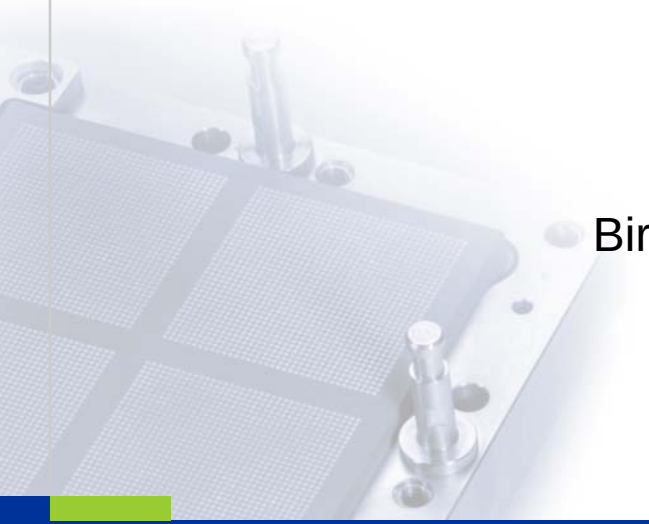
R|R|Z|N

Digitale Signaturen in Theorie und Praxis



Sicherheitstage SS/05

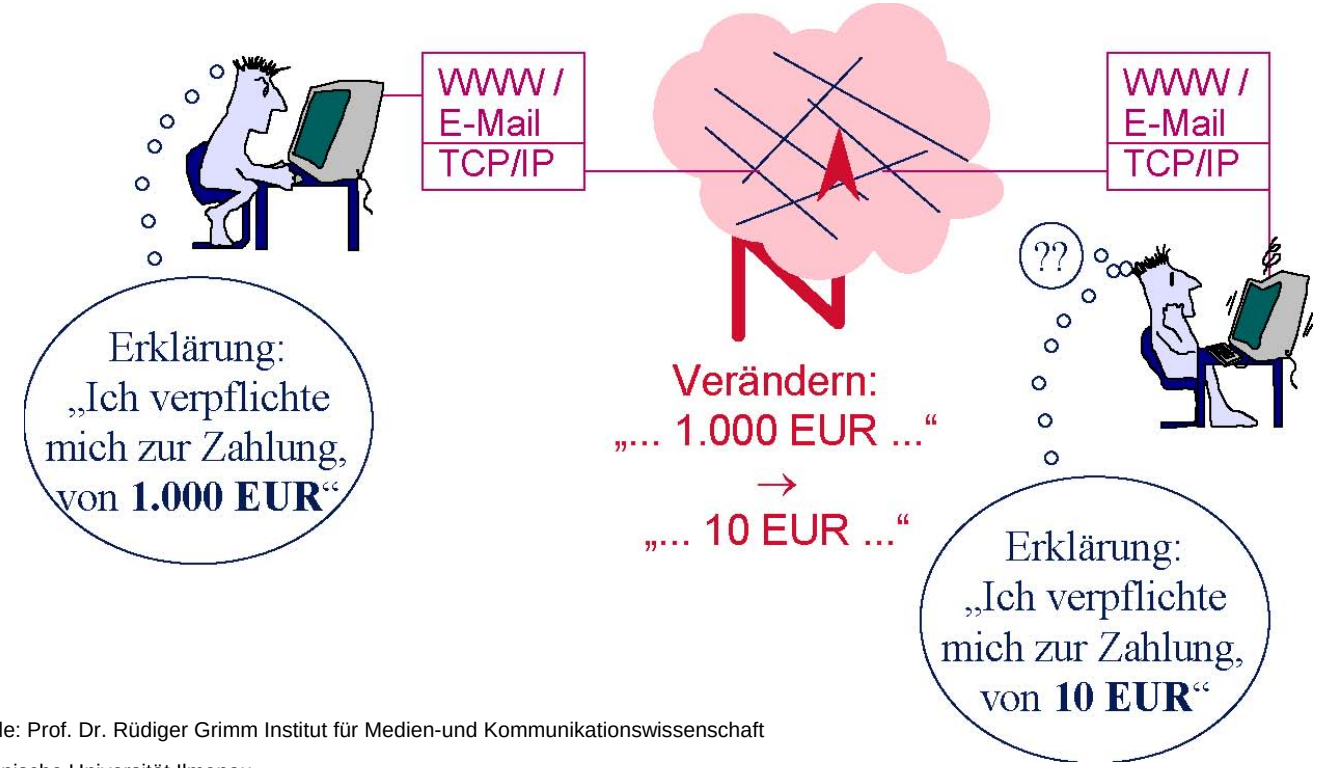
Birgit Gersbeck-Schierholz, RRZN

Gliederung

R|R|Z|N

- **Sicherheitsziele der digitalen Signatur**
- **Digitale Zertifikate in der Praxis**
- **Kryptografische Techniken**
- **Die Zertifizierungsinstanz der Universität Hannover (UH-CA)**
- **Benutzerschnittstelle der UH-CA**

