

Vertrauenswürdige Kommunikation durch digitale Signaturen

Sicherheitstage WS 05/06

Birgit Gersbeck-Schierholz, RRZN

Schlüsselweitwurf

Zum besseren Verständnis alles auf symmetrische V. projizieren: hybride Verfahren asym. V. wird nur für den geheimen Schlüsseltausch benötigt

Motivation und Grundlagen:

- Sicherheitsziele der digitalen Signatur
- Kryptografische Techniken
- Funktion einer CA

Zertifikate von der UH-CA:

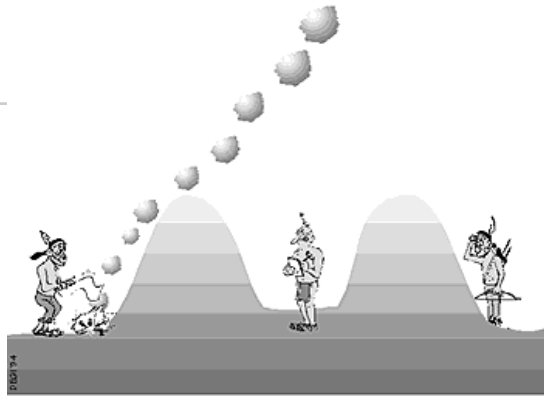
- Konkrete Einsatzgebiete
- *Beantragungsverfahren*
- *Neues Web-Frontend der UH-CA*

PKI:

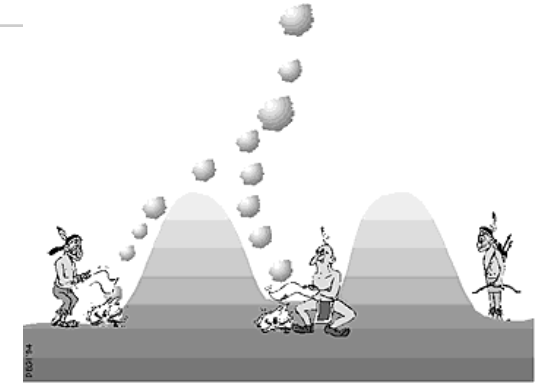
- DFN-weite Public Key Infrastruktur
- UH-CA, Zertifizierungsinstanz der Universität Hannover

Sicherheitsziele der digitalen Signatur

R | R | Z | N |

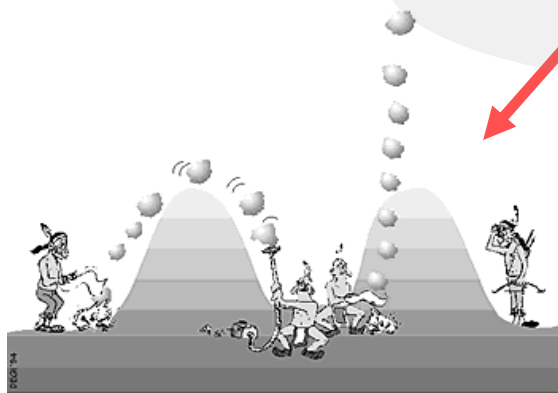


Mitlesen der Daten
durch Dritte

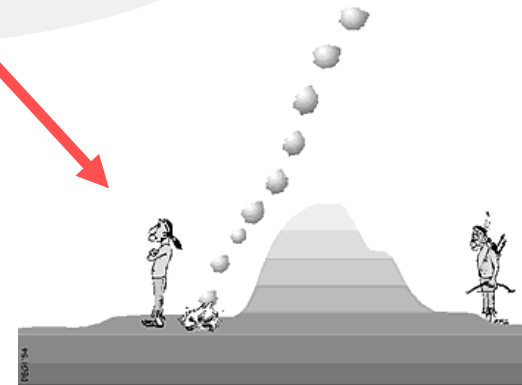


Verändern der Daten

Bekannte Risiken der Internet-Kommunikation

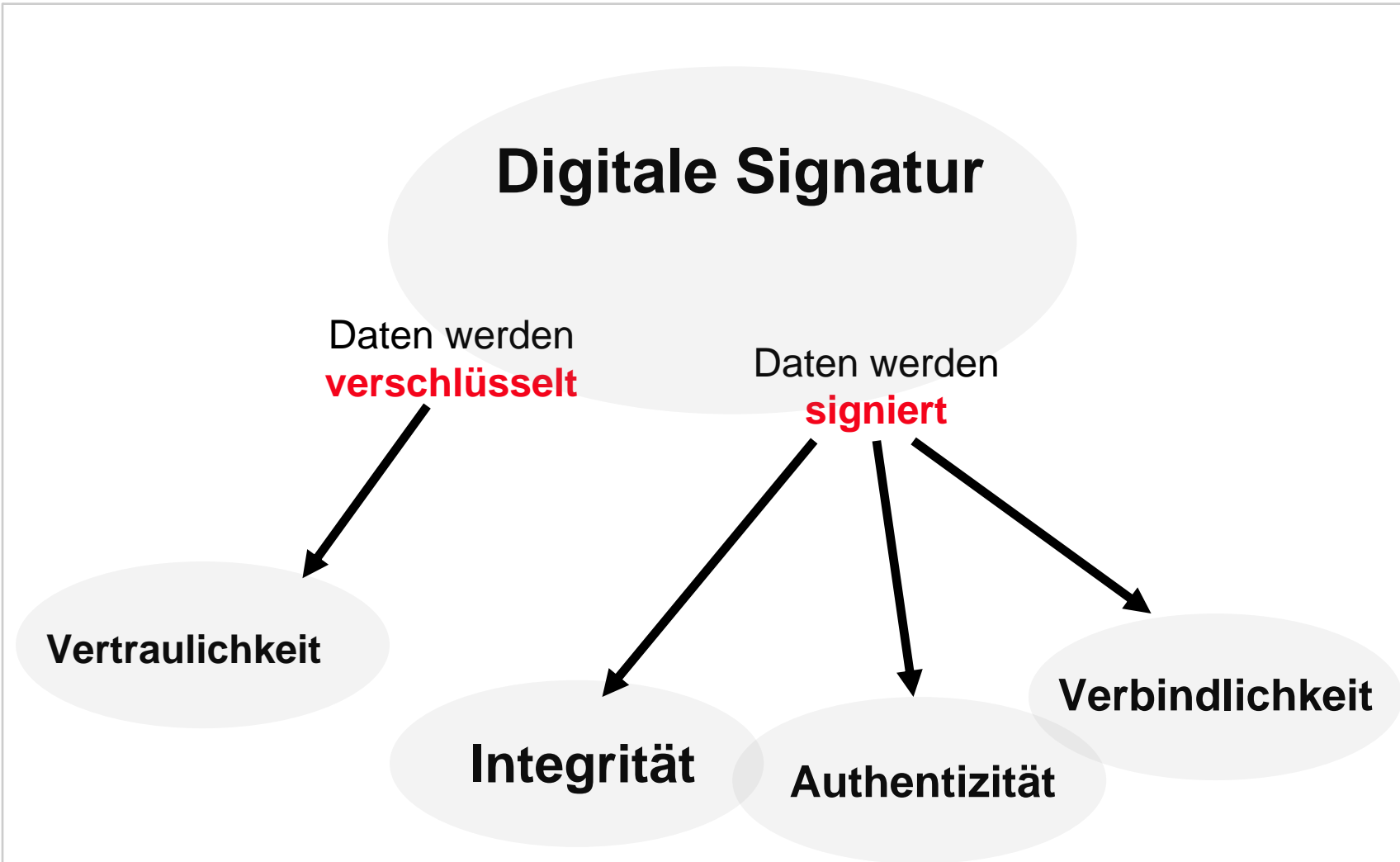


Fälschen der Identität
des Absenders



Abstreiten der Daten

Quelle der Grafiken: CryptMail User's Guide, Copyright © 1994 Utimaco Belgium



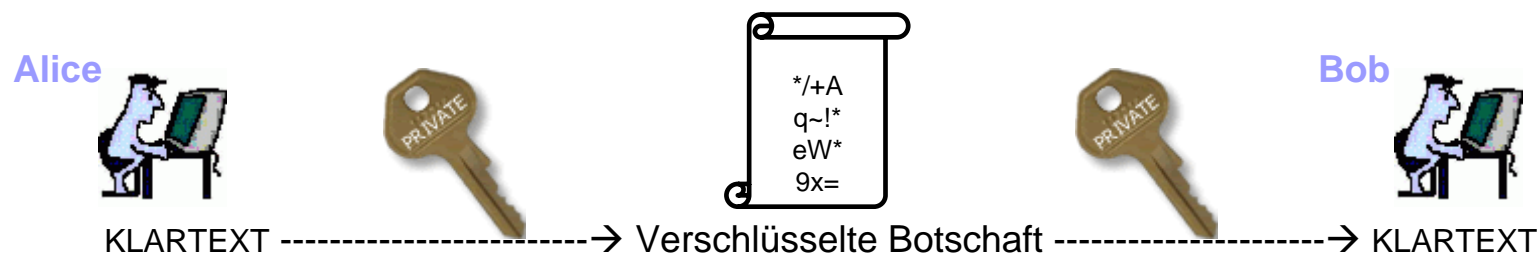
- **Digitale Zertifikate sind elektronische Dateien, die Personen und Server eindeutig identifizieren**
- **Digitale Zertifikate ermöglichen die authentische und vertrauliche Kommunikation über das Internet**



