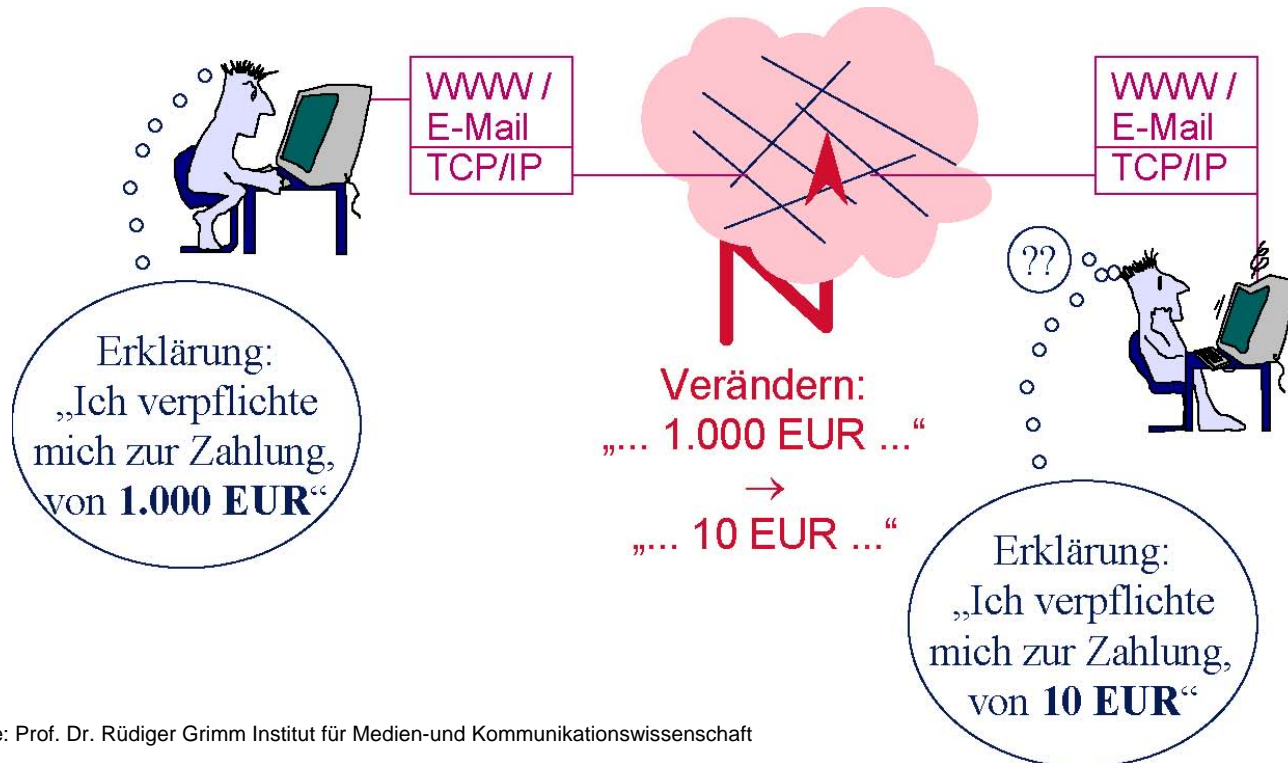


Digitale Signaturen in Theorie und Praxis

Sicherheitstage SS/05

Birgit Gersbeck-Schierholz, RRZN

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



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

Die eindeutige Identität des Absenders soll gewährleistet sein

Authentizität

Die Daten sollen von Dritten nicht gelesen werden können