Sicherheitsrisiken im Internet



Quelle: Prof. Dr. Rüdiger Grimm Institut für Medien-und Kommunikationswissenschaft

Technische Universität Ilmenau

Sicherheitsziele der digitalen Signatur

R|R|Z|N

Die eindeutige Identität des Absenders soll gewährleistet sein

Authentizität

Die Daten sollen von Dritten nicht gelesen werden können

Vertraulichkeit

S i c h e r h e i t s z i e l e

Die Daten sollen nicht verändert werden

Integrität

Die Daten können nicht mehr abgestritten werden

Verbindlichkeit

Sicherheitsziele der digitalen Signatur

R|R|Z|N

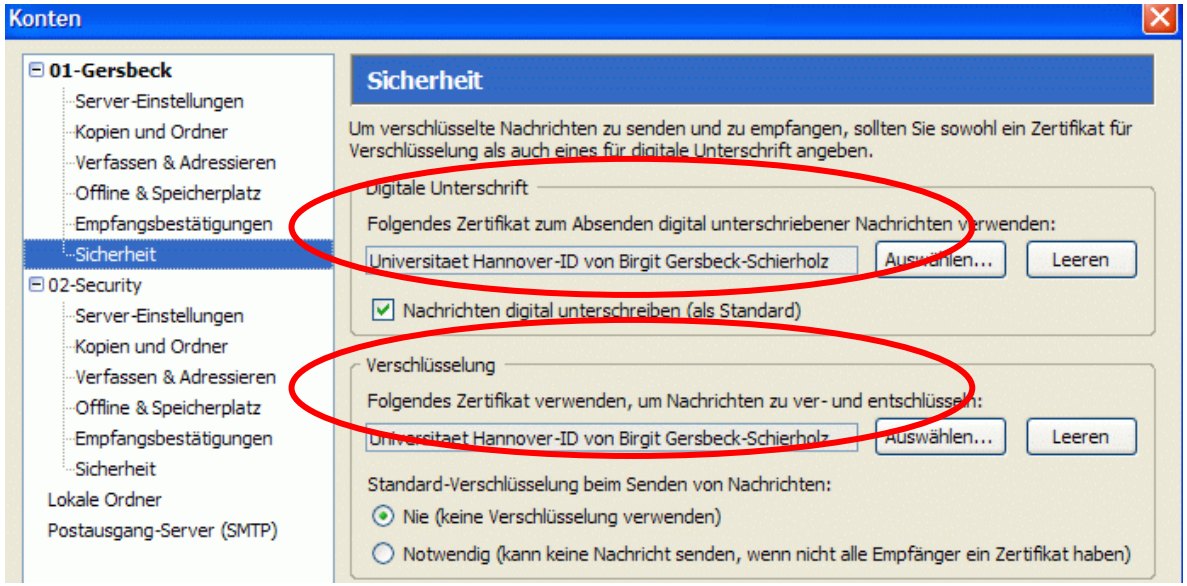
- Diese Sicherheitsziele können mit kryptografischen Methoden, digitalen Zertifikaten bzw. digitaler Signatur, erreicht werden

R|R|Z|N

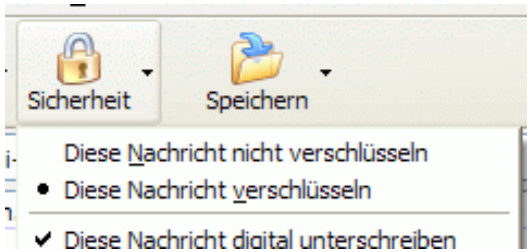
Signierte und verschlüsselte E-Mail

(Beispiel: Thunderbird)

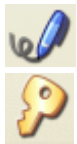
Implementieren



Verfahren wählen

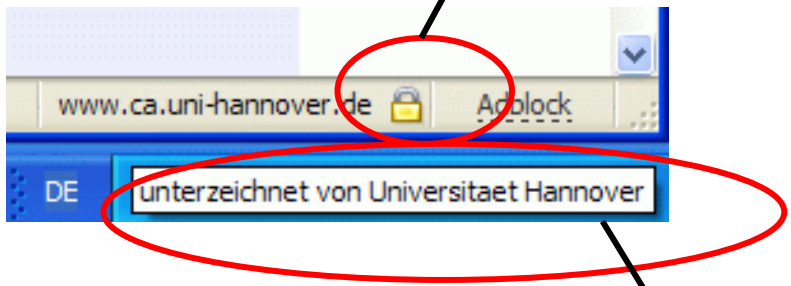


Darstellung beim Empfänger



- **Gesicherte Kommunikation mit Servern**

SSL-verschlüsselte Server-Verbindung
(https)