Kryptografische Techniken

■ Symmetrische Verschlüsselung

- Ältestes Verfahren zur Verschlüsselung -> „Cäsar-Chiffre“
- Moderne Symmetrische Verschlüsselungsverfahren:
 - 3DES, IDEA, Blowfish, AES usw. (Schlüssellänge derzeit ca. 128 – 196 bit)
- Beide Kommunikationspartner benutzen **den gleichen** Schlüssel zur Ver- und Entschlüsselung



Prinzip: Es gibt nur einen Schlüssel (Geheimnis)

Vorteil: Sicheres Verfahren mit guter Performance aufgrund rel. geringer Schlüssellängen

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

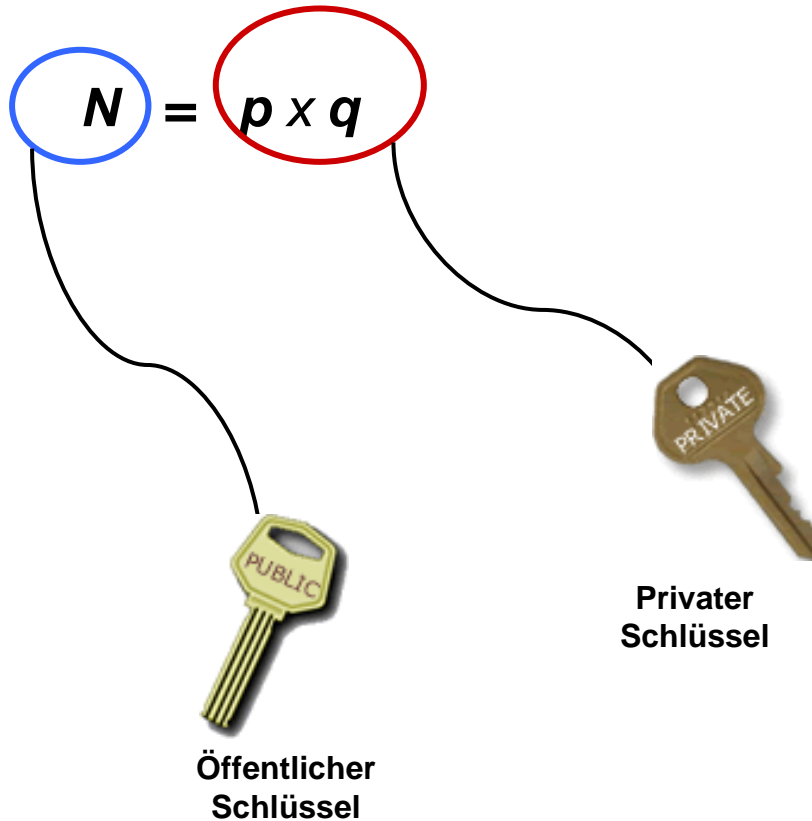
- Gibt es seit 1976 (Diffie/Hellmann)
- Das Revolutionäre war damals **die Idee die Schlüssel zum Ver- und Entschlüsseln zu trennen**
- Jeder Kommunikationspartner verfügt über ein **Schlüsselpaar**, dieses besteht aus 2 unterschiedlichen Schlüsseln:
 1. **Geheimer Schlüssel** (*private key*) zum Verschlüsseln (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!

- **Worauf basiert die Asymmetrische Verschlüsselung?**
 - Einwegfunktionen (Primzahlen, diskrete Logarithmen, elliptische Kurven)

- **Aktuelle Verfahren:**
 - 1976 Diffie-Hellmann (Schlüsseltausch)
 - Diskrete Logarithmen
 - 1977 **RSA** – Rivest, Shamir, Adleman
 - Primzahlen
 - El´Gamal
 - Diskrete Logarithmen
 - 1985 Elliptische Kurven (ECC)
 - 1994 DAS – Digital Signature Algorithm
 - Modifikation des El´Gamal-Verfahrens

■ RSA

- Basiert im Wesentlichen auf der Schwierigkeit der Primfaktorzerlegung



p und q sind sehr große Primzahlen

- Exkurs: **Wie sicher ist die asymmetrische Verschlüsselung?**
 - Bei Auswahl hinreichend großer Primzahlen können p und q nicht ermittelt werden

Beispiel: **RSA-640**

$N =$ 310 7418240490 0437213507 5003588856 7930037346 0228427275 4572016194
8823206440 5180815045 5634682967 1723286782 4379162728 3803341547
1073108501 9195485290 0733772482 2783525742 3864540146 9173660247
7652346609

wurde am **2. November 2005** faktorisiert und zwar in:

$p =$ 1634733 6458092538 4844313388 3865090859 8417836700 3309231218
1110852389 3331001045 0815121211 8167511579

×

$q =$ 1900871 2816648221 1312685157 3935413975 4718967899 6851549366
6638539088 0271038021 0449895719 1261465571

→20.000 US-Dollar

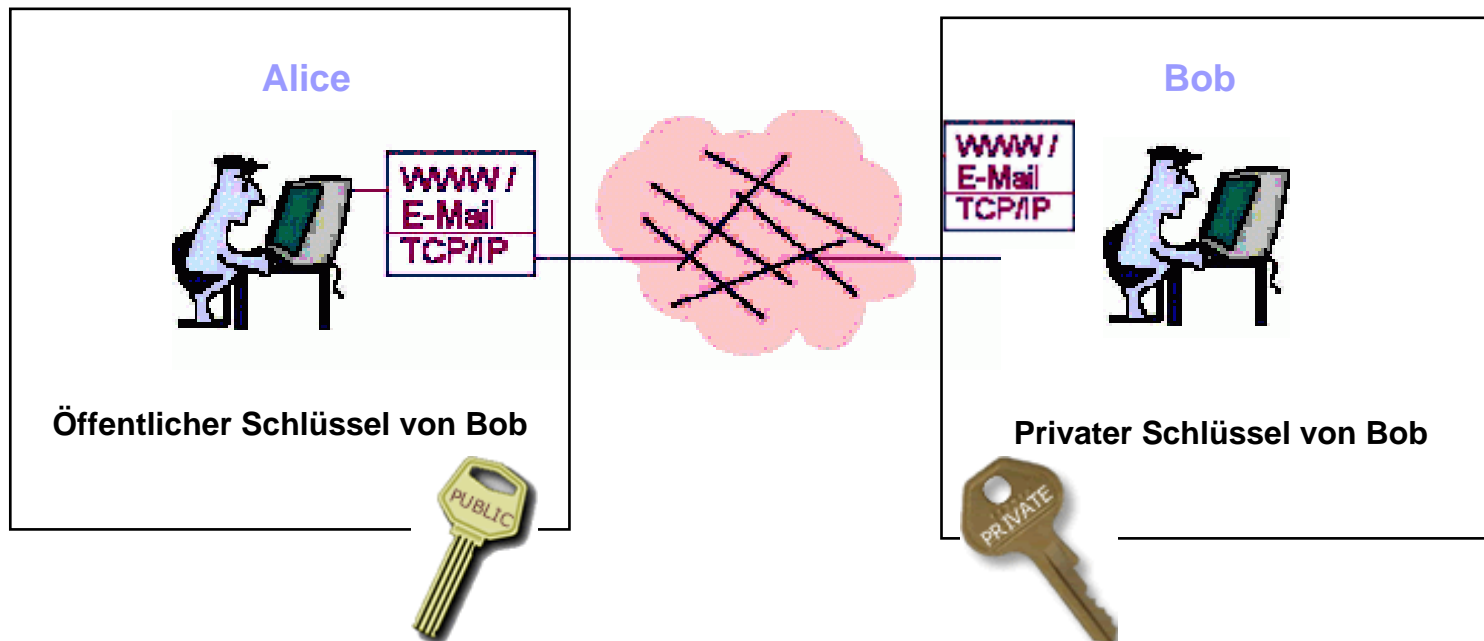
<http://www.rsasecurity.com/rsalabs/node.asp?id=2093>

- Die aktuell für RSA-Verschlüsselungsverfahren empfohlenen Schlüssellängen von **1024** und **2048** Bit können mit praktikablen Mitteln nicht entschlüsselt werden