Vertraulichkeit

Sicherheitsziele

Die Daten sollen nicht verändert werden

Integrität

Die Daten können nicht mehr abgestritten werden

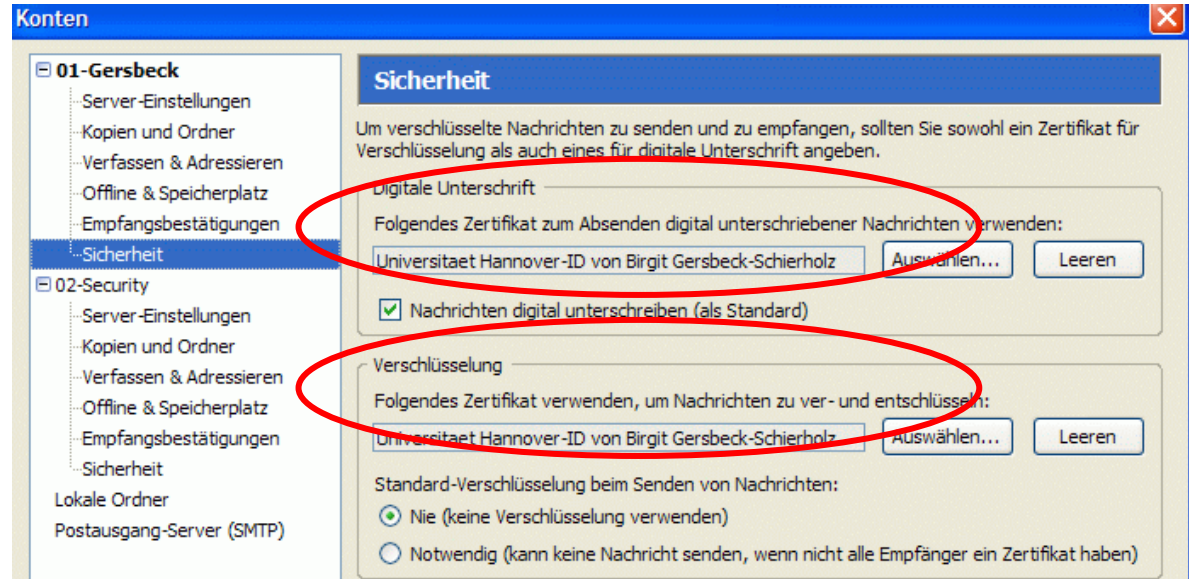
Verbindlichkeit

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

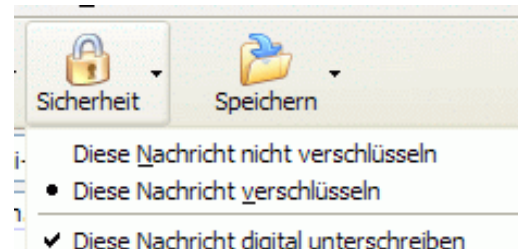
■ Signierte und verschlüsselte E-Mail

(Beispiel: Thunderbird)