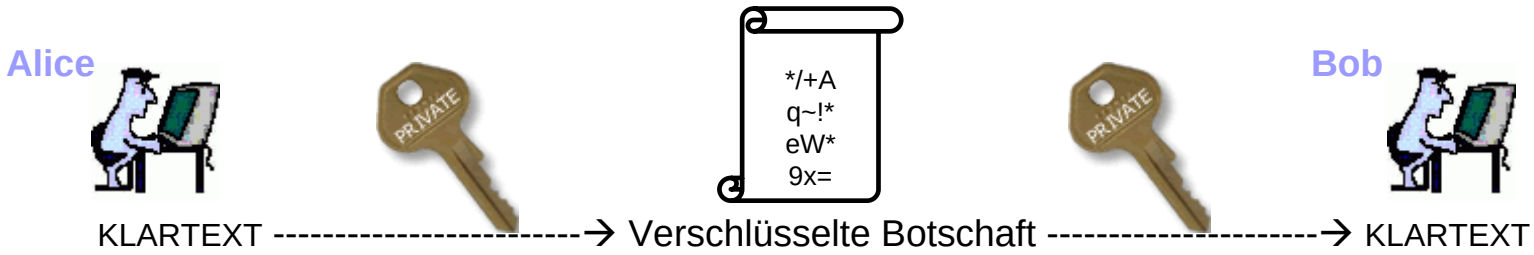


Zertifizierungsstelle (CA)

Symmetrische Verschlüsselung

- Ältestes Verfahren zur Verschlüsselung
- Moderne Symmetrische Verschlüsselungsverfahren:
  - 3DES, IDEA, Blowfish, AES usw. (Schlüssellänge derzeit ca. 128 – 196 bit)

- Beide Kommunikationspartner benutzen den gleichen Schlüssel zur Ver- und Entschlüsselung



Vorteil: sicheres Verfahren mit guter Performance

Nachteil: der Schlüsselaustausch ist nur über ein persönliches Treffen oder einen Kurier zu realisieren

- Mühseliger Transport von Schlüsseln über weite Entfernungen
- Sichere Verbindung zum Schlüsseltausch notwendig

Asymmetrische Verschlüsselung

- Gibt es seit 1976 (Diffie/Hellmann)
- Das Revolutionäre war **die Idee die Schlüssel zum Ver- und Entschlüsseln zu trennen**

- Jeder Kommunikationspartner verfügt über ein **Schlüsselpaar**, dieses besteht aus zwei unterschiedlichen Schlüsseln:

1. ***Geheimer Schlüssel*** *(private key),* zum Verschlüsseln (nur für mich)
2. ***Öffentlicher Schlüssel*** *(public key),* zur Rückgewinnung des Textes (für alle anderen)

- **Was mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem geheimen Schlüssel lesbar gemacht werden und umgekehrt**

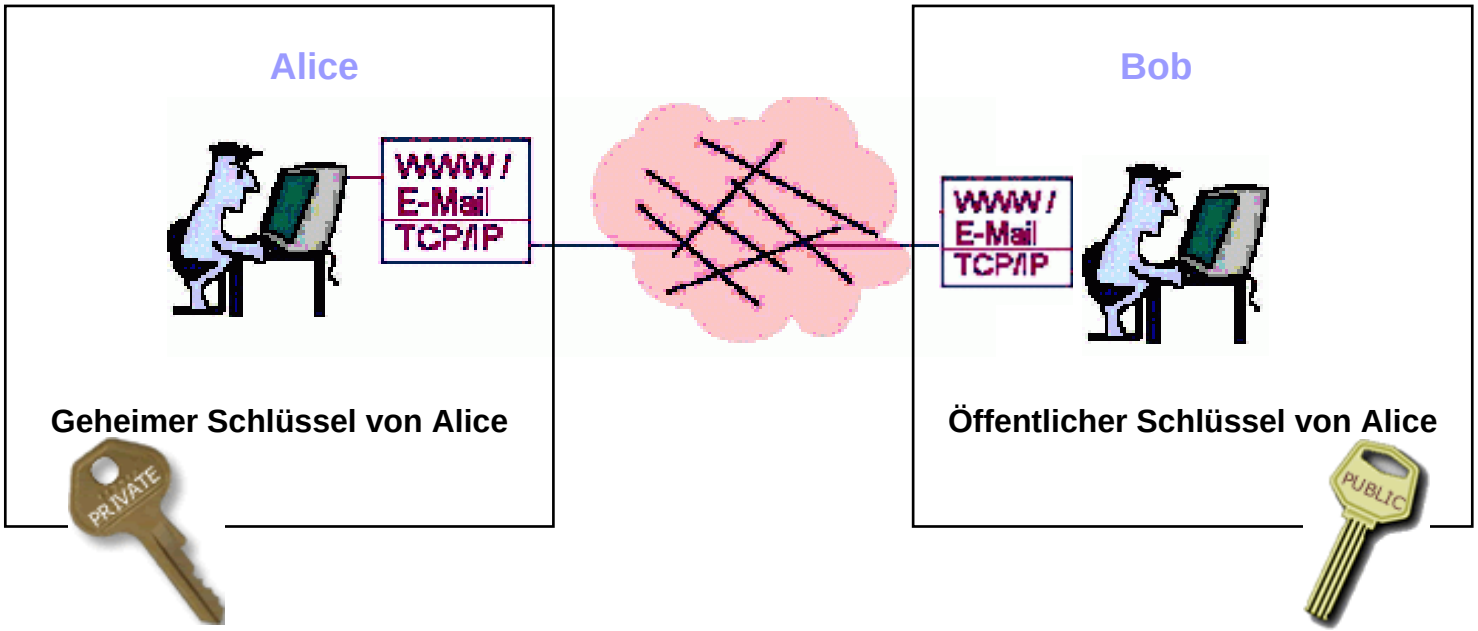
Vorteil: gesicherte Kommunikation zwischen Partnern die sich nicht kennen, da kein Schlüsseltausch notwendig ist