■ Asymmetrische Verschlüsselung: **Daten verschlüsseln**

gewährleistet

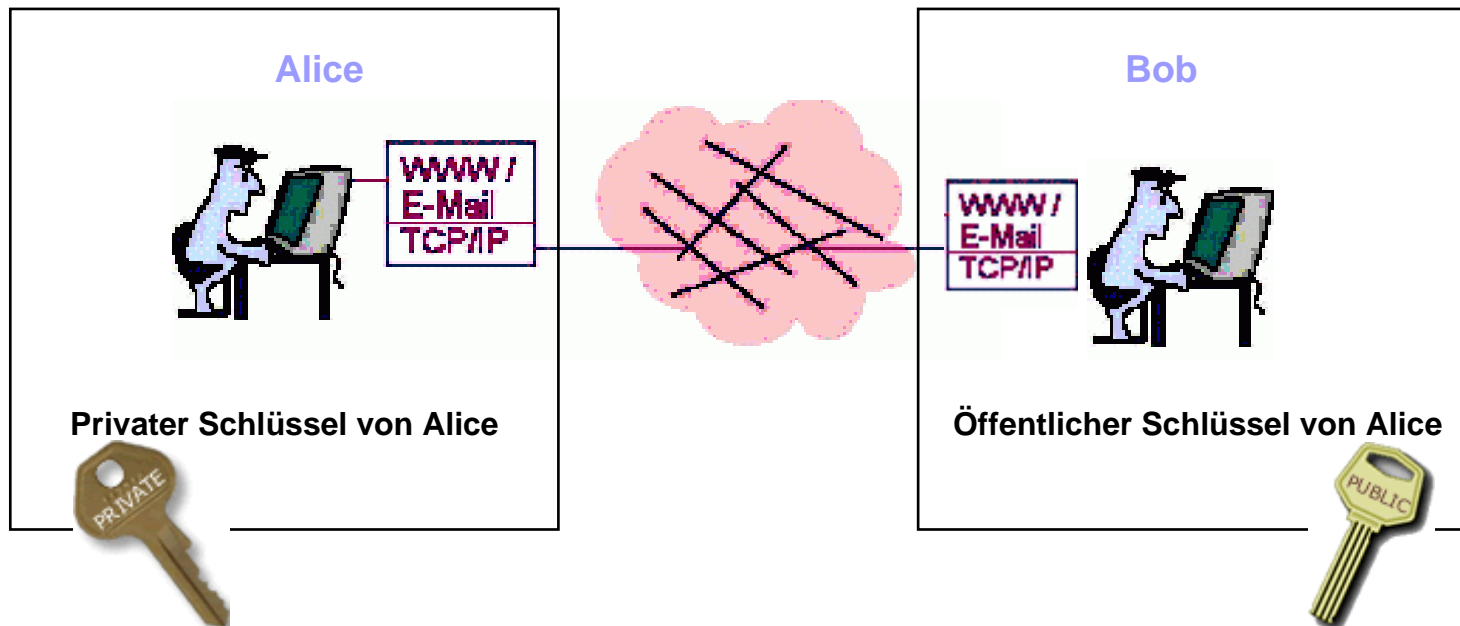
- Vertraulichkeit : Daten können von Dritten nicht gelesen werden



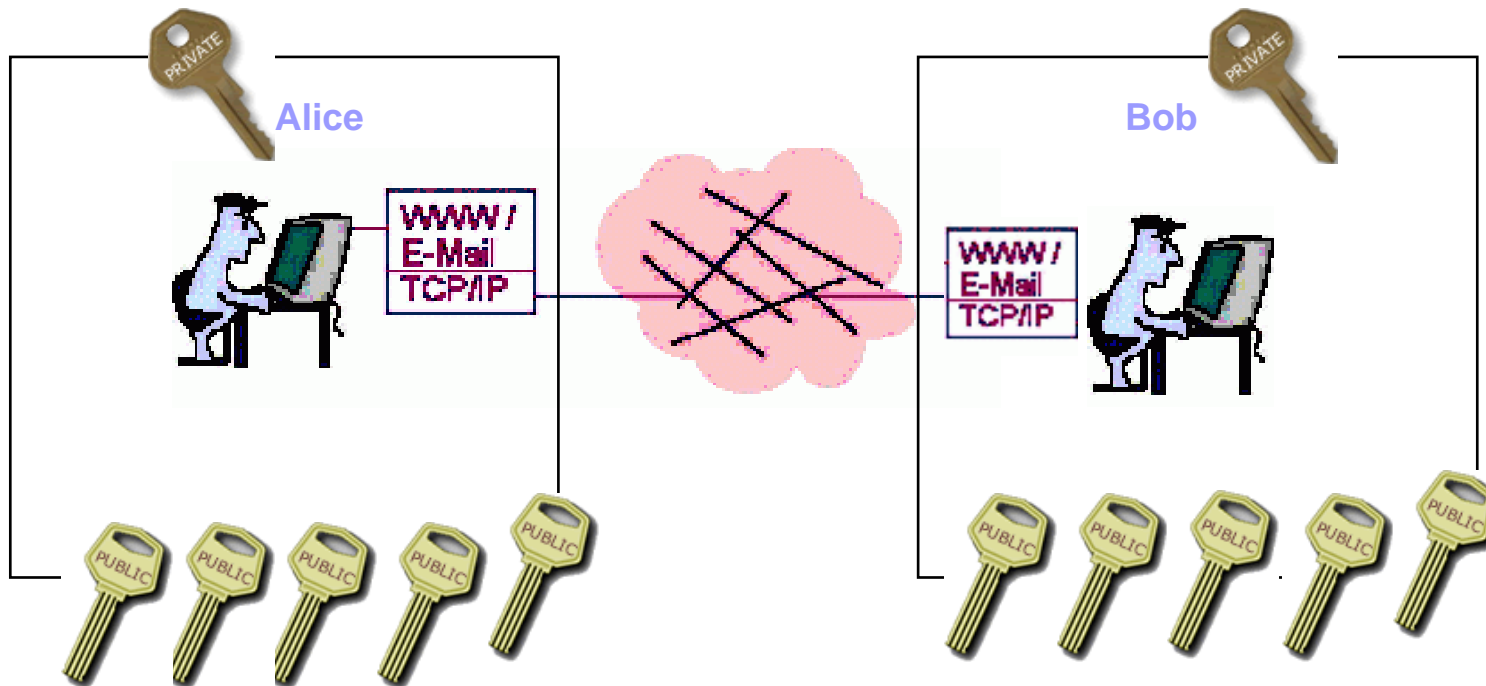
■ Asymmetrische Verschlüsselung - Daten signieren

gewährleistet

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

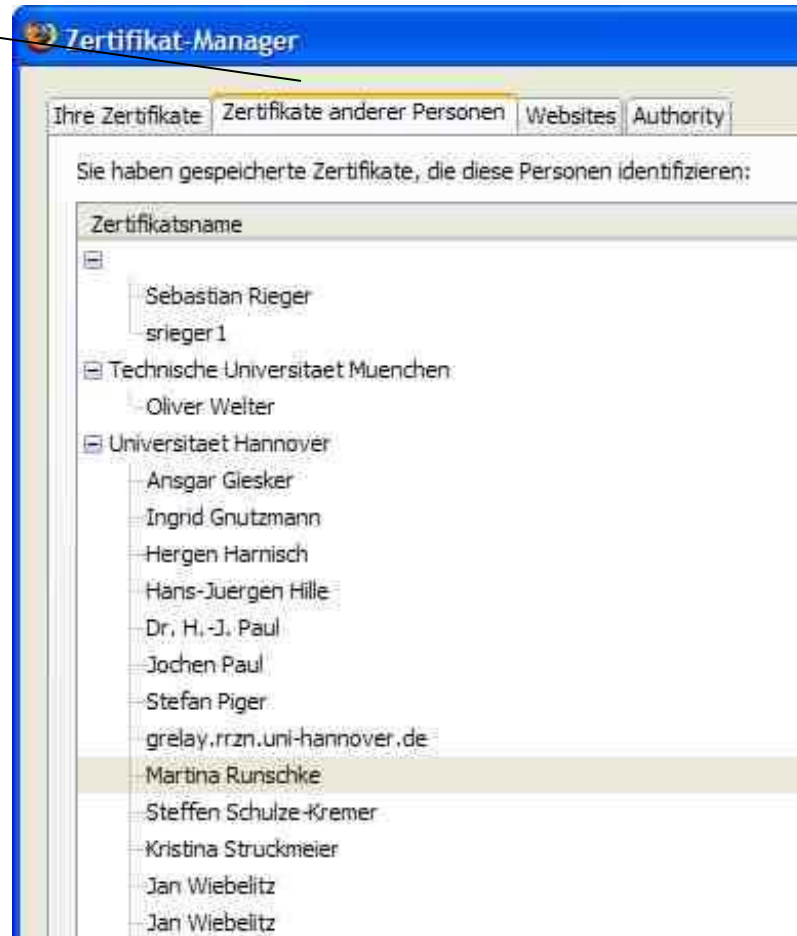


- **Nutzer verfügt in der Regel über**
 - **mehrere** (viele) Öffentliche Schlüssel (jeweils einen pro Kommunikationspartner)
 - **einen** privaten Schlüssel



