LU07c - Der Aufbau eines digitalen Zertifikates

Lernziele

- Den Standard für den Aufbau eines digitalen Zertifikates nennen können.
- Wichtigsten Teile des digitalen Zertifikates nennen und erläutern können.

Einleitung

Digitale Zertifikate bilden das Rückgrat sicherer Kommunikation im Internet. Sie dienen dazu, einen öffentlichen Schlüssel eindeutig an eine Identität – etwa eine Person, einen Server oder eine Organisation – zu binden. Damit können Kommunikationspartner prüfen, ob ein Schlüssel tatsächlich zu dem angegebenen Inhaber gehört.

Der Aufbau eines Zertifikats folgt festgelegten Standards (z. B. X.509) und enthält typischerweise Angaben wie den Namen des Inhabers, den öffentlichen Schlüssel, die Gültigkeitsdauer, die ausstellende Zertifizierungsstelle (CA) sowie eine digitale Signatur. Diese Struktur sorgt dafür, dass Zertifikate sowohl maschinell überprüfbar als auch vertrauenswürdig sind.

Bestandteile

Feld / Bestandteil	Beschreibung	Beispiel
Version	Gibt den Standard an, meist X.509 v3.	v3
Seriennummer	Eindeutige Kennung des Zertifikats.	0x5F23A9
Signaturalgorithmus	Algorithmus, mit dem die CA das Zertifikat signiert hat.	sha256RSA
Issuer (Aussteller)	Zertifizierungsstelle, die das Zertifikat ausgestellt hat.	CN=DigiCert Global Root CA
Subject (Inhaber)	Identität des Zertifikatsinhabers.	CN=www.beispiel.de, O=Beispiel GmbH
Public Key	Öffentlicher Schlüssel des Inhabers.	RSA 2048-bit Schlüssel
Validity	Gültigkeitsdauer (von – bis).	01.01.2025 – 31.12.2025
Extensions	Zusätzliche Infos, z. B. Key Usage oder SAN-Einträge.	DNS: www.beispiel.de, DNS: beispiel.com
Signature	Digitale Signatur der CA über den Zertifikatsinhalt.	Hexadezimaler Wert

Zusatzinformationen

Attributzertifikate

Die Eigenschaften des im Public-Key-Zertifikat enthaltenen Schlüssels – und damit der Geltungsbereich des Public-Key-Zertifikates – können durch Attributzertifikate genauer festgelegt werden. Attributzertifikate enthalten selbst keinen öffentlichen Schlüssel, sondern verweisen auf das betroffene Public-Key-Zertifikat über dessen Seriennummer.

Zertifizierungsinstanzen

Der Aussteller eines Zertifikats heißt Zertifizierungsinstanz und sollte vertrauenswürdig sein. Die digitale Signatur stellt Authentizität und Integrität sicher, benötigt aber wiederum ein Zertifikat für den Signaturschlüssel der CA. Daraus entsteht die Public-Key-Infrastruktur (PKI). Zertifizierungsstellen unterscheiden sich stark in der Qualität: von kostenlosen, kaum geprüften Zertifikaten bis hin zu teuren, hochsicheren Chipkarten-Zertifikaten. Maßgeblich sind die Zertifizierungsrichtlinien (Certificate Policy, CP).

Gültigkeit

Zertifikate haben eine begrenzte Laufzeit. Unsichere Zertifikate müssen vorzeitig gesperrt werden, damit Vertrauen gewahrt bleibt. Sperrinformationen werden typischerweise über Sperrlisten (CRL), Webseiten oder zunehmend per Online-Abfrage veröffentlicht.

Der X.509 Standard

Struktur und Inhalt von digitalen Zertifikaten werden durch diverse Standards vorgegeben. Aus der Vielzahl von Standards wurde der X.509 Stanard am meisten verwendet. Ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat wird im X.509-System immer an einen „Distinguished Name“ oder einen „Alternative Name“ wie eine E-Mail-Adresse oder einen DNS Eintrag gebunden.

Sperren von Zertifikaten

X.509 beinhaltet ausserdem einen Standard, mittels dessen Zertifikate seitens der Zertifizierungsstelle wieder ungültig gemacht werden können, wenn deren Sicherheit nicht mehr gegeben ist (z. B. nach dem öffentlichen Bekanntwerden des Private Keys für das Signieren von E-Mails). Die Zertifizierungsstelle kann hierfür ungültige Zertifikate in *Zertifikatsperrlisten* (certificate revocation list, kurz CRL) führen. Die automatische Überprüfung, ob ein Zertifikat inzwischen Teil einer Sperrliste ist, ist allerdings nicht in allen Programmen, die X.509-Zertifikate akzeptieren, standardmässig aktiviert.

Struktur des X.509-Zertifikats

- Zertifikat
    - Version
    - Seriennummer
    - Algorithmen-ID
- Aussteller
    - Land/Region
    - Bundesland/Kanton
    - Ort
    - Organisationseinheit
    - Organisation
    - Gemeinsamer Name
- Gültigkeit
    - Von
    - Bis
- Zertifikatinhaber
- Zertifikatinhaber-Schlüsselinformationen
    - Public-Key-Algorithmus
    - Public Key des Zertifikatinhabers
- Eindeutige ID des Ausstellers (optional)
- Eindeutige ID des Inhabers (optional)
- Erweiterungen
    - o …
- Zertifikat-Signaturalgorithmus
- Zertifikat-Signatu

Beispiel eines X.509 Zertifikates

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
        Validity
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After : Oct 29 17:39:10 2001 GMT
        Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/Email=xyz@anywhere.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                    8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                    f0:b4:95:f5:f9:34:9f:f8:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:xyz@anywhere.com
            Netscape Comment:
                mod_ssl generated test server certificate
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: md5WithRSAEncryption
        12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
        3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
        82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
        cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
        4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
        d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
        44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
        ff:8e
```