Nachteil: schlechte Performance

- **Anwendungsbeispiel für asymmetrische Verschlüsselung (1)**
  - Signieren

    gewährleistet

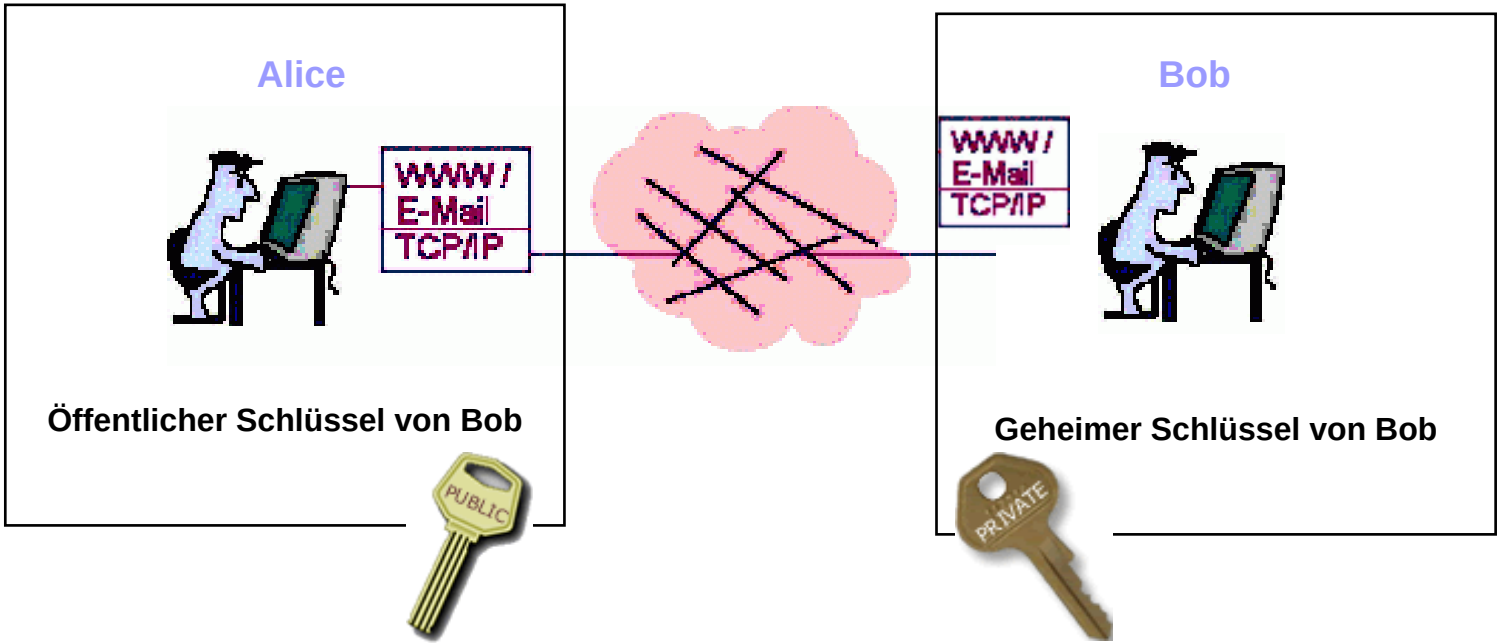
    – **Authentizität** : Identität des Absenders ist eindeutig
    – **Integrität** : Daten wurden nicht verändert
    – **Verbindlichkeit** : kann nicht mehr abgestritten werden