■ Schlüsselmanagement im Browser und Mailklienten

Öffentliche Schlüssel der Kommunikationspartner

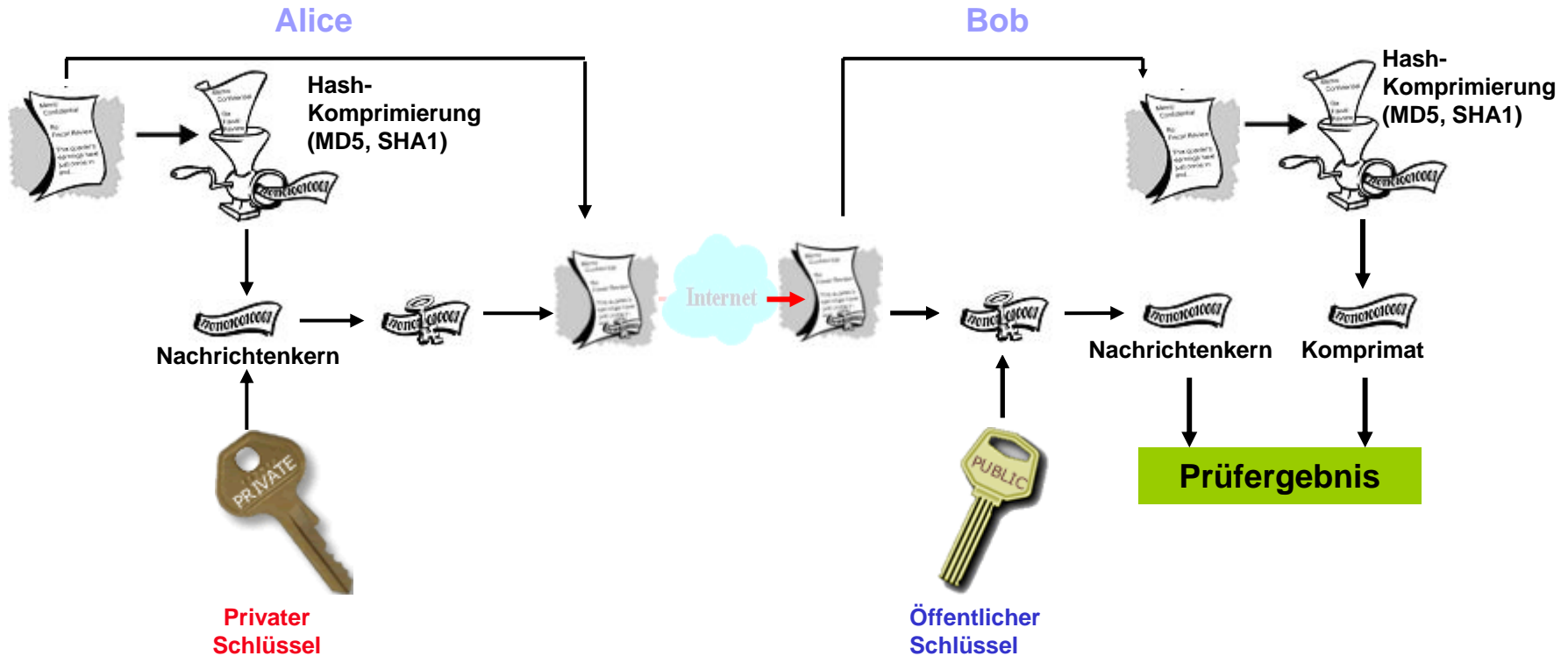


■ Prüfsummen/Hashverfahren

- Verschlüsselung ohne Schlüssel
- Hash-Wert:
 - Ein „digitaler Fingerabdruck“ eines Objektes
 - Verkürzung des Objektes auf einen „Identifikator“

- Aktuelle Verfahren
 - HAVAL (basierend auf MD5)
 - HMAC
 - MD2, MD4, **MD5**
 - RIPEMD-160
 - **SHA-1** (basierend auf MD4)
 - SHA-256 (basierend auf MD4)
 - SHA-512 (basierend auf MD4)
 - SNEFRU

■ Schematische Darstellung des Signiervorganges (Hybrides Verfahren)



Schlüssel und Zertifikate

- **Kann man den Angaben im öffentlichen Schlüssel vertrauen?**
 - Wie kann ich erkennen, wem ein öffentlicher Schlüssel wirklich gehört oder ob ich schon eine Fälschung besitze?
 - 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).
 - Ein vertrauenswürdiger Dritter kann mittels einer Urkunde/Zertifikat den Schlüssel beglaubigen

- **Zertifikate**
 - Beglaubigung von Schlüsseln
 - stellen die eindeutige, zweifelsfreie Zuordnung zwischen einem Schlüsselpaar und einer Person oder einem Rechner her
 - Dabei wird die **reale Identität** an die **digitale Identität** gebunden

- **Zertifizierungsinstanz, CA (Certification Authority)**
 - Vertrauenswürdiger Dritte
 - Nach Prüfung von Identität und öffentlichem Schlüssel, stellt die CA das Zertifikat aus

- ein **Zertifikat** nach dem **Standard X.509v3** besteht im Wesentlichen aus 4 Teilen:

Öffentlicher Schlüssel



```
00:ab:77:e0:53:4a:4a:6b:42:8b:e0:4b:91:14:6f:
df:e7:28:4f:58:e5:43:b5:01:71:fa:24:2f:6c:4e: ...
39:04:62:2f:fd:20:4a:a3:d0:00:78:c8:e7:44:7a
```

Angaben über den Schlüsselinhaber
(Common Name nach X.509v3)

```
C=DE, O=Universitaet Hannover,
OU=RRZN, CN=Birgit Gersbeck-
Schierholz/serialNumber=3
```

Attribute wie Seriennummer und
Gültigkeitsdauer

```
Serial Number: 3 (0x3)
Signature Algorithm: sha1WithRSAEncryption
Validity   Not Before: May 26 15:42:55 2004 GMT
           Not After : May 26 15:42:55 2005 GMT
```

Beglaubigung (digitale Signatur) der CA,
dass die Angaben stimmen



```
-----BEGIN CERTIFICATE-----
...MBwGA1UEChMVVW5pdmVyc2l0YWV0I
m5vdmVyMRAwDgYDVQQLEAdSUlpOX0NB...
sDUNW/3L63Epioz xuah/9jzoLI+/Q32Dg==
-----END CERTIFICATE-----
```

■ X.509 Hierarchie

- Aufbau einer Zertifikatkette
- Dadurch, dass die CA wiederum von einer übergeordneten Zertifizierungsstelle beglaubigt wird, entsteht eine Hierarchie des Vertrauens
- Die Aussteller-Signatur in einem Zertifikat ist jeweils mit dem privaten Schlüssel des Ausstellers verschlüsselt worden
- Mit dem im Zertifikat enthaltenen öffentlichen Schlüssel kann das in der Hierarchie darüber liegende Zertifikat verifiziert werden

■ Zertifikat : Angaben im Browser



Zertifikatnehmer

Zertifizierungsstelle

Gültigkeitszeitraum

Fingerabdruck, Hashfunktionen
MD5 und SHA1

■ Zertifikat : Angaben im Browser

The screenshot shows a browser window titled "Zertifikat-Ansicht: 'CA der Universitaet Hannover (UH-CA), G02 - DFN-Ver...". The window has two tabs: "Allgemein" (selected) and "Details". Below the tabs, it states "Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:" followed by a list containing "SSL-Zertifizierungsstelle".