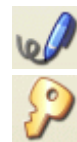
Implementieren



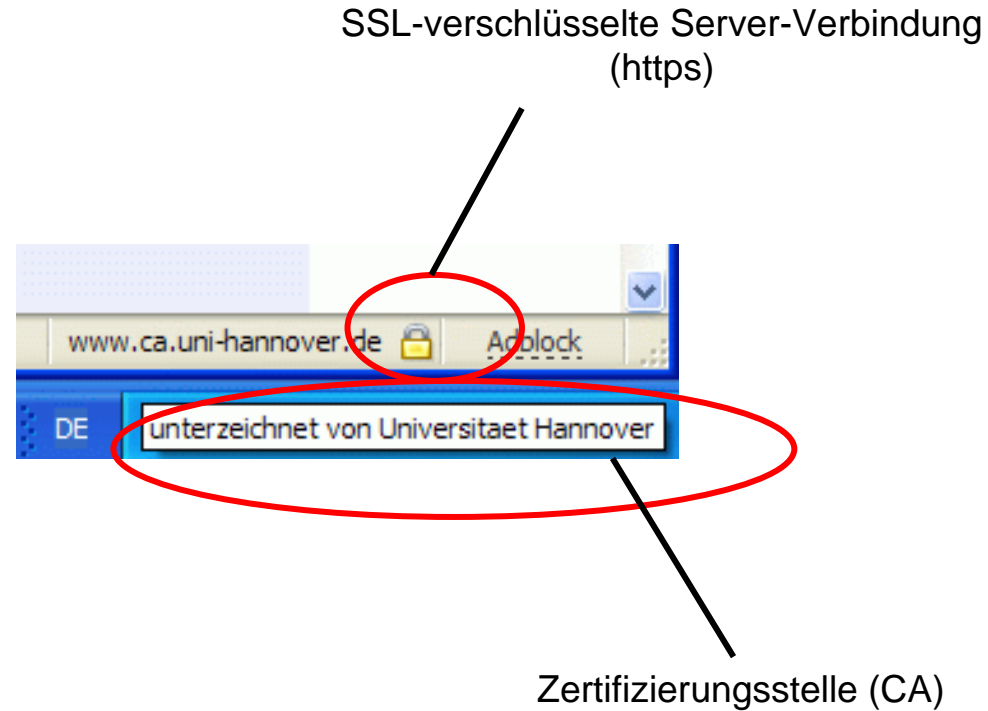
Verfahren wählen



Darstellung beim Empfänger

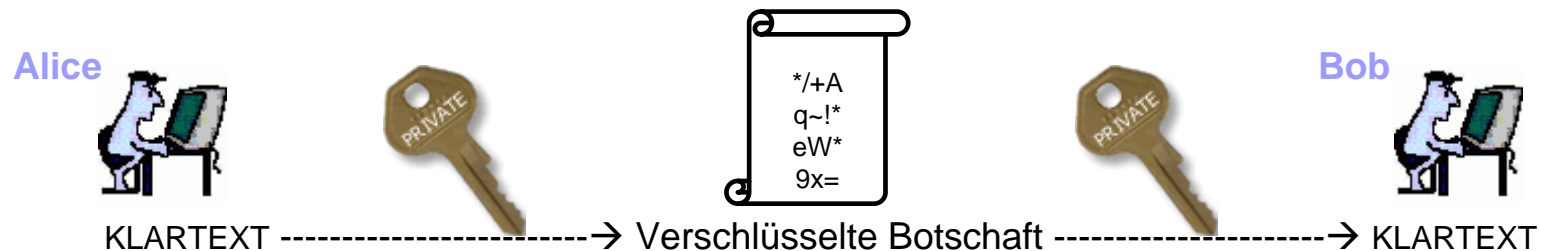


■ Gesicherte Kommunikation mit Servern