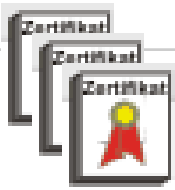
- **Anwendungsbeispiel für asymmetrische Verschlüsselung (2)**
  - Verschlüsseln

    gewährleistet

    – Vertraulichkeit : Daten können von Dritten nicht gelesen werden



- **Digitale Zertifikate**



Das Dilemma der **asymmetrischen Verschlüsselungsverfahren**:

Kann man den Angaben im öffentlichen Schlüssel vertrauen?

- Dies ist nur dann kein Problem, wenn man den Schlüssel persönlich vom Eigentümer bekommen hat (Vorteil der Schlüsselverteilung gegenüber der symmetrischen Verschlüsselung wäre damit hinfällig).

Die Zertifizierungsinstanz, CA (Certification Authority)

- stellt als vertrauenswürdige Instanz die eindeutige, zweifelsfreie Zuordnung zwischen einem Schlüsselpaar und einer Person oder einem Rechner her
- Dabei wird die **reale Identität** an eine **digitale Identität** gebunden
- Nach Prüfung der Identität und des öffentlichen Schlüssels, stellt die CA ein Zertifikat aus.

Die Zertifizierungsinstanz der Universität Hannover (UH-CA)

R|R|Z|N

- Zertifizierungsstelle der Universität Hannover seit Mai 2004
- Zertifizierungsrichtlinien zum Betrieb

UH-CA

- Zertifiziert öffentliche Schlüssel für Nutzer und Server
- Benutzerschnittstelle*:* *www.ca.uni-hannover.de*
- Zertifikate für Mitglieder der Universität Hannover
- Integriert in die PKI (Public Key Infrastructure) des Deutschen Forschungsnetzes

DFN CERT

Die Zertifizierungsinstanz der Universität Hannover (UH-CA)

R|R|Z|N

- **Zertifizierungsrichtlinien zum Betrieb der UH-CA**

https://www.ca.uni-hannover.de/Zertifizierungsrichtlinien.htm

- **Basis für das Vertrauen der Zertifikatnehmer**
- **Bestimmt die Qualität des Zertifikats**
- **Definiert die Sicherheitsanforderungen an die CA**
  - *Persönliche Identifizierung der Teilnehmer*
  - *Offline-CA (CA-Hardware nicht am Netz)*
  - *…*

Policy

Standard X.509v3:
Festlegung der Struktur eindeutiger Namen (distinguished name, DN)
C=DE, O=Universitaet Hannover, OU=<Einrichtung/Institut>, CN=<eindeutiger Name>, email=<Email-Adresse>

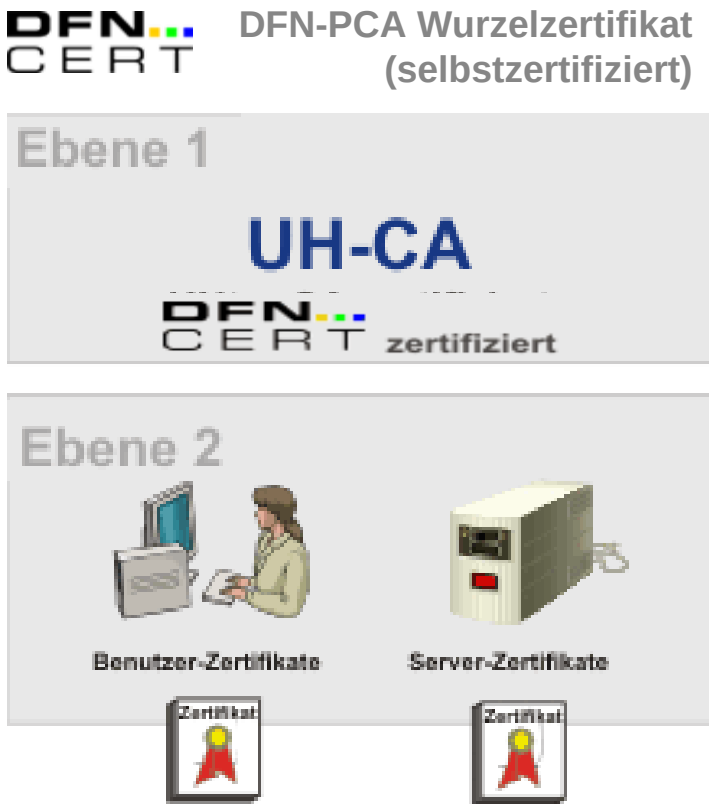
Die Zertifizierungsinstanz der Universität Hannover (UH-CA)