The main content is divided into several sections:

- Herausgegeben für:**
 - Allgemeiner Name (CN): CA der Universitaet Hannover (UH-CA), G02
 - Organisation (O): Universitaet Hannover
 - Organisationseinheit (OU): RRZN_CA
 - Seriennummer: 06:D0:D6:6F
- Herausgegeben von:**
 - Allgemeiner Name (CN): DFN-Verein PCA Classic - G01
 - Organisation (O): DFN-Verein
 - Organisationseinheit (OU): DFN-PKI
- Validität:**
 - Herausgegeben am: 16.06.05
 - Läuft ab am: 16.06.09
- Fingerabdrücke:**
 - SHA1 Fingerprint: FE:1A;DC:29:58:E2:FD:9D:C5:FF:B5:65:5D:60:85:B2:6F:3A:9C:64
 - MD5 Fingerprint: 4C:12:14:13:14:81:48:79:D8:BA:25:75:67:63:5F:88

ZERTIFIKAT des Zertifikatnehmers UH-CA

1. **public key** der UH-CA
2. Mit **private key** der DFN-PCA verschlüsselte Signatur

ZERTIFIKAT der Zertifizierungsstelle DFN-PCA

1. **public key** der DFN-PCA
2. Mit **private key** der darüberliegenden Instanz verschlüsselte Signatur (da Root-CA, selbstzertifiziert)

Digitale Zertifikate - praktische Anwendung

■ S/MIME Zertifikate

- Persönliches Zertifikat zum Unterschreiben (signieren) und Verschlüsseln von E-Mail

■ SSL Server-Zertifikate

- Ermöglicht gesicherten Datenaustausch nach einer Server-Authentifizierung
- Gewährleistet damit Vertraulichkeit, Integrität, einseitige Authentifizierung

■ SSL Client-Zertifikate

- Ermöglicht gesicherten Datenaustausch nach Authentifizierung beider Kommunikationspartner
- Gewährleistet damit Vertraulichkeit, Integrität, beidseitige Authentifizierung und ersetzt so Credentials wie z. B. Username-Passwort-Paare -> „Single Sign On“

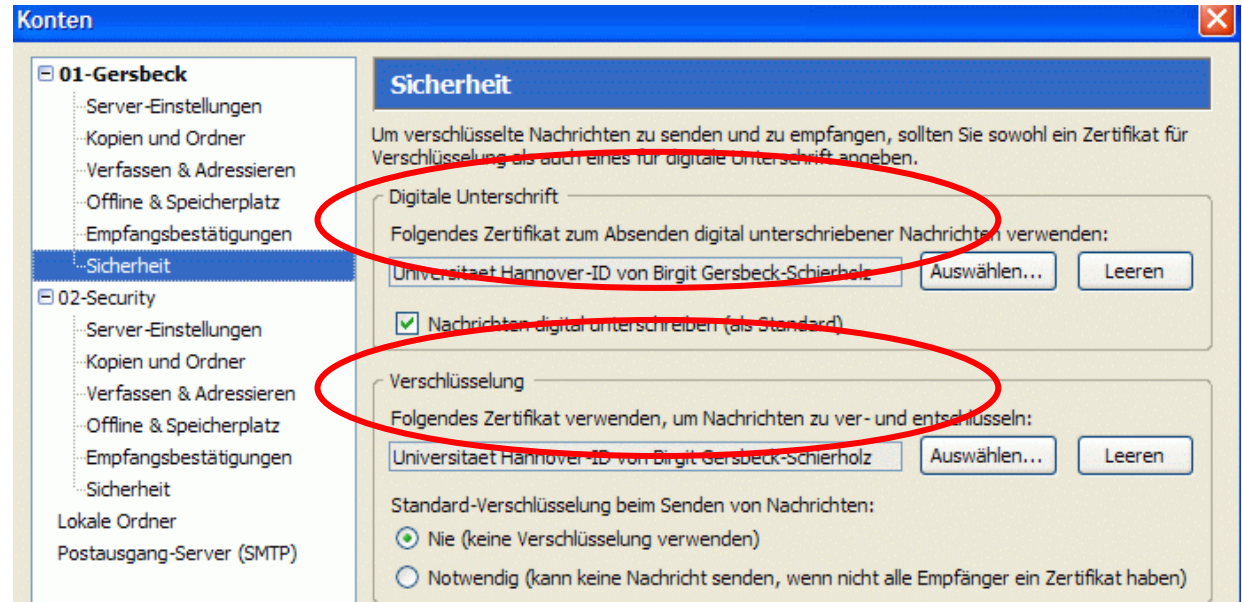
■ Code Signing

- Gewährleistet Authentizität und Integrität von Programm-Code (z.B. Office-Macros)

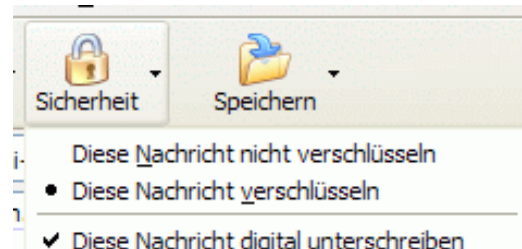
■ Signieren und Verschlüsseln von E-Mail

(Beispiel: Thunderbird)

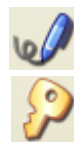
Implementieren:



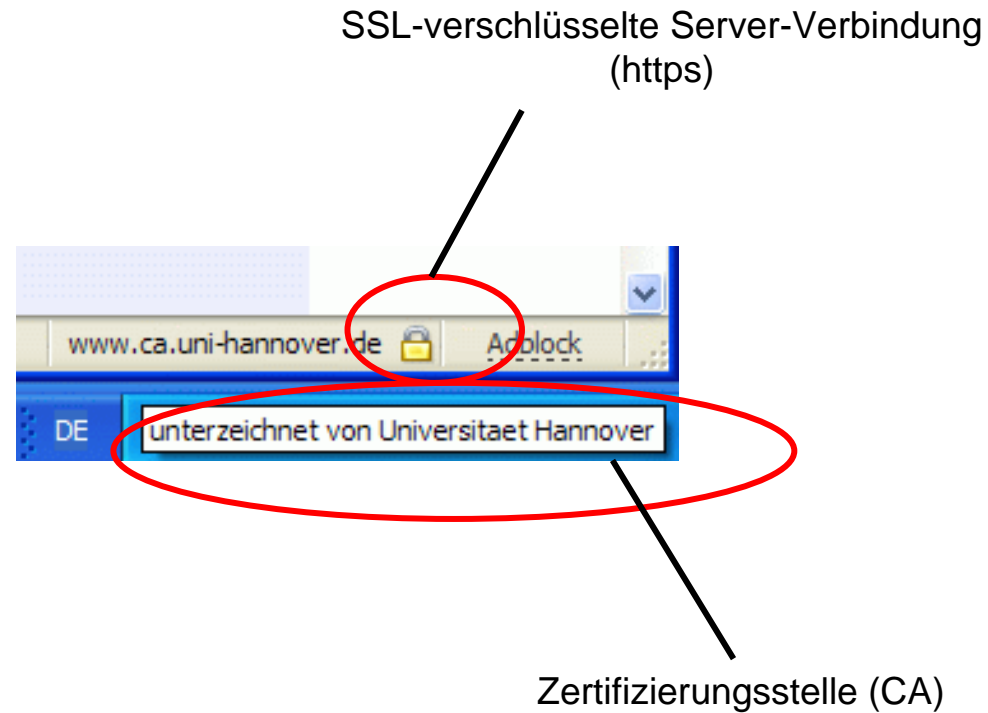
Verfahren wählen:



Darstellung beim Empfänger:



■ Gesicherte Kommunikation mit Servern



■ Warum HTTPS?

■ Weil HTTP...

- ... nicht die Vertraulichkeit der Daten gewährleistet
- ... keine Möglichkeit bietet die Integrität der Daten zu prüfen
- ... nur äußerst unzureichende Methoden zur Authentisierung liefert
- ... Digest Authentisierung zwar ein verschlüsseltes Passwort überträgt, aber die weitere Kommunikation wieder unverschlüsselt abläuft

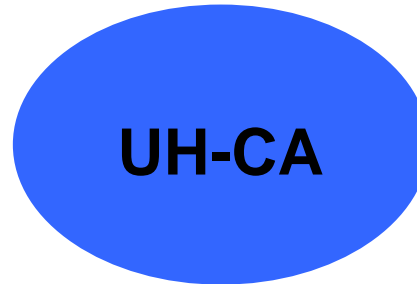
■ HTTPS Server

- Verfügen über ein X.509 Zertifikat
- Authentizität wird vom Klienten überprüft
- Kommunikation erfolgt verschlüsselt, z.B. Austausch von Formulardaten, Login, ..
- Können vom Klienten eine Authentisierung verlangen
- Gewährleisten Schutz vor Manipulation

Certification Authority: UH-CA

- Zertifizierungsstelle der Universität Hannover seit Mai 2004

- Benutzerschnittstelle:
www.rrzn.uni-hannover.de/zertifizierung.html



- Zertifiziert öffentliche Schlüssel für Nutzer und Server

- Zertifikate für Mitglieder der Universität Hannover

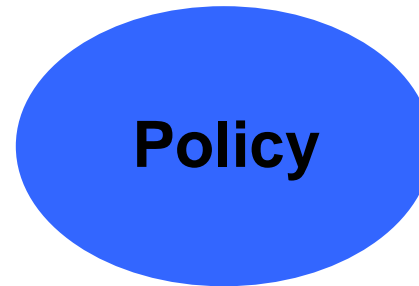
- Integriert in die PKI (Public Key Infrastructure) des Deutschen Forschungsnetzes

DFN
CERT

■ Zertifizierungsrichtlinien zum Betrieb der UH-CA

- Basis für das Vertrauen der Zertifikatnehmer und der Zertifikat-Nutzer („relying party“)

<http://www.rzrn.uni-hannover.de/uhca-policy.html>



- Beschreibt das Zertifikat-Format nach dem Standard X.509

- Definiert die Sicherheitsanforderungen an die CA

- *Persönliche Identifizierung der Teilnehmer*

- *Offline CA ...*

- Veröffentlichungsintervalle von Rückruflisten (CRLs)