■ 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



TWO KEYS
1 Public
1 Private

- 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

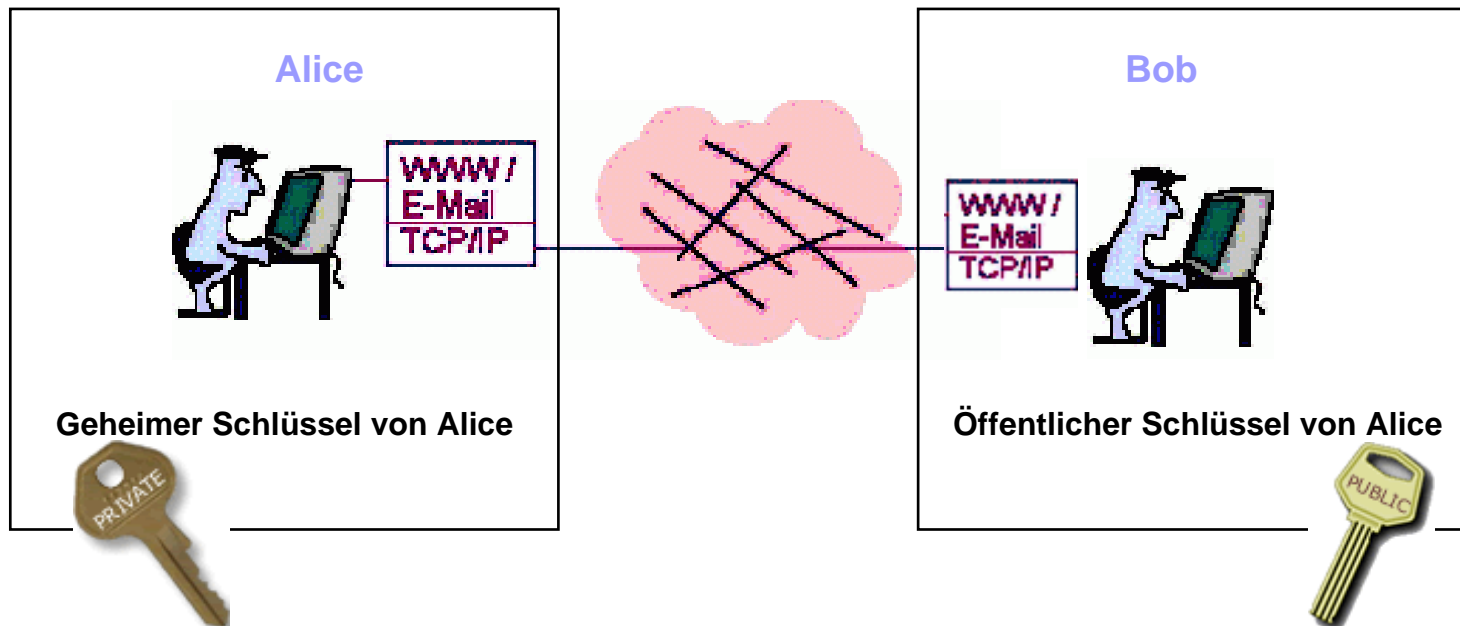
Nachteil: schlechte Performance

■ Anwendungsbeispiel für asymmetrische Verschlüsselung (1)

