Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

http://www.iaik.tugraz.at/

L2 – Public Key Kryptographie

Einführung in die Informationssicherheit

Übersicht

- Grundlagen über elektronische Signaturen
  - Signaturerzeugung
  - Signaturen verifizieren
  - Beispiele anhand des RSA Algorithmus
- Verteilung öffentlicher Schlüssel und PKIs
- Rechtliche Aspekte elektronischer Signaturen

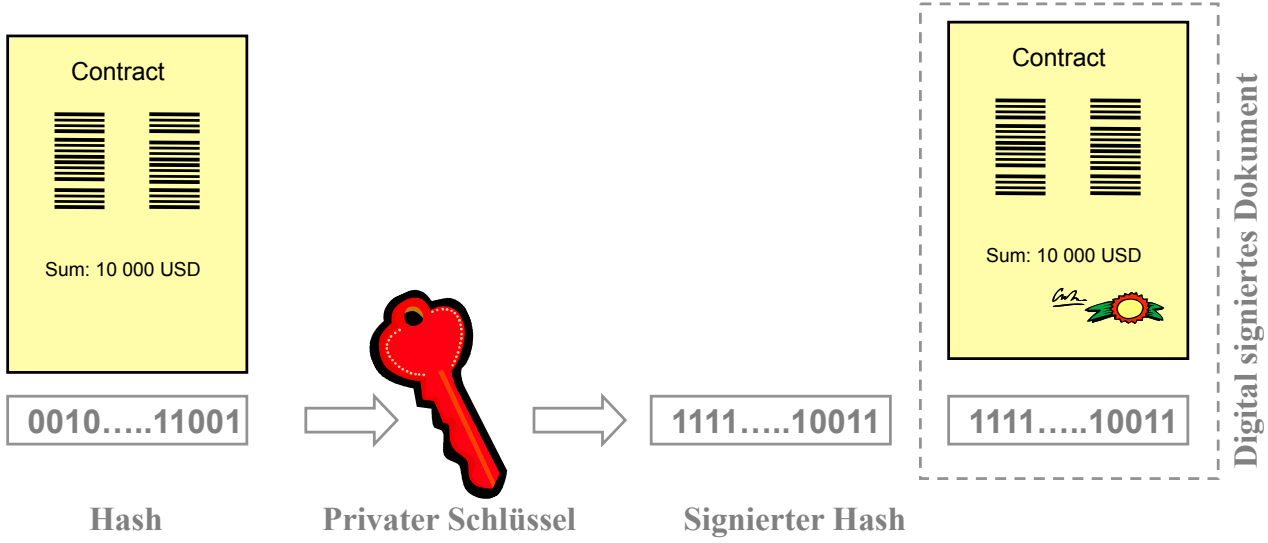
Motivation

- Prozesse des täglichen Lebens werden immer mehr in die elektronische (digitale) Welt verlagert.
- Daher ist ein elektronisches Äquivalent zur herkömmlichen Unterschrift wichtig:
  - Eine Signatur sollte nicht leicht fälschbar sein.
  - Eine Signatur soll eine gewisse Verbindlichkeit für den Unterzeichner darstellen.
  - Eine Signatur sollte einfach zu verifizieren sein.