■ **Bearbeitung von Zertifizierungsanträgen:**

- Online-Antrag
- 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**



■ DFN-PKI - alt und neu

Alte Policy, Laufzeit bis 25.05.2006:

DFN CERT DFN-PCA Wurzelzertifikat
(selbstzertifiziert)



Neue Policy, Laufzeit ab 16. Juni 2005:



Benutzerschnittstelle der UH-CA

The screenshot shows a web browser window with the URL <http://www.rrzn.uni-hannover.de/>. The page header features the RRZN logo and the text 'Regionales Rechenzentrum für Niedersachsen' and 'Universität Hannover'. A navigation bar includes links for 'A-Z', 'Hotline', 'Kontakt', 'Sitemap', and 'Intern'. Below the header is a grid of service categories:

- IT Sicherheitsmeldungen**
 - 22.11.2005
 - Warnung vor Schwachstelle im Internet Explorer
 - Handbuch**
 - 17.11.2005
 - Fortran 95 nachgedruckt
 - Virenmeldung**
 - 17.11.2005
 - Warnung vor neuer Sober-Variante
 - Handbuch**
 - 16.11.2005
 - C++ wieder erhältlich
 - News-Liste
- Organisation**
 - Über uns
 - Mitarbeiter
 - Nutzungsregelungen
 - Stellenangebote
 - Dienstleistungskatalog
- Netz**
 - Datennetz
 - Mail-Service
 - Netzdienste
 - Netzzugang
- Arbeitsplatzrechner**
 - PC/Workstation
 - Server
 - Anwendersoftware
 - Software-Info DB
 - Gerätebeschaffung
- Forschung & Lehre**
 - Rechnernetze
 - Forschung
 - Lehre
 - Publikationen
 - Software
- Zentrale Server**
 - Betriebskonzept
 - Anwendungen
 - Hochleistungsrechnen
 - Archiv/Backup
 - SAP
- IT-Sicherheit** (circled in red)
 - Antivirensoftware
 - Anwenderinfos
 - Administratoreninfos
 - Zertifizierung (UH-CA)
- Angebote**
 - Handbücher
 - Kurse
 - Druckausgabe
 - Softwaredistribution
 - Verkauf & Verleih
- Multimedia**
 - Audio/Video
 - 3D/Visualisierung
 - Digital Imaging
 - CD/DVD-Authoring
 - TYPO3

Startseite Neues Fenster Neuer Tab http://www.rrzn.uni-hannover.de/zertifizierung.html

Zertifizierung (UH-CA)

R|R|Z|N
Regionales Rechenzentrum für Niedersachsen

Universität Hannover

A-Z Hotline Kontakt Sitemap Intern

RRZN > IT-Sicherheit > Zertifizierung (UH-CA) >

Organisation
Forschung und Lehre
Netze
Zentrale Server
IT-Sicherheit
Antivirensoftware
Anwenderinfos
Administratoreninfos
Abo Security Mails
IT-Sicherheitsbeauftragt. UH
RRZN-Netzschutz
Zertifizierung (UH-CA)
FAQ
Arbeitsplatzrechner
Angebote
Multimedia
News
Suche

Zertifizierung an der Universität Hannover (UH-CA, PKI)

Im Rahmen einer DFN-weiten Public Key Infrastruktur (PKI) stellt die Zertifizierungsinstanz (Certification Authority, CA) der Universität Hannover (UH-CA) Zertifikate für folgende Anwendungszwecke aus:

- Signieren und Verschlüsseln von E-Mail (Nutzer-Zertifikate)
- Server-Authentifizierung (Server-Zertifikate)
- Signieren von Programm-Code

die UH-CA sieht ihre Aufgabe darin, mit dem Einsatz digitaler Zertifikate die authentische und vertrauliche Kommunikation über das Internet zu fördern. Hierzu wurde sie als Teilnehmer am PKI-Projekt des DFN (Deutsches Forschungsnetz) von der DFN-PCA (DFN-Toplevel Certification Authority) zertifiziert, welche die Root-CA (Wurzel-CA, Stamm-Zertifizierungsstelle) der PKI bildet.

▸ Die neue Zertifizierungsinstanz der Universität Hannover (UH-CA, G02)

Die ~~alte~~ Zertifizierungsinstanz der Universität Hannover (UHtopCA/UH-CA), deren CA-Zertifikat im nächsten Jahr abläuft und auch nicht verlängert wird (Gültigkeitszeitraum des CA-Zertifikates der alten UH-CA: 25.05.04 - 25.05.06) erreichen Sie hier.

- Zertifizierungsanträge sollten nur noch bei der neuen UH-CA eingereicht werden!

Bei Fragen wenden Sie sich bitte an Birgit Gersbeck-Schierholz, Tel.: 762-19789.



Neuer Tab
EÖ English/German ...
Google
Abkürz.
CA
UH-CA
PKI - Pilot
DFN-Verein: DFN-PKI
Stud.IP
IT-Security
Zertifikatsserver
View Document - W...
CERTs
GV

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

Kontakt:
uhtopca@ca.uni-hannover.de

Das Zertifikat läuft 2006 aus:

Das Zertifikat läuft 2006 aus:

Das Zertifikat läuft 2006 aus:

Organisation

Forschung und Lehre

Netze

Zentrale Server

IT-Sicherheit

Antivirensoftware

Anwenderinfos

Administratoreninfos

Abo Security Mails

IT-Sicherheitsbeauftr. UH

RRZN-Netzschutz

Zertifizierung (UH-CA)

Zertifizierungsrichtlinien

FAQ

Arbeitsplatzrechner

Angebote

Multimedia

News

Suche

Die neue Zertifizierungsinstanz der Universität Hannover (UH-CA, G02)

Im Rahmen einer DFN-weiten Public Key Infrastruktur (PKI) stellt die neue Zertifizierungsinstanz (Certification Authority, CA) der Universität Hannover (UH-CA, G02) Zertifikate für folgende Anwendungszwecke aus:

- **Signieren und Verschlüsseln von E-Mail (Nutzer-Zertifikate)**
- **Server-Authentifizierung (Server-Zertifikate)**
- **Signieren von Programm-Code**

Die UH-CA sieht ihre Aufgabe darin, mit dem Einsatz digitaler Zertifikate die authentische und vertrauliche Kommunikation über das Internet zu fördern. Hierzu wurde sie als Teilnehmer am PKI-Projekt des DFN (Deutsches Forschungsnetz) von der DFN-PCA (DFN-Toplevel Certification Authority) zertifiziert, welche die Root-CA (Wurzel-CA, Stamm-Zertifizierungsinstanz) der PKI bildet.

Spezifizierung und Services:

1. Zertifizierungsrichtlinien (Policy)
2. CA-Zertifikate zum Download
3. (Kurz-)Anleitungen
4. Öffentliches PKI-Portal
5. Kontakt im RRZN für die Registrierung und Zertifizierung

■ Antrag auf ein persönliches E-Mail-Zertifikat

The screenshot shows the website interface for RRZN (Regionales Rechenzentrum für Niedersachsen) at the University of Hannover. The header includes the RRZN logo and the text 'Regionales Rechenzentrum für Niedersachsen' on the left, and 'Universität Hannover' with its logo on the right. A navigation bar contains links for 'A-Z', 'Hotline', 'Kontakt', 'Sitemap', and 'Intern'. Below the navigation bar, a breadcrumb trail reads 'RRZN > IT-Sicherheit > Zertifizierung (UH-CA) >'. On the left side, there is a vertical menu with various categories, including 'Organisation', 'Forschung und Lehre', 'Netze', 'Zentrale Server', 'IT-Sicherheit', 'Antivirensoftware', 'Anwenderinfos', 'Administratoreninfos', 'Abo Security Mails', 'IT-Sicherheitsbeauftragt. UH', 'RRZN-Netzschutz', 'Zertifizierung (UH-CA)', 'FAQ', 'Arbeitsplatzrechner', 'Angebote', 'Multimedia', 'News', and 'Suche'. The main content area is titled '(Kurz-)Anleitungen' and contains a list of links: 'Nutzer-Zertifikate (Signieren und Verschlüsseln von E-Mail)' and 'Server-Zertifikate'. Below this, there is a section titled 'Kurzanleitung für Nutzer-Zertifikate (Signieren und Verschlüsseln von E-Mail)' with a numbered list of six steps: 1. Laden Sie sich unbedingt als erstes die CA Zertifikate herunter und installieren Sie sie in Ihrem Browser. - Das Wurzelzertifikat der DFN-PCA. - Das UH-CA Zertifikat. 2. Lesen Sie sich die Policy der UH-CA durch. 3. Füllen Sie den Antrag auf Zertifizierung am Bildschirm aus. 4. Unterschreiben Sie den ausgedruckten Antrag und legen ihn persönlich, (weisen Sie sich mit Ihrem Personalausweis aus) bei der Registrierungsstelle (RA) der UH-CA im RRZN vor. 5. Nach Erhalt der Antwort E-Mail importieren Sie sich das Zertifikat in den Browser. 6. Sichern Sie sich das Zertifikat auf Diskette bzw. einen anderen externen Datenträger. At the bottom of this section, it says 'Eine ausführliche Erklärung zum Beantragen eines Zertifikates finden Sie unter dem Menüpunkt Anleitungen.'