■ Signieren

gewährleistet

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

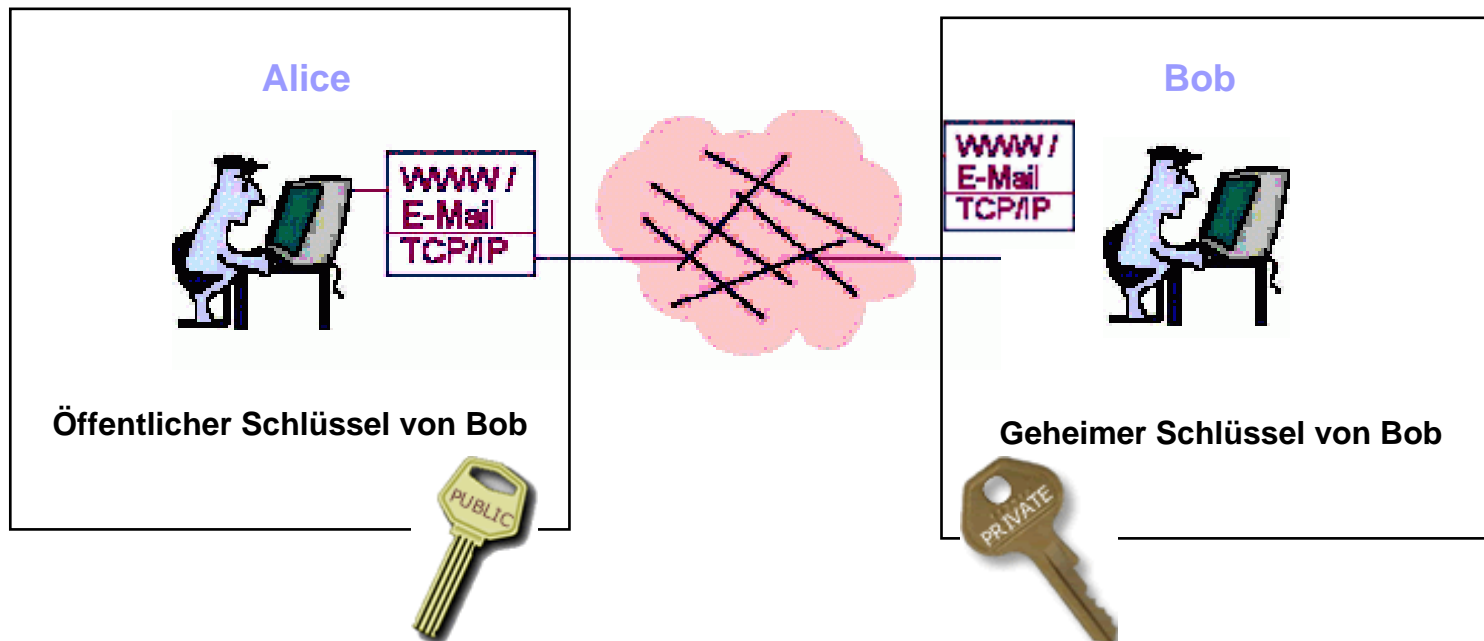


■ Anwendungsbeispiel für asymmetrische Verschlüsselung (2)

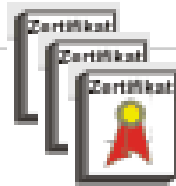
■ Verschlüsseln

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.

- Zertifizierungsstelle der Universität Hannover seit Mai 2004

- Zertifizierungsrichtlinien zum Betrieb

- 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



■ 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)*

...



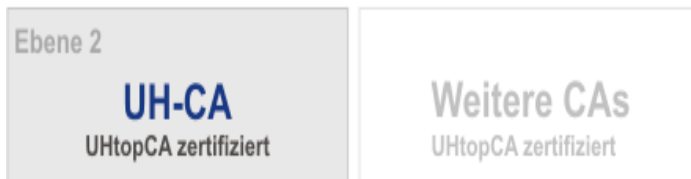
Policy

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>*

Zertifizierungshierarchie

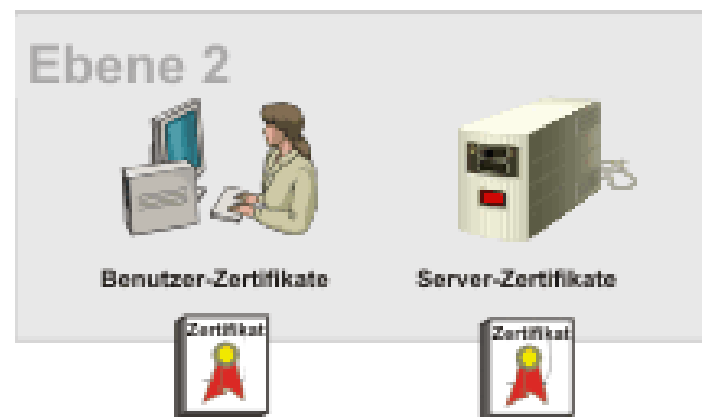
Alte Policy, Laufzeit bis 25.05.2006:

DFN CERT DFN-PCA Wurzelzertifikat
(selbstzertifiziert)



Neue Policy, Laufzeit ab Juni/Juli 2005:

DFN CERT DFN-PCA Wurzelzertifikat
(selbstzertifiziert)



