X.509v3 Zertifizierungsinstanz der Universität Würzburg

Markus Krieger
Rechenzentrum Uni Würzburg
ca@uni-wuerzburg.de

Notwendigkeit von Zertifikaten

Steigende Anzahl von Kommunikationsbeziehungen zu Nutzern/Ressourcen erfordert:

- Verschlüsselung gegen Mitlesen
- Signatur um Veränderungen zu erkennen/nicht Abstreitbarkeit
- Authentisierung zur Feststellung der Identität
- Authorisierung eines Zugriffs

→ Public Key Verfahren

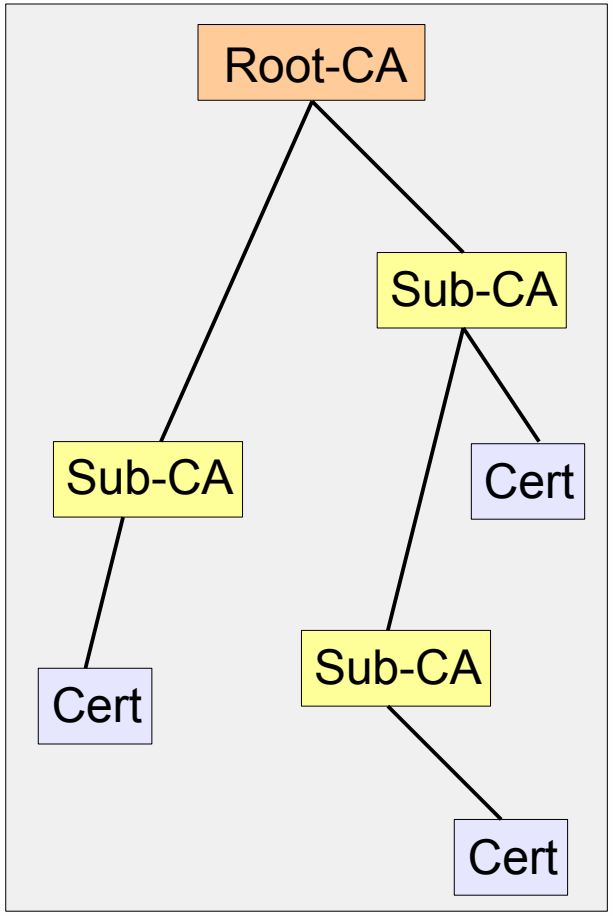
→ Zertifikate, die einen Key mit einer Identität verknüpfen

ABER: Wie kann ein Schlüsseltausch / eine Identitäts-prüfung effizient erfolgen?

→ X.509v3 Zertifikate mit Zertifizierungsinstanz

Zertifizierungsinstanz (CA)

- Signiert Zertifikate
- Gibt Policy vor (Certification Practice Statement, CPS)
- Sorgt für die Eindeutigkeit der zertifizierten Identitäten
- Pflegt Certificate Revocation List (CRL)
- Hierarchie mit Unter-CAs bildet Certificate Chain.
- Applikation muss lediglich die Root-CA kennen und ihr vertrauen



Zertifikatstypen

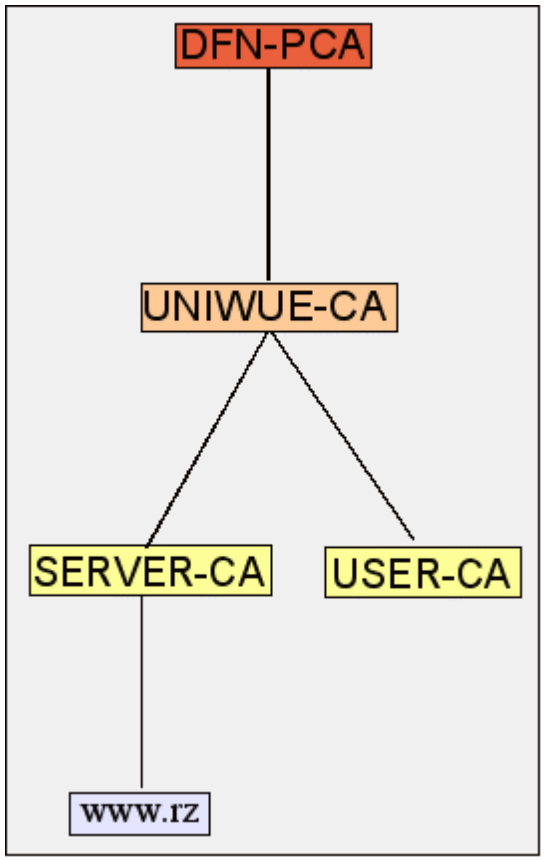
- CA-Zertifikate (Zertifikate Signieren, CRL Signieren)
  - Das Rootzertifikat ist als einziges Zertifikat „Self signed“
- Serverzertifikate (Signieren, Verschlüsseln)
  - Verwendung für SSL (HTTPS, IMAPS, ...)
- Userzertifikate (Signieren, Authentifizieren, Verschlüsseln)