R|R|Z|N

Zertifizierungshierarchie

Alte Policy, Laufzeit bis 25.05.2006:

Neue Policy, Laufzeit ab Juni/Juli 2005:

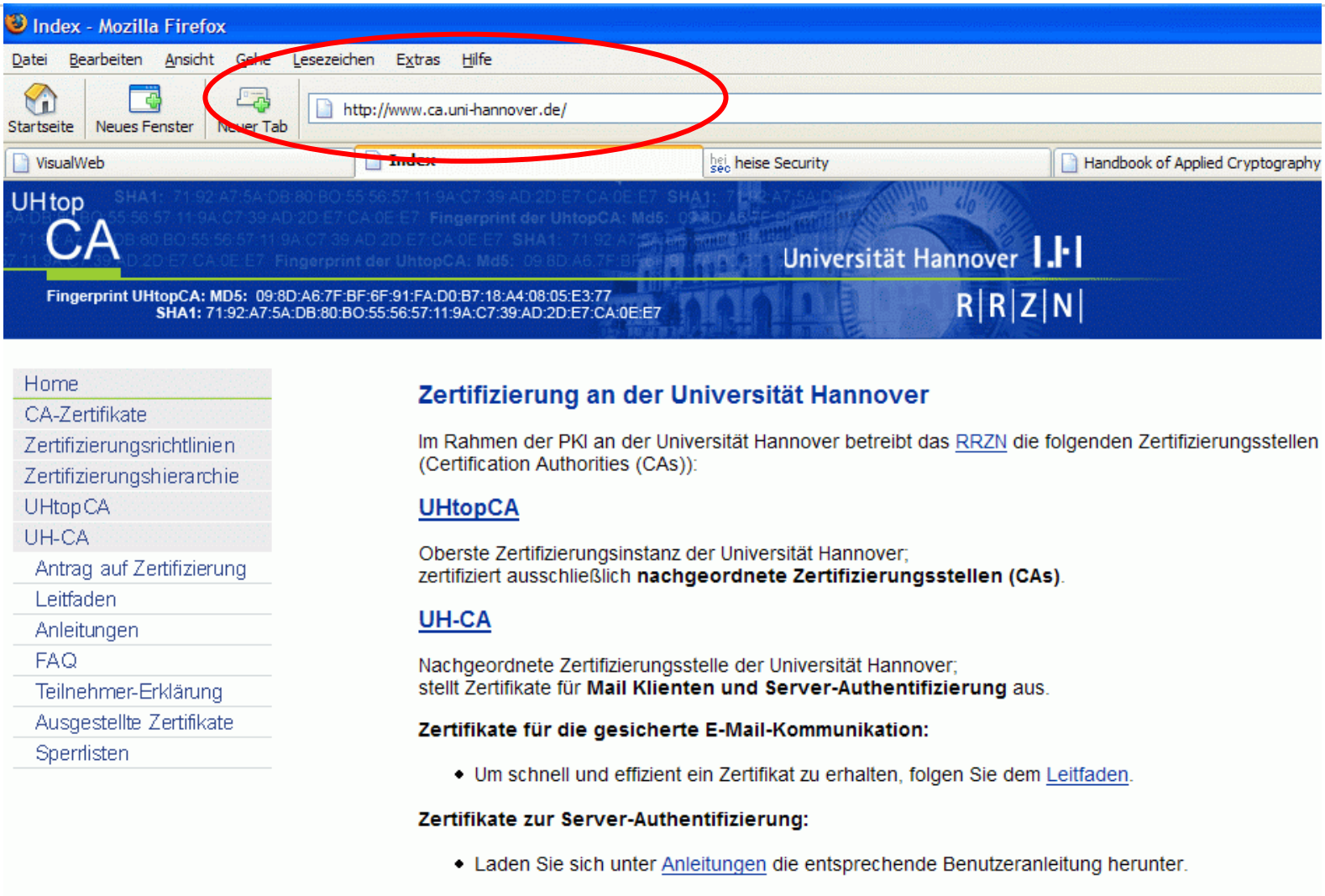


Die Zertifizierungsinstanz der Universität Hannover (UH-CA)

R|R|Z|N

- **Aufgaben der PKI**
  - **Bearbeitung von Zertifizierungsanträgen**
    - Webinterface
    - Schriftliche Teilnehmererklärung
    - Persönliche Identifizierung
  - **Ausstellen von Zertifikaten**
  - **Verwalten und Verteilen von Zertifikaten**
    - Verzeichnisdienst
    - Bereitstellung über die Webschnittstelle
    - Benachrichtigung der Zertifikatnehmer (Ausstellung, Sperrung, Gültigkeit)
    - Backup
  - **Sperrung von Zertifikaten, z.B. bei Kompromittierung oder Schlüsselverlust**
  - **Regelmäßige Veröffentlichung von Sperrlisten**