■ Aufgaben der PKI

■ Bearbeitung von Zertifizierungsanträgen

- Webinterface
- Schriftliche Teilnehmererklärung
- Persönliche Identifizierung

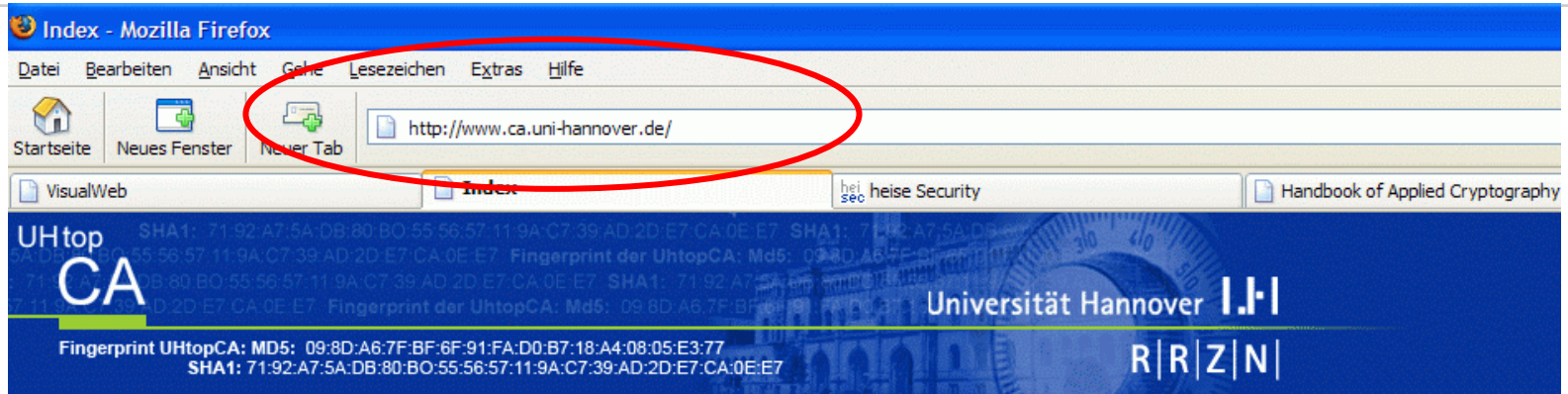
■ Ausstellen von Zertifikaten

■ 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



- Home
- CA-Zertifikate
- Zertifizierungsrichtlinien
- Zertifizierungshierarchie
- UHtopCA
- UH-CA
 - Antrag auf Zertifizierung
 - Leitfaden
 - Anleitungen
 - FAQ
 - Teilnehmer-Erklärung
 - Ausgestellte Zertifikate
 - Sperrlisten

Zertifizierung an der Universität Hannover

Im Rahmen der PKI an der Universität Hannover betreibt das [RRZN](#) die folgenden Zertifizierungsstellen (Certification Authorities (CAs)):

UHtopCA

Oberste Zertifizierungsinstanz der Universität Hannover;
zertifiziert ausschließlich **nachgeordnete Zertifizierungsstellen (CAs)**.

UH-CA

Nachgeordnete Zertifizierungsstelle der Universität Hannover;
stellt Zertifikate für **Mail Klienten und Server-Authentifizierung** aus.

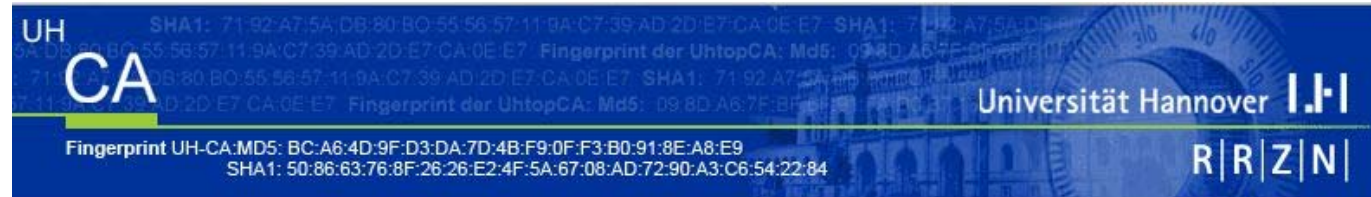
Zertifikate für die gesicherte E-Mail-Kommunikation:

- ◆ Um schnell und effizient ein Zertifikat zu erhalten, folgen Sie dem [Leitfaden](#).

Zertifikate zur Server-Authentifizierung:

- ◆ Laden Sie sich unter [Anleitungen](#) die entsprechende Benutzeranleitung herunter.

■ Zugriff auf ausgestellte Zertifikate (1)



- Home
- CA-Zertifikate
- Zertifizierungsrichtlinien
- Zertifizierungshierarchie
- UHtopCA
- UH-CA
- Antrag auf Zertifizierung
- Leitfaden
- Anleitungen
- FAQ
- Teilnehmer-Erklärung
- Ausgestellte Zertifikate**
- Sperrlisten

Zertifikate UH-CA

Die von der UH-CA ausgestellten Zertifikate sind zur Zeit nur über den [Public PKI-Server](#) verfügbar.