Digitale Signaturen

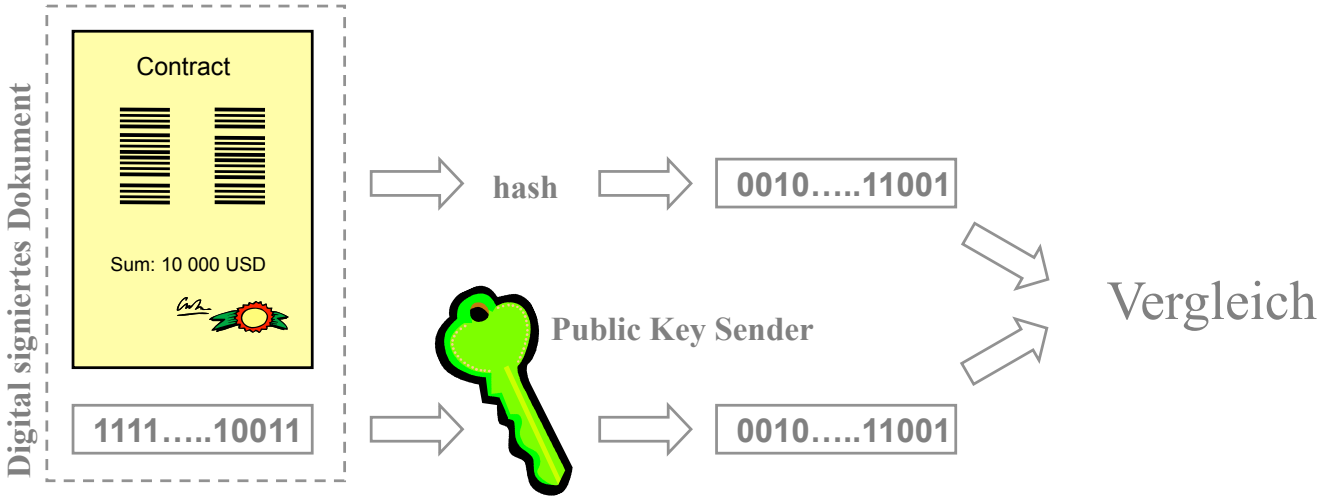
- Gedacht als eletronisches Äquivalent zu handschriftlichen Signaturen.
- Basieren auf Public Key Kryptographie:
  - Der Unterzeichner (signatory) erzeugt die Signatur mit seinem privaten Schlüssel.
  - Der Überprüfer (verifier) verifiziert die Gültigkeit der Signatur mit dem öffentlichen Schlüssel des Unterzeichners.
- Weil der Unterzeichner seinen privaten Schlüssel für die Signaturerzeugung benutzt, kann er nicht leugnen, am Signaturprozess beteiligt gewesen zu sein (non-repudiation).

Signaturerzeugung



- Die Nachricht wird gehasht.
- Benutze den privaten Schlüssel und den Signaturalgorithmus um den Hashwert zu unterschreiben.
- Hänge die Signatur an die Nachricht an.

Signatur - Verifikation



- Die ursprüngliche Nachricht wird gehasht.
- Dieser Hashwert, der signierte Hashwert (die Unterschrift) und der Public Key sind die Inputs für die Verifikationsfunktion.
- Diese Funktion gibt als Antwort: Akzeptieren oder Ablehnen (also Signatur ist gültig, ungültig)

Beispiel – RSA

- Signieren: $s = h(m)^d \mod n$.
- Verifizieren: $v = s^e \mod n$,
  if $v = h(m)$ then `accept`, else `reject`.
- Wähle: $p = 11$, $q = 5$, $e = 3$, $m = 7$
  - D.h.: $n = 55$, $(p-1)(q-1) = 40$, $d = 27$
  - Der Einfachheit halber: $h(m) = m$
  - Signieren $s = 7^{27} = 28 \mod 55$
  - Verifizieren: $v = 28^3 = 7 \mod 55$, $v = h(m) \Rightarrow$ `valid`

Wichtige Signaturalgorithmen

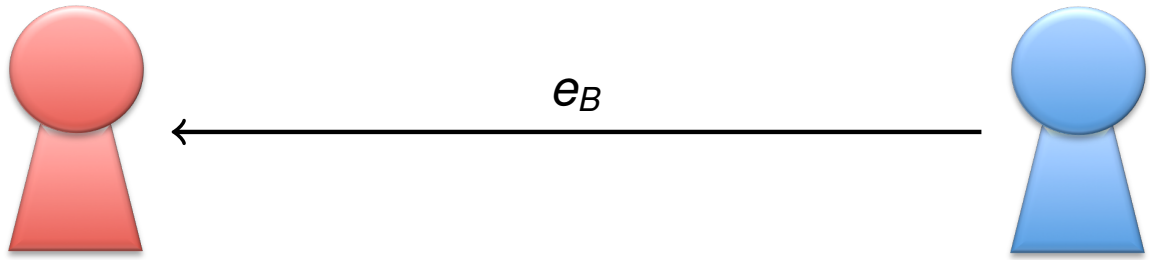
- RSA
  - In vielen Standards, weit verbreitet, große Akzeptanz
  - Sehr große Schlüssellängen (min. 1024 bits, besser 2048 bits)
- DSA
  - In vielen Standards, nicht ganz so weit verbreitet
  - Sehr große Schlüssellängen (min. 1024 bits, besser 2048 bits)
- ECDSA
  - In vielen Standards, noch nicht weit verbreitet
  - Kurze Schlüssellängen (min. 163 bits, besser 192/224 bits)

`http://www.keylength.com/`

Public Key Infrastrukturen (PKI)

