Fakultät für
Informatik und
Mathematik

HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

ZERTIFIKATE

Arten und Validierung

Prof. Dr. Peter Trapp

Fakultät 07 – Hochschule München

Überprüfung eines Zertifikates

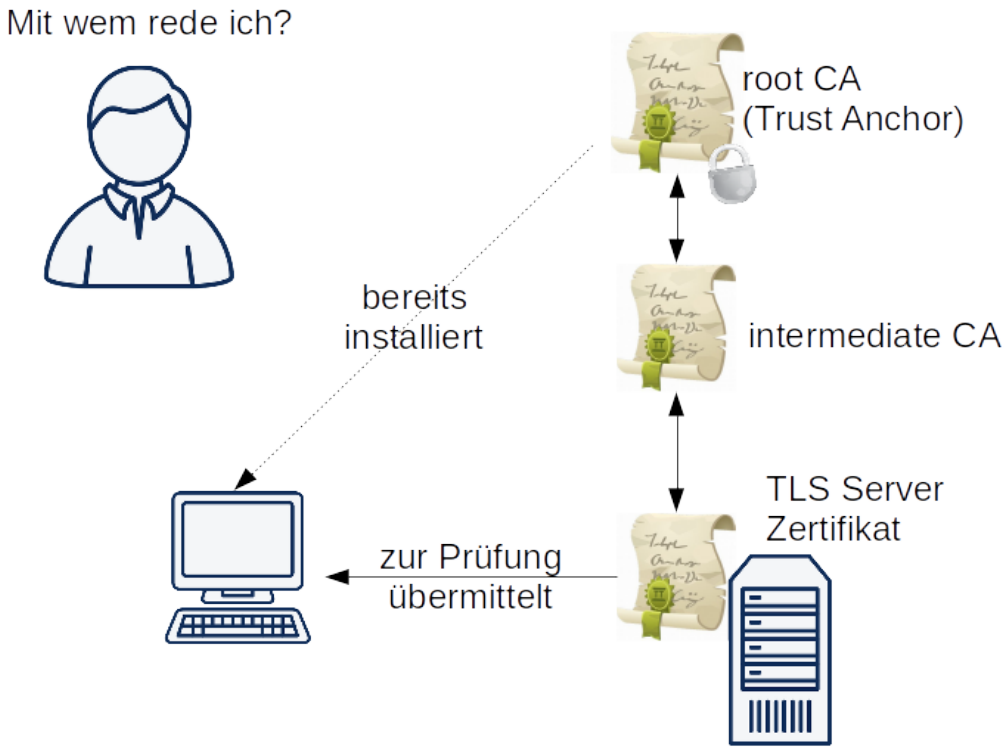

Abbildung: [1]

Signierungsarten von Zertifikaten

Ein Zertifikat wird durch die Signierung eines öffentlichen Schlüssels erzeugt. Hierbei können drei Arten unterschieden werden:

- Selbstsignierte Zertifikate (self-signed)
- „Einfache" Zertifikate
  - Domain-Validation (DV)
  - Organisation-Validation (OV)
- Extended-Validation-Zertifikat (EV)

Selbstsignierte Zertifikate (self-signed)

Hierbei bestätigt die/der Ersteller/in selbst die Authentizität des Zertifikats. Eine Prüfung muss durch die/den Anwender/in aufwändig durchgeführt werden.

Zum Beispiel durch einen Anruf bei der ausstellenden Person mit Abgleich des Fingerabrucks des Zertifikats.

Domain-Validation (DV) Zertifikate

Hierbei wird lediglich geprüft, ob die anfragende Person Adminitrationsrechte auf der Domain hat.

Dies kann auf vielfälltige Art geschehen:

- Secret in einem erreichbaren URL-Pfad hinterlegen
- Secret in DNS Record hinterlegen.
- Bestätigung per E-Mail an ,,administrative Accounts", z. B. admin@<domain>.tld

Mögliche Implementierungen siehe `https://letsencrypt.org/how-it-works/`
Weitere News: `https://www.heise.de/security/meldung/Gefaelschtes-Microsoft-Zertifikat-im-Umlauf-2576861.html`

Organisation-Validation (OV) Zertifikate

„Die Überprüfung des Unternehmens erfolgt über ein amtliches Dokument des Antragstellers. Die Telefonnummer muss in einem öffentlichen Telefonbuch einsehbar sein. Der WHOIS-Eintrag muss mit den Unternehmensdaten übereinstimmen."
(`https://www.ssl-zertifikate.de/`)

Extended-Validation (EV) Zertifikate

„Organisationseintrag in einem öffentlichen Register z.B. Handelsregister. Die Telefonnummer muss in einem öffentlichen Telefonbuch einsehbar sein. Der WHOIS-Eintrag muss mit den Organisationsdaten übereinstimmen. Abschluss eines EV-Vertrages.” (`https://www.ssl-zertifikate.de/`)