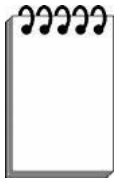
Prof. Dr. Martin Leischner
Netzwerksysteme und TK

Sicherheit in Netzen
Lehrgespräch: Zertifikate und PKI

1. X.509 PKI-Infrastruktur
2. Aufbau eines X.509 Zertifikats
3. PKI-Szenarien
4. Browser Root Stores

X.509 PKI-Infrastruktur

- **X.509** *(Public-key and attribute certificate frameworks)*
  ist Teil der ITU-T Standard-Familie
  X.500 *(Information technology – Open Systems Interconnection – The Directory)*
- Was genau ist ein Zertifikat?
- **X.509 ist als zentraler Vertrauensdienst baumartig aufgebaut.**
- **Es sind auch alternative Ansätze denkbar, etwa eine vernetzte Vertrauens-struktur.**
- Wäre für X.509 eine zentrale, globale CA, von der alle Zertifikate direkt oder indirekt signiert werden sinnvoll?
- Wenn ja, wie müsste diese CA grundsätzlich organisiert werden?
- **X.509-Zertifikate sind ASN.1 codiert.**



Aufbau eines X.509 Zertifikats

<table>
<tr><th colspan="3">X509v3 Zertifikat
DN - Distinguished Name (Zertifikatsname)</th></tr>
<tr><td>DN - Distinguished Name
(Zertifikatsname)</td><td>Version</td><td>Seriennummer</td></tr>
<tr><td>Signatur-Algo.</td><td>gültig ab:</td><td>gültig bis</td></tr>
<tr><td colspan="3"><u>Identitätsdaten des Ausstellers:</u>
Land/Region, Bundesland, Ort, Organisationseinheit, Organisation
Common Name (Name des Ausstellers)</td></tr>
<tr><td colspan="3"><u>Identitätsdaten des Inhaber:</u>
Land/Region, Bundesland, Ort, Organisationseinheit, Organisation
Common Name (Nutzerzertifikat: Vorname+Nachname, Serverzertifikat: voll qualifizierter Hostname)</td></tr>
<tr><td>Public Key Algorithmus</td><td>Public Key des Inhabers</td><td>X.509 v3
Extensions (z.B. CRL)</td></tr>
</table>

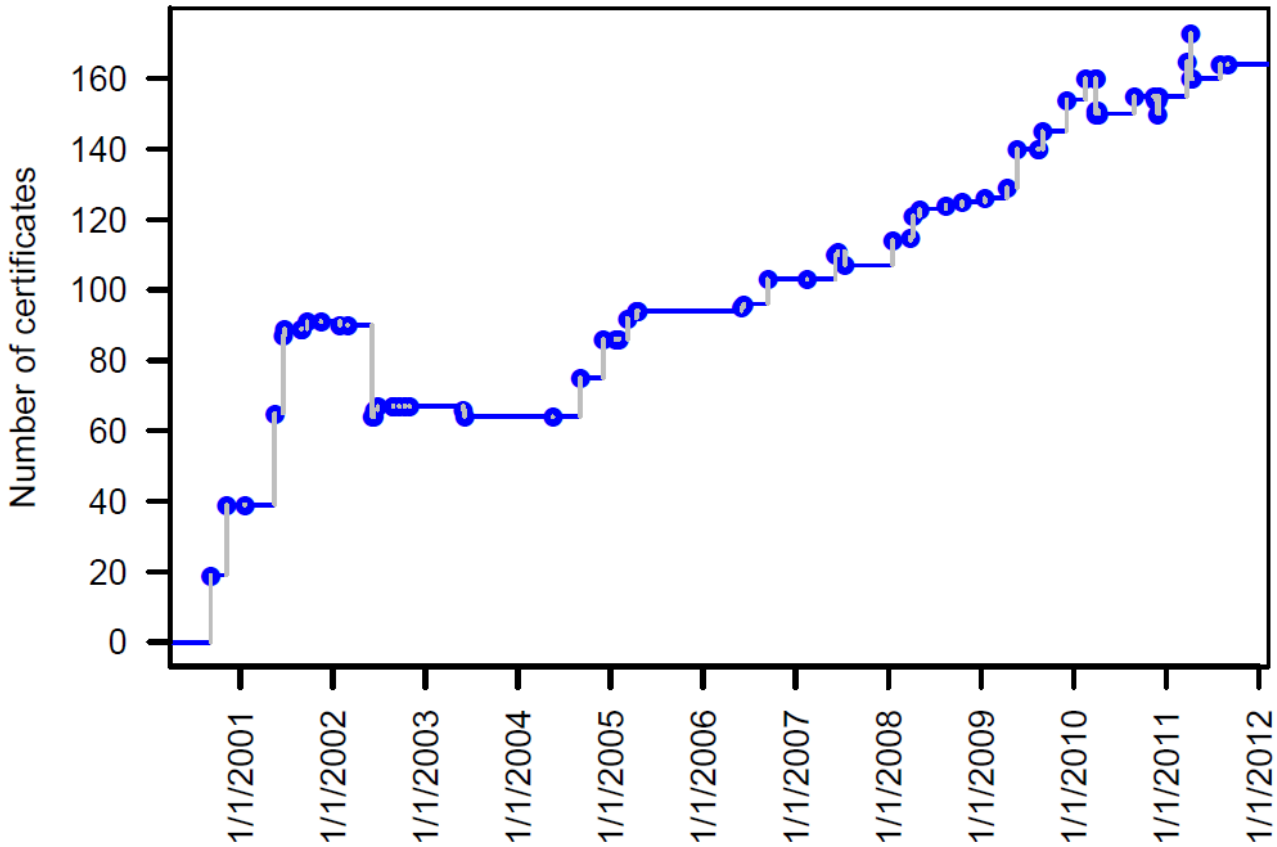
Zertifikate, CAs und PKI in X.509

Begriffe:

- Root-Zertifikate
- Certification Authority (CA)
- Host Certificate
- Intermediate Certificate
- Intermediate Certification Authority (ICA)
- Root Store
- Cross-Signing

nach: *R. Holz*, L. Braun, N. Kammenhuber, and G. Carle. The *SSL Landscape* – A *Thorough Analysis* of the *X.509 PKI Using Active* and *Passive Measurements*. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference – ACM Press, 427-444, 2011

Größe des Mozilla Root Store



aus: *R. Holz*, L. Braun, N. Kammenhuber, and G. Carle. The *SSL Landscape* – A *Thorough Analysis* of the *X.509 PKI Using Active* and *Passive Measurements*. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference – ACM Press, 427-444, 2011

Literatur

- ***R. Holz***, **L. Braun, N. Kammenhuber, and G. Carle. The *SSL Landscape* – A *Thorough Analysis* of the *X.509 PKI Using Active* and *Passive Measurements*. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference – ACM Press, 427-444, 2011**