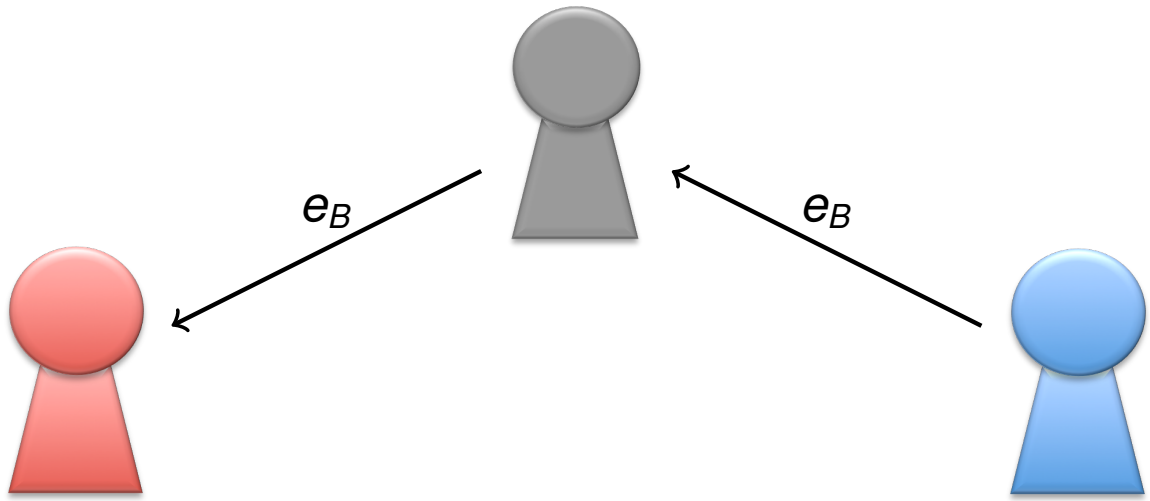
- Wie komme ich zu den öffentlichen Schlüsseln, die ich zur Verifikation benötige?
- Wie überprüfe ich die Authentizität des jeweiligen öffentlichen Schlüssels?

Public Key Distribution



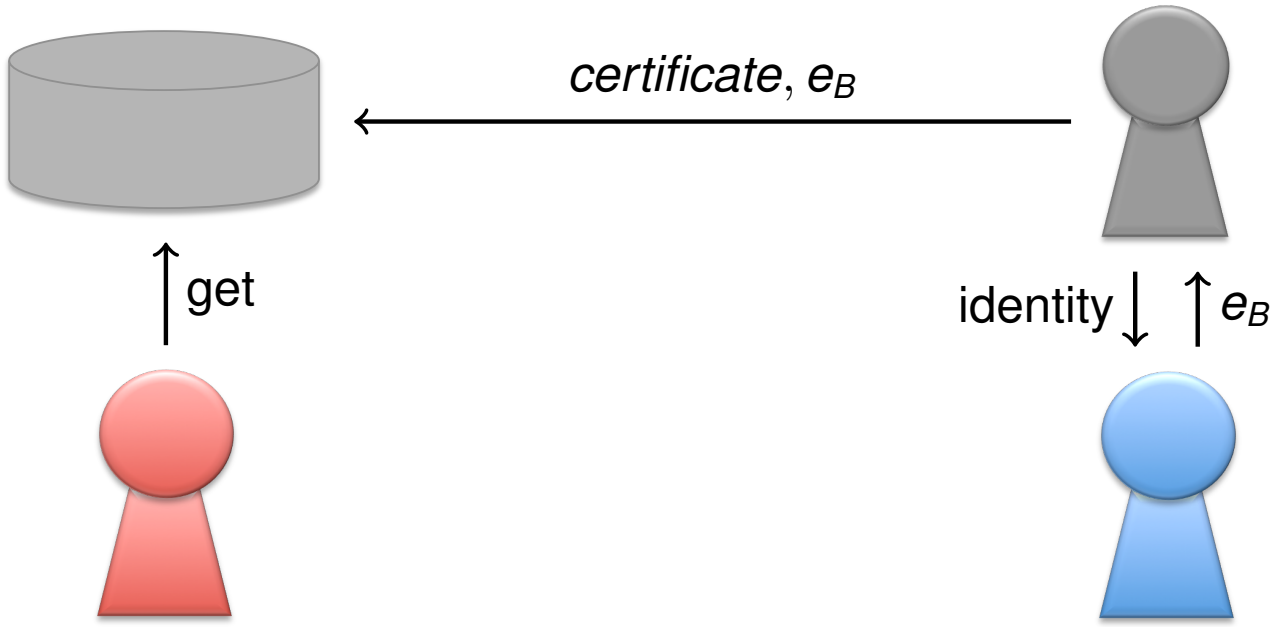
- Direkter Kontakt
  - Distanz?
  - Jedesmal treffen, wenn Signatur erstellt wird?
  - Kann man die Identität genau überprüfen?