■ Antrag auf ein persönliches E-Mail-Zertifikat

The screenshot shows a web browser window with the URL `https://pki.pca.dfn.de/uh-ca/cgi-bin/pub/pki?cmd=basic_csr&...&CSR_TYPE=IE`. The browser's address bar and tabs are visible. The main content area is titled "Beantragen eines Nutzer-Zertifikats" and contains a form with the following sections:

- Zertifikatsdaten**
 - E-Mail *:
 - Name (Vor- und Nachname) *:
 - Institutskürzel:
- Nutzerangaben**
 - Bitte geben Sie hier zusätzliche Kontaktdaten ein:
 - E-Mail:
 - Telefon:
 - PIN (Mindestens 8 beliebige Zeichen) *:
 - Nochmalige Eingabe der PIN zur Bestätigung *:
 - Die PIN wird von Ihnen benötigt, um sich gegenüber dem Zertifizierungssystem zu autorisieren, z.B. wenn Sie Ihr Zertifikat sperren wollen. Bitte notieren Sie sich die PIN.
 - Ich stimme den AGB zu (Zertifizierungsrichtlinie) *:
 - Ich stimme der Veröffentlichung des Zertifikats zu.
 - Wenn Sie der Veröffentlichung nicht zustimmen, wird Ihr Zertifikat nicht im Verzeichnisdienst zur Verfügung stehen.

At the bottom of the form is a "Weiter" button.

■ Antrag auf ein Server-Zertifikat

The screenshot shows the top navigation bar of the RRZN website. On the left, the logo 'R|R|Z|N' is displayed above the text 'Regionales Rechenzentrum für Niedersachsen'. On the right, the text 'Universität Hannover' is shown next to the university logo. Below this, a horizontal menu contains links for 'A-Z', 'Hotline', 'Kontakt', 'Sitemap', and 'Intern'. A breadcrumb trail below the menu reads 'RRZN > IT-Sicherheit > Zertifizierung (UH-CA) >'.

Organisation
Forschung und Lehre
Netze
Zentrale Server
IT-Sicherheit
Antivirenssoftware
Anwenderinfos
Administratoreninfos
Abo Security Mails
IT-Sicherheitsbeauftragt. UH
RRZN-Netzschutz
Zertifizierung (UH-CA)
FAQ
Arbeitsplatzrechner
Angebote
Multimedia
News
Suche

(Kurz-)Anleitung für Server-Zertifikate

1. Einleitung
2. Vorbereitung
3. Erzeugen eines Schlüsselpaares und Erstellen eines Zertifizierungsantrages (Certificate Signing Request, CSR)
4. Beantragen des Zertifikates bei der UH-CA
5. Einpflegen von Zertifikat und privatem Schlüssel in den Server

1. Einleitung

Mit einem Serverzertifikat wird Ihr Server von einer vertrauenswürdigen Instanz zertifiziert.

Dadurch wird es Ihren Benutzern ermöglicht die Authentizität des Servers eindeutig nachzuvollziehen.

Wer kann sich zertifizieren lassen?

Die Certification Authority (CA) der Universität Hannover bietet Administratoren, insbesondere von Einrichtungen der Universität Hannover, die SSL-Zertifizierung von Servern an.

2. Vorbereitung

Lesen der Policy

SSL-Zertifikate werden von der UH-CA ausschließlich auf der Grundlage der Zertifizierungsrichtlinien (Policy) ausgestellt. Bitte lesen Sie die Policy sorgfältig durch. Die dort beschriebenen Zertifizierungsrichtlinien und die Anforderungen an die Zertifikatnehmer beinhalten Aussagen über die Qualität der ausgestellten Zertifikate.

3. Erzeugen eines Schlüsselpaares und Erstellen eines Zertifizierungsantrages (Certificate Signing Request, CSR)

■ Zertifikate suchen, Zertifikat zurückrufen, Sperrlisten

The screenshot shows a web browser window titled "UH-CA - Mozilla Firefox". The address bar contains the URL: `https://pki.pca.dfn.de/uh-ca/cgi-bin/pub/pki?cmd=getStaticPage&name=index`. The page header includes the "UH CA" logo, the "Universität Hannover" logo, and the "DFN Deutsches Forschungsnetz" logo. Below the header, there are navigation tabs for "Nutzer" and "CA-Informationen". Under the "Nutzer" tab, there are three buttons: "Beantragen eines Zertifikats", "Zertifikat zurückrufen", and "Suche nach Zertifikaten". The "Suche nach Zertifikaten" button is highlighted. Below the buttons, there is a search form with the text "Bitte geben Sie die E-Mail-Adresse des Zertifikats ein, das Sie suchen." and an input field containing the email address "gersbeck@rrzn.uni-hanr". At the bottom of the form, there are two buttons: "OK" and "Zurücksetzen".

„Klippen“

- Beispiel 1:
 - Ich erhalte eine signierte E-Mail -> mein Mail-Client stuft die Signatur als ungültig ein und meldet eine wenig Vertrauen erweckende Warnung

- Beispiel 2:
 - Ich wähle eine Verbindung zu einem Webserver, der sich mit einem Zertifikat ausweist -> mein Browser schlägt Alarm und warnt mich vor möglichem Betrug

- Ursache in beiden Fällen:
 - die Zertifikate der Zertifizierungshierarchie **DFN-PCA, UH-CA** sind noch nicht in Standard-Browsern und Mail-Klienten enthalten.
- Etwas lästig aber unabdingbar: die CA-Zertifikate müssen nachinstalliert werden.

■ Zertifikate der Zertifizierungsinstanzen:



2. CA-Zertifikate zum Download

Die Vertrauenswürdigkeit der Kommunikation innerhalb der PKI wird nur dann uneingeschränkt von Ihrem System anerkannt, wenn Sie folgende Root- bzw. CA-Zertifikate der DFN-PKI in Ihren Browser geladen haben. Aktivieren Sie die Links durch jeweils einen Mausklick und bestätigen Sie die CAs als vertrauenswürdig:

Wurzelzertifikat der PKI des Deutschen Forschungsnetzes (DFN)

SHA1 Fingerprint = 12:63:41:60:D0:8C:FE:6A:87:6D:F7:86:D3:AD:C2:F7:74:FF:21:9F

MD5 Fingerprint = EF:08:E6:9F:6A:C7:25:2C:58:8C:55:FD:45:13:31:0A

Zertifikat der Zertifizierungsstelle der Universität Hannover(UH-CA)

SHA1 Fingerprint = FE:1A:DC:29:58:E2:FD:9D:C5:FF:B5:65:5D:60:85:B2:6F:3A:9C:64

MD5 Fingerprint = 4C:12:14:13:14:81:48:79:D8:BA:25:75:67:63:5F:88

Die Fingerprints dienen zum Abgleich des geladenen Zertifikates mit den Angaben des Ausstellers. Je nachdem, wem Sie bei der Überprüfung dieser Fingerprints vertrauen wollen, verlassen Sie sich auf die Angaben oben, schauen auf der Homepage des Ausstellers nach oder, wenn Sie den ganzen Internet-Verkehr für unsicher halten, rufen Sie beim Aussteller an und lassen sich den Fingerprint durchgeben.