■ Zugriff auf ausgestellte Zertifikate (2)

OpenCA

CA

- [Download des CA-Zertifikates](#)
- [Zertifikatsrückruflisten](#)

Nutzer

- [Beantragen eines Zertifikates](#)
- [Download des beantragten Zertifikates](#)
- [Zertifikatstest](#)
- [Rückruf](#)

Zertifikate

- [Gültige](#)
- [Abgelaufene](#)
- [Zurückgerufene](#)
- [Suspendierte](#)
- [Suche](#)

Anträge

Public PKI Server

Dieser Server stellt alle nötigen Informationen für die Nutzer der Zertifizierung bereit. Bitte laden Sie als erstes [hier](#) die Zertifikate der übergeordneten Zertifikatsstelle.

Initialisierung

[Download des CA-Zertifikates](#)
[Importieren Sie es in Ihren Browser]

Verwaltung Ihrer Zertifikate

[Beantragen eines Zertifikates](#)
[Zertifizierung beantragen]

Zugriff auf ausgestellte Zertifikate (3)

OpenCA

CA

- Download des CA-Zertifikates
- Zertifikatsrückruflisten

Nutzer

- Beantragen eines Zertifikates
- Download des beantragten Zertifikates
- Zertifikatstest
- Rückruf

Zertifikate

- Glütige
- Abgelaufene
- Zurückgerufene
- Suspendierte
- Suche

Anträge

- Zertifizierungsanträge
- Rückrufanträge

Valid Certificates

Die Liste wurde zuletzt aktualisiert am **Sat Jun 4 15:16:43 2005 GMT**.

Extra References > >>

Serial	Common Name	Issued on	E-Mail	Role
6	Ansgar Giesker	Jun 10 11:55:08 2004 GMT	giesker at rrzn.uni-hannover.de	Benutzer
7	Steffen Schulze-Kremer	Jul 8 08:50:01 2004 GMT	schulze-kremer at rrzn.uni-hannover.de	Benutzer
8	Reinhard Obendorf	Jul 8 08:50:51 2004 GMT	obendorf at RRZN.uni-hannover.de	Benutzer
9	Eberhard Froriep	Jul 9 07:32:02 2004 GMT	froriep at rrzn.uni-hannover.de	Benutzer
10	Christine Peter	Jul 22 09:05:15 2004 GMT	peter at rrzn.uni-hannover.de	Benutzer
11	Christian Grimm	Jul 30 09:18:03 2004 GMT	grimm at rvs.uni-hannover.de	Benutzer
12	www.rvs.uni-hannover.de	Jul 30 09:18:32 2004 GMT	www at rvs.uni-hannover.de	Web Server
14	cip13.amp.uni-hannover.de	Aug 12 12:03:18 2004 GMT	paul at physik.uni-hannover.de	Web Server
15	www.itp.uni-hannover.de	Aug 17 11:10:40 2004 GMT	webmaster at itp.uni-hannover.de	Web Server
16	Denis Goehr	Aug 19 07:46:11 2004 GMT	goehr at rvs.uni-hannover.de	Benutzer
17	Dirk Hennig	Aug 19 08:08:25 2004 GMT	dhennig at rrzn.uni-hannover.de	Benutzer
18	hawaii.rvs.uni-hannover.de	Aug 24 09:26:27 2004 GMT	wiebelitz at rvs.uni-hannover.de	Mail Server
19	lanai2.rvs.uni-hannover.de	Aug 24 09:26:52 2004 GMT	wiebelitz at rvs.uni-hannover.de	Mail Server
20	Stefan Piger	Aug 25 07:33:27 2004 GMT	piger at rvs.uni-hannover.de	Benutzer
21	Anne Schubach	Aug 25 11:56:53 2004 GMT	schubach at ifgb.uni-hannover.de	Benutzer
23	grelay.rrzn.uni-hannover.de	Sep 3 10:38:52 2004 GMT	gorden at rrzn.uni-hannover.de	Mail Server
24	Juergen Gaertner	Sep 8 10:21:33 2004 GMT	gaertner at rrzn.uni-hannover.de	Benutzer
25	Olga Urbach	Sep 9 07:26:00 2004 GMT	urbach at rrzn.uni-hannover.de	Benutzer
26	Jochen Paul	Sep 9 10:13:33 2004 GMT	paul at physik.uni-hannover.de	Benutzer
27	mail.sra.uni-hannover.de	Sep 22 07:43:51 2004 GMT	postmaster at sra.uni-hannover.de	Mail Server