Public Key Distribution



- Man erhält den Schlüssel von einer Trusted Third Party (TTP):
  - Erleichtert die Distribution
  - Wie kann man sicher gehen, dass der Schlüssel authentisch ist?

Public Key Distribution



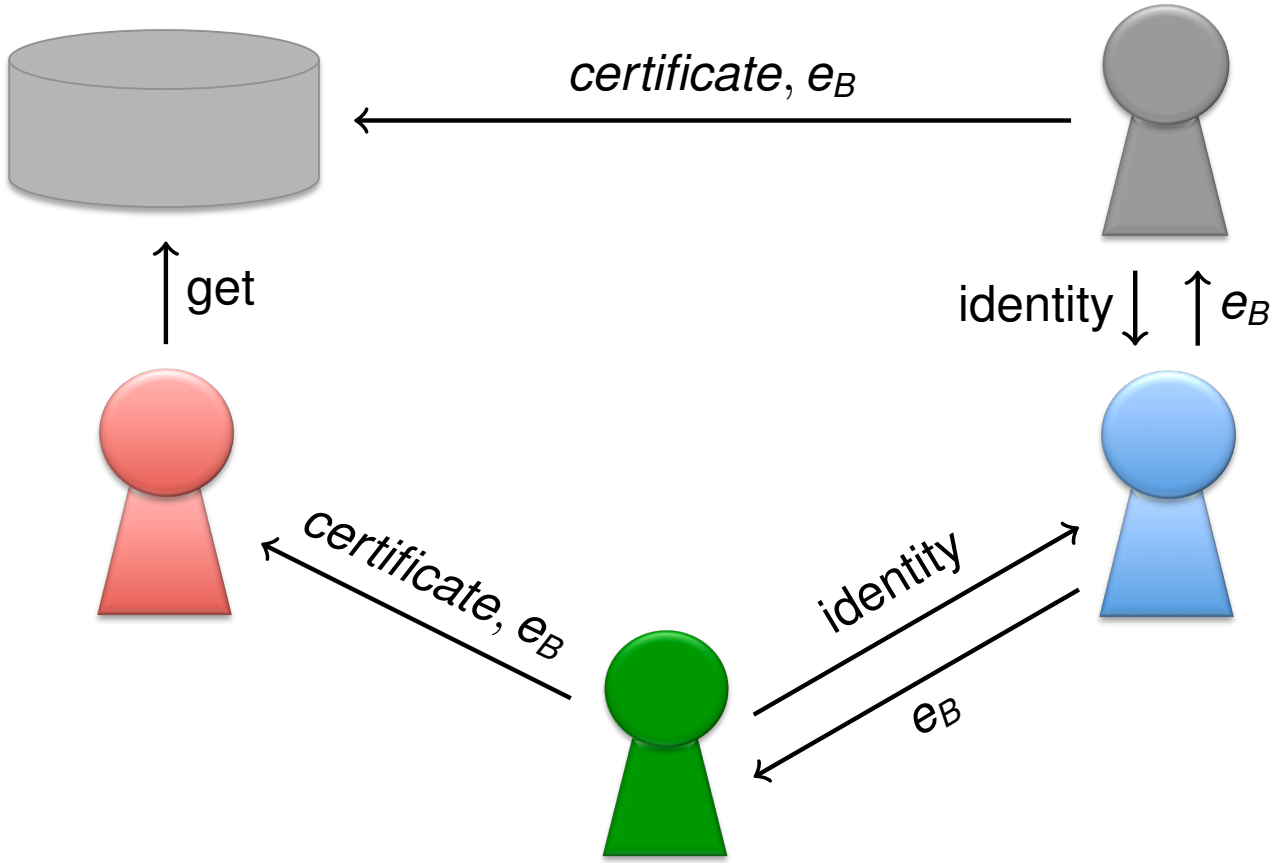
- Alice bekommt den Schlüssel in zertifizierter Form:
  - Das “Initial key exchange”-Problem ist dadurch nicht gelöst . . .
  - Widerrufsmechanismen (revocation) sind erforderlich

PKI – Realisierungen in der Praxis

- PGP
  - Aus der Open Source community
  - Relativ einfach
- X.509
  - Basiert auf X.500 (ISO)
  - Umfangreich und komplex
- Der Unterschied der beiden Zugänge liegt im zugrundeliegenden Vertrauensmodell (trust model)

PGP

- Web of trust (user-centric trust)
- User agiert als CA und signiert die Schlüssel von anderen Usern



PGP (User Responsibility)

http://xkcd.com/364/

- User education?
- Widerruf?
- Ist Vertrauen transitiv?

