

# Lernzusammenfassung

## Zertifikate

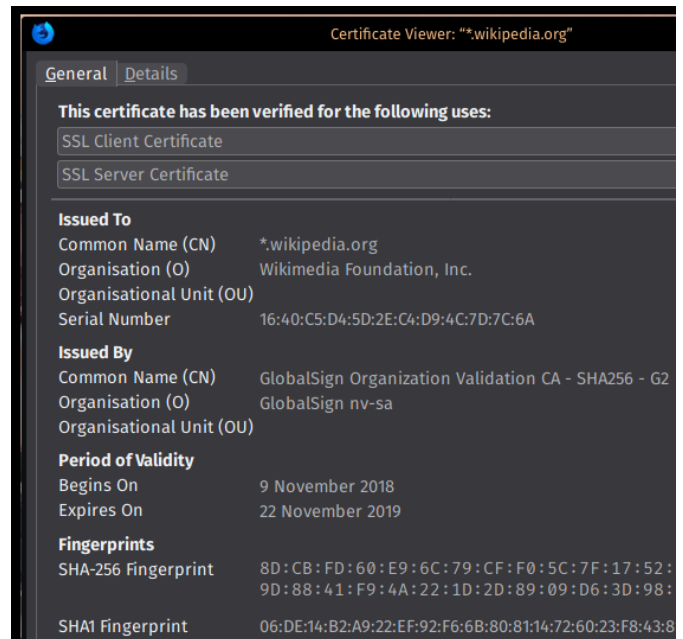
Ein **digitales Zertifikat** ist ein **digitaler Datensatz**, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und die Möglichkeit gibt dessen **Authentizität und Integrität** durch kryptografische Verfahren **zu prüfen**.

**Anhand des Zertifikates kann überprüft werden, ob der Schlüssel von der/dem Person/Rechner/Organisation stammt, mit der/dem man kommunizieren möchte.**

### Welche Eigenschaften hat ein digitales Zertifikat?

Ein Zertifikat ist ein Datensatz. Gemäß dem **Standard X509** muss ein Zertifikat bestimmte Angaben enthalten, kann aber auch zusätzliche optionale Informationen haben. Zu den Pflichtangaben gehören u.a.:

- Namen des Zertifikatsinhabers
- Zertifizierungsstelle
- Gültigkeitsdauer
- Seriennummer
- **öffentlicher Schlüssel des Inhabers (damit kann die Echtheit des Schlüssels überprüft werden) und**
- digitale Signatur der ausstellenden Zertifizierungsstelle, so dass verifiziert werden kann, ob das Zertifikat echt ist.



### Einsatzgebiete von digitalen Zertifikaten

Die Einsatzgebiete von digitalen Zertifikaten sind vielfältig. Sie werden meistens dort eingesetzt, wo die Identität festgestellt werden muss. Insbesondere findet man Zertifikate in den folgenden Systemen:

- **SSL/TLS:** Bei Netzwerkprotokollen sollen Zertifikate sicherstellen, dass sich der Server identifiziert.
- **E-Mail-Verschlüsselung:** zur Bestätigung der Echtheit von E-Mails werden ebenfalls Zertifikate eingesetzt.
- **Digitale Signatur:** Zertifikate werden auch für die digitale Signatur benötigt, um Dokumente als unverfälscht ansehen zu können.
- **Identitätsprüfung bei Systemanmeldung:** wenn sich zwei Rechner verbinden und vertraulich miteinander kommunizieren möchten (z.B. über VPN), reicht ein Passwort oft nicht aus. Denn dieses kann erspäht oder erraten werden. Auch hier sollte zur Identifikation ein Zertifikat verwendet werden.