Aufbau eines Zertifikats

```
Version: 3 (0x2)
Serial Number:7 (0x7)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=DE, O=Universitaet Wuerzburg, CN=SERVER-CA/emailAddress=ca@uni-wuerzburg.de
Validity
    Not Before: Apr  2 10:48:58 2004 GMT
    Not After : Apr  2 10:48:58 2006 GMT
Subject: C=DE, O=Universitaet Wuerzburg, OU=Rechenzentrum, CN=www.rz.uni-
wuerzburg.de/emailAddress=plehn@rz.uni-wuerzburg.de
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:e1:67:25:e0:3e:9d:97:20:d3:21:a1:83:ba:48:
            ...
X509v3 extensions:
    X509v3 Key Usage:
        Digital Signature, Key Encipherment
    X509v3 Subject Key Identifier:
        44:6D:AA:33:F1:49:D3:E3:AA:3A:68:ED:68:07:A6:4E:BD:D7:88:FD
    X509v3 Authority Key Identifier:
        keyid:2C:8A:99:A2:08:21:FD:65:83:3E:B9:D5:67:86:F1:8C:2B:15:B7:21
        DirName:/C=DE/O=Universitaet Wuerzburg/CN=UNIWUE-CA/emailAddress=ca@uni-wuerzburg.de
        serial:01
    X509v3 CRL Distribution Points:
        URI:http://ca.uni-wuerzburg.de/server-ca.crl
            ...
Signature Algorithm: sha1WithRSAEncryption
    3f:10:96:1a:61:79:ac:02:e4:21:7b:f2:58:9d:85:7b:69:fc:
    ...
```

UNIWUE-CA

- Sub-CA zur DFN-PCA
- Zuständigkeit auf die Universität Würzburg eingeschränkt.
- UNIWUE-CA zertifiziert nur Sub-CAs.
- USER-CA ist Platzhalter, da innerhalb der Uni die Strukturen für eine PKI fehlen.



Certificate Signing Request

- RSA-Schlüsselpaar erstellen
  - openssl genrsa -des3 -out key.pem 1024
- CSR erzeugen
  - openssl req -new -sha1 -key key.pem -out csr.pem
- Wichtig: Subject-DN muss folgende Form haben:

  „C=DE, O=Universitaet Wuerzburg, OU=<Bereich>, CN=<Name>“
- Überprüfen des CSR
  - openssl req -noout -text -in <csr.pem>
- Fingerprint für Teilnehmererklärung
  - openssl req -noout -modulus -in server.csr | openssl sha1 -c

Zertifikat beantragen

- CSR vorab zur Prüfung an ca@uni-wuerzburg.de
- Teilnehmererklärung ausfüllen (mit Fingerprint und Angabe eines gültigen Personal-/Reisepasses)
- Akkreditierungsschreiben von Zeichnungsberechtigtem einholen
- Persönliches Erscheinen mit Teilnehmererklärung und angegebenem Ausweiss bei der CA

→ Sobald alle Voraussetzungen erfüllt sind, kann die CA das Zertifikat ausstellen und per Mail verschicken

- Zertifikat überprüfen
  - openssl x509 -noout -text -in <cert.pem>

GRID-RA

- GRID-CA stellt eigene Zertifikatshierarchie dar.
- Zertifikate werden nur direkt von der DFN-PCA ausgestellt.
- Um Teilnehmern der Uni Würzburg ein persönliches Erscheinen in Hamburg zu ersparen betreibt das RZ eine Registrierungsstelle (RA).
- Diese nimmt Teilnehmeranträge, Akkreditierungen und CSRs entgegen und leitet sie nach einer Prüfung an die DFN-PCA weiter.
- Zertifikate werden direkt von der DFN-PCA an den Zertifikatnehmer geschickt.

Einrichtung Apache

Folgende Direktiven müssen in der „httpd.conf“ angepasst werden:

- SSLEngine on
- SSLCertificateFile /path/to/server.crt
- SSLCertificateKeyFile /path/to/server.key
- SSLCertificateChainFile /path/to/ca.crt

Beim Starten des Apache muss des SSL-Modul durch Angabe von „-D SSL“ aktiviert werden

Kommandos & Links

OpenSSL:

- openssl help bzw. openssl <commando> help
- openssl s_client -connect <host:port> -showcerts -CAfile root-ca-cert.pem

Links:

- DFN-PCA: http://www.dfn-pca.de
- UNIWUE-CA: http://ca.uni-wuerzburg.de
- CSRs: http://ca.uni-wuerzburg.de/csr