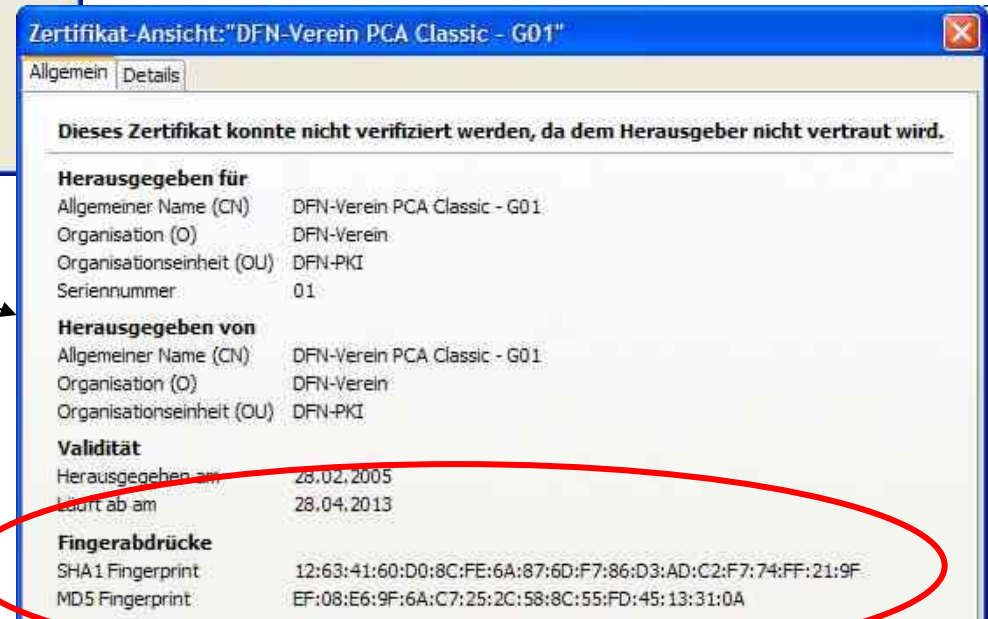
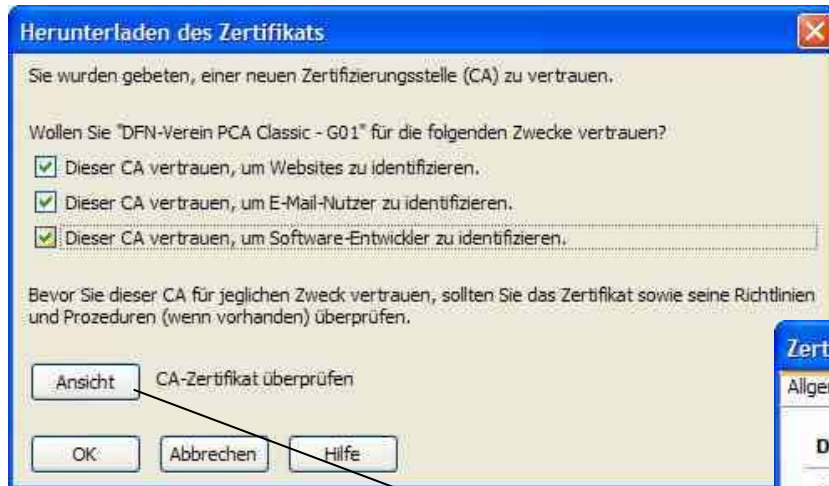
Vollständige Liste aller gängigen Zertifikatsformate:

- ▶ DFN-Wurzelzertifikat
- ▶ UH-CA-Zertifikat

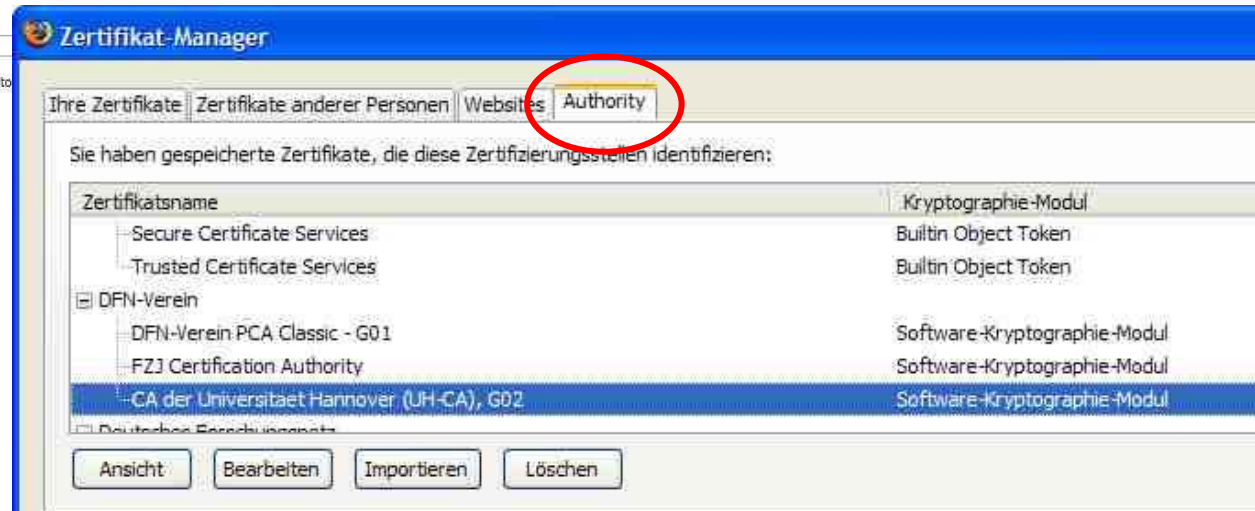
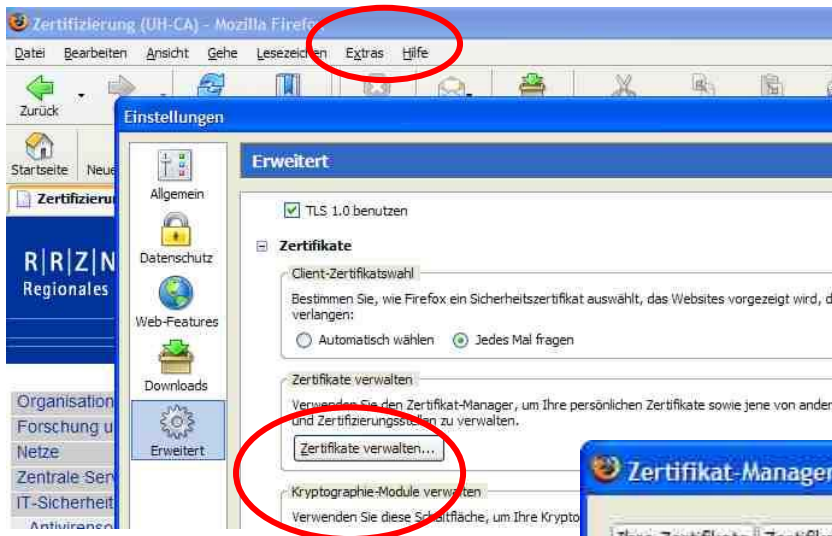
■ Zertifikate der Zertifizierungsinstanzen:



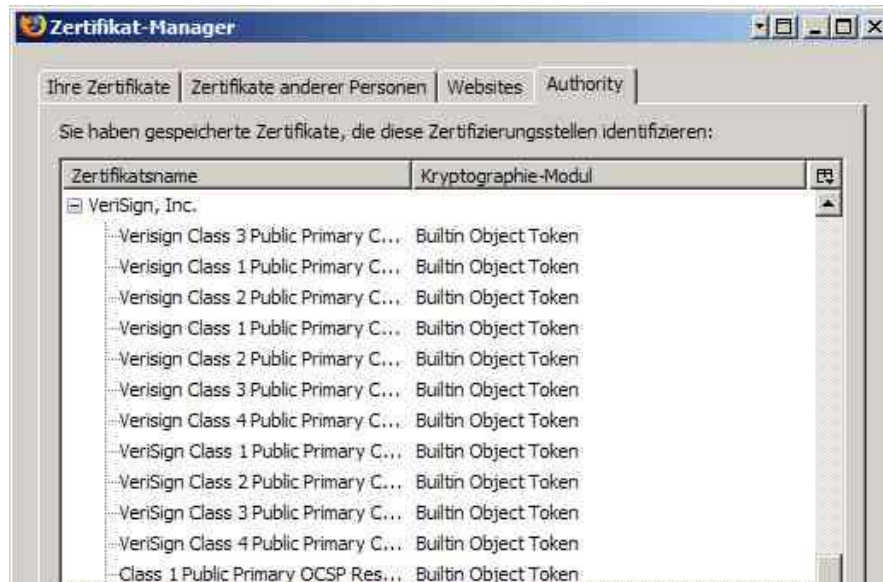
Zertifikate der Zertifizierungsinstanzen:



Zertifikate der Zertifizierungsinstanzen:



■ Zertifikate der Zertifizierungsinstanzen:



- **Der private Schlüssel muss geschützt werden! Bei Kompromittierung ist das Zertifikat hinfällig!**
- **Mit einer Kopie des Schlüssels kann der Angreifer eine falsche Identität vortäuschen und vertrauliche Daten entschlüsseln. Missbrauch wird nicht zwingend erkannt!**
- **Anwendungen, die Zertifikate verwenden, speichern i.d.R. private Schlüssel (Software – PSE (Private Security Environment))**
 - **Beispiel Firefox, Thunderbird:** privater Schlüssel wird, durch Master-Passwort geschützt, in gesichertem Bereich gehalten (Keystore)
 - **Beispiel Windows:** Schlüssel wird in Registry-Schlüsselcontainer gehalten. Schutz durch Master-Passwort nur bei Wahl der hohen Sicherheitsstufe!
- **Für Anwendungen mit hohen Sicherheitsanforderungen reicht die Software-PSE möglicherweise nicht aus!**
 - Einsatz von USB-Token, Chipkarten

- 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/>