Benutzerschnittstelle der UH-CA



Benutzerschnittstelle der UH-CA

- **Zugriff auf ausgestellte Zertifikate (1)**

Benutzerschnittstelle der UH-CA

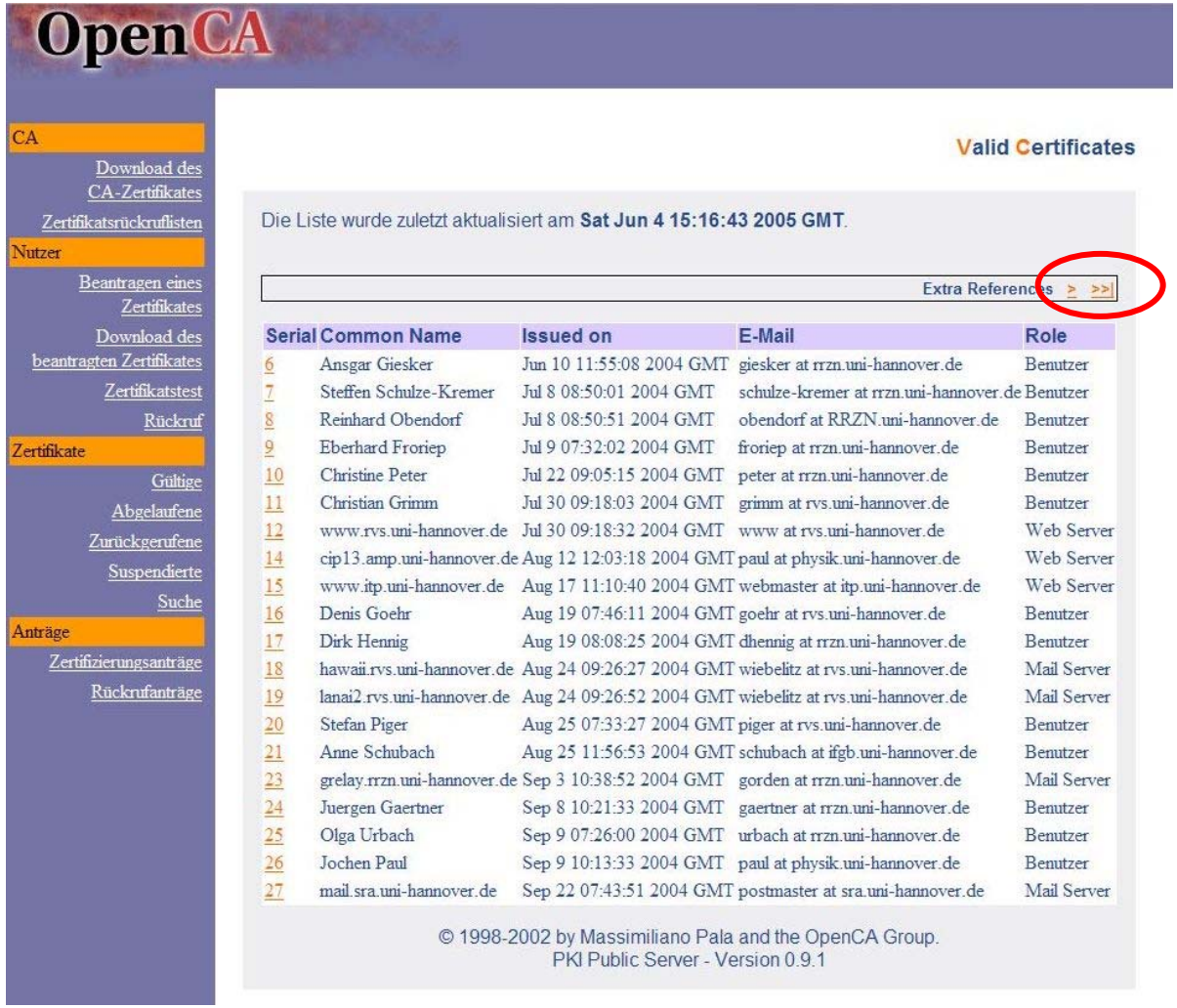
R|R|Z|N

- **Zugriff auf ausgestellte Zertifikate (2)**

Benutzerschnittstelle der UH-CA

R|R|Z|N

- **Zugriff auf ausgestellte Zertifikate (3)**

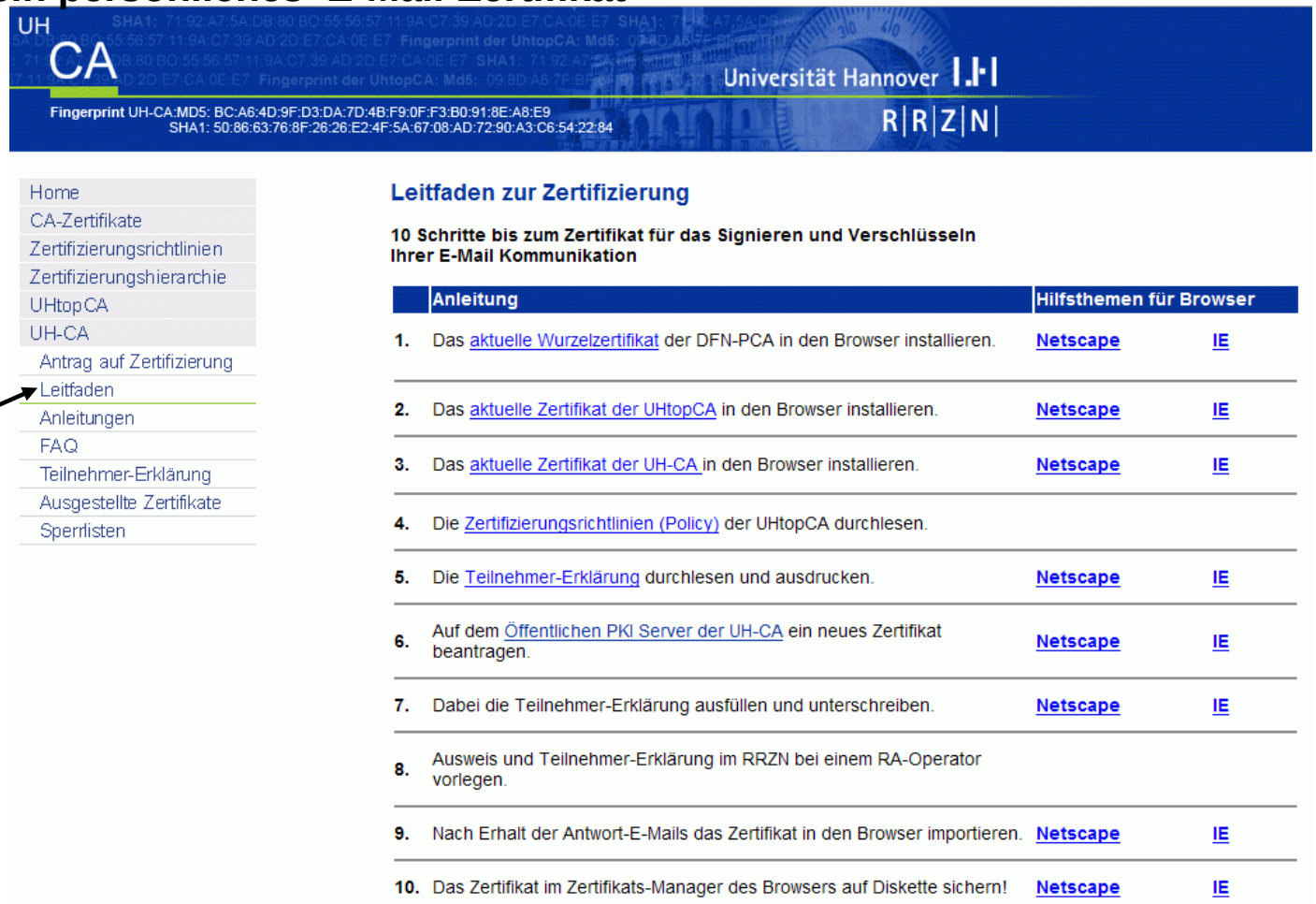


Zugriff auf Sperrlisten

Benutzerschnittstelle der UH-CA

R|R|Z|N

Antrag auf ein persönliches E-Mail-Zertifikat



Benutzerschnittstelle der UH-CA

R|R|Z|N

- **Antrag auf ein Server-Zertifikat**

Literatur

- S. Singh, *Geheime Botschaften, Hanser*, 2000
- C. Adams, S. Lloyd, *Understanding PKI, 2nd Edition*, Addison Wesley, 2003
- A. Nash, W.Duane, C. Joseph, D. Brink, *PKI, e-security implementieren, Deutsche Ausgabe*, RSA, 2002
- A.J. Menezes, P.C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography, last updated October 4*, 2004, *http://www.cacr.math.uwaterloo.ca/hac/*
- B. Gersbeck-Schierholz, *UH-CA: Zertifikate für digitale Signaturen und Verschlüsselung, http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/UH_CA_Sicherheitstage04_231104.pdf*

Auf eine sicherere Zukunft!