmod 600 apache.pem

#Zertifikat prüfen
openssl x509 -text -noout -in apache.pem

#5. Virtuellen Server konfigurieren
cd /etc/apache2/sites-available
cat << EOF > ssl.conf
<VirtualHost *:443>
ServerName [FQDN]
SSLEngine ON
SSLCertificateFile /etc/apache2/ssl/apache.pem
DocumentRoot /var/www/html
</VirtualHost>
EOF
# [FQDN] ersetzen

a2ensite ssl
systemctl restart apache2
```

Am Ende kommt im Browser immer noch eine Sicherheitsabfrage, weil das Zertifikat selbst signiert wurde und der Browser somit die Signatur des Zertifikats nicht prüfen kann.

Revision #3
Created 24 October 2025 21:02:12 by Felix
Updated 25 October 2025 09:56:21 by Felix