© 1998-2002 by Massimiliano Pala and the OpenCA Group.
PKI Public Server - Version 0.9.1

Zugriff auf Sperrlisten



- Home
- CA-Zertifikate
- Zertifizierungsrichtlinien
- Zertifizierungshierarchie
- UHtopCA
- UH-CA
- Antrag auf Zertifizierung
- Leitfaden
- Anleitungen
- FAQ
- Teilnehmer-Erklärung
- Ausgestellte Zertifikate
- Sperrlisten**

Sperrlisten der UH-CA

Diese Seite enthält die aktuellsten Sperrlisten (CRLs - Certificate Revocation List) der UH-CA. Laden Sie sich diese CRLs in regelmäßigen Abständen herunter, um einen möglichst aktuellen Status für Ihren Browser oder Mailclients zu erreichen.

Die Sperrlisten werden mindestens einmal pro Monat von der UH-CA aktualisiert und stehen in den folgenden Formaten zur Verfügung. Zum Importieren klicken Sie bitte einfach auf den passenden Link.

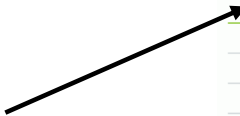
Format	Erläuterung
PEM	PEM-Format z.B. für Webserver, ASCII-codierte Form
DER	Browserimportierbare CRL
TXT	Textformat zum Ansehen, die Seite kann sehr lang werden
CRL	Primäre Rückrufliste

Antrag auf ein persönliches E-Mail-Zertifikat

UH CA
Fingerprint UH-CA: MD5: BC:A6:4D:9F:D3:DA:7D:4B:F9:0F:F3:B0:91:8E:A8:E9
SHA1: 50:86:63:76:8F:26:26:E2:4F:5A:67:08:AD:72:90:A3:C6:54:22:84

Universität Hannover I.H.I
R|R|Z|N

- Home
- CA-Zertifikate
- Zertifizierungsrichtlinien
- Zertifizierungshierarchie
- UHtopCA
- UH-CA
- Antrag auf Zertifizierung
- Leitfaden**
- Anleitungen
- FAQ
- Teilnehmer-Erklärung
- Ausgestellte Zertifikate
- Sperrlisten



Leitfaden zur Zertifizierung

10 Schritte bis zum Zertifikat für das Signieren und Verschlüsseln Ihrer E-Mail Kommunikation

Anleitung	Hilfsthemen für Browser
1. Das aktuelle Wurzelzertifikat der DFN-PCA in den Browser installieren.	Netscape IE
2. Das aktuelle Zertifikat der UHtopCA in den Browser installieren.	Netscape IE
3. Das aktuelle Zertifikat der UH-CA in den Browser installieren.	Netscape IE
4. Die Zertifizierungsrichtlinien (Policy) der UHtopCA durchlesen.	
5. Die Teilnehmer-Erklärung durchlesen und ausdrucken.	Netscape IE
6. Auf dem Öffentlichen PKI Server der UH-CA ein neues Zertifikat beantragen.	Netscape IE
7. Dabei die Teilnehmer-Erklärung ausfüllen und unterschreiben.	Netscape IE
8. Ausweis und Teilnehmer-Erklärung im RRZN bei einem RA-Operator vorlegen.	
9. Nach Erhalt der Antwort-E-Mails das Zertifikat in den Browser importieren.	Netscape IE
10. Das Zertifikat im Zertifikats-Manager des Browsers auf Diskette sichern!	Netscape IE

- 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!