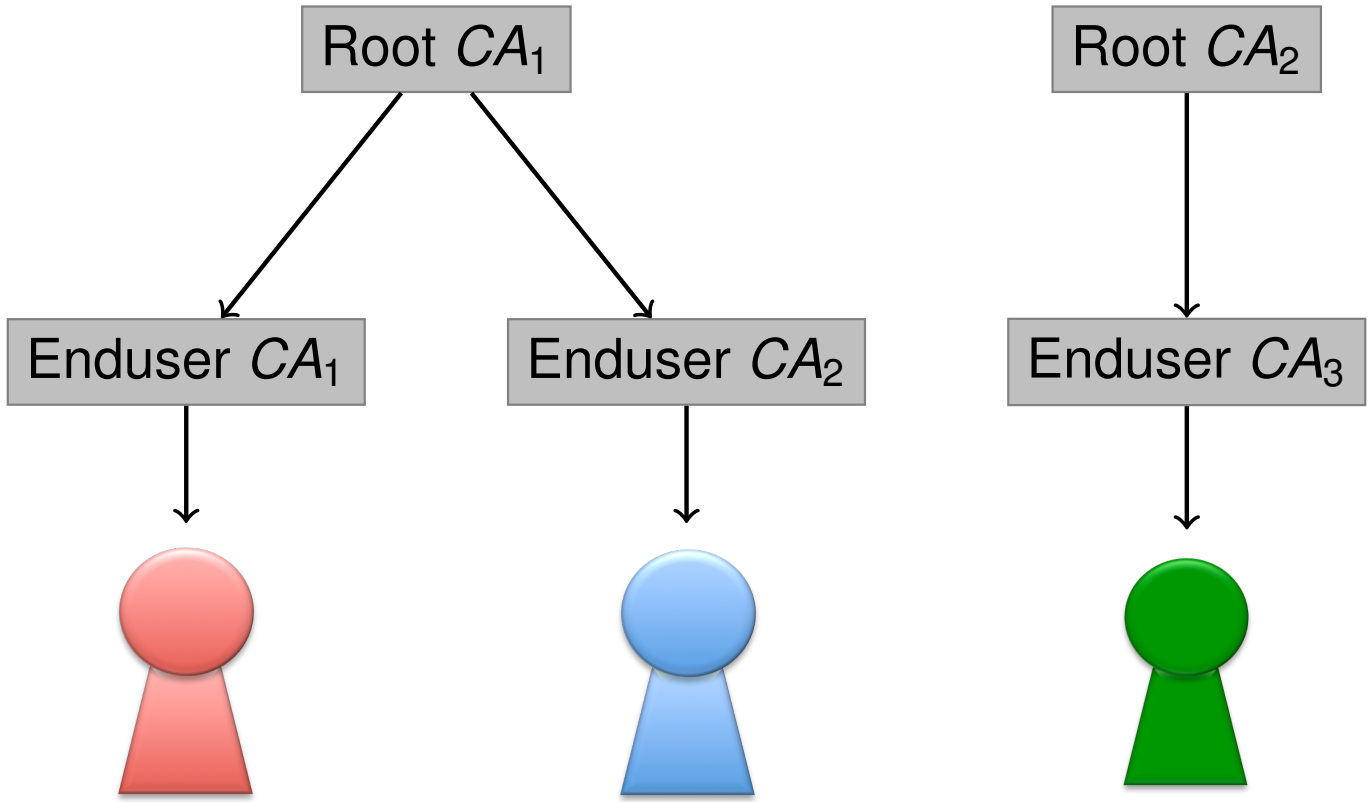
OpenPGP

- IETF Internet Standard (RFC 4880)

```
pub    1024D/0x12345678 2005-09-05
       D44C 6A5B 71B0 427C CED3 025C BD7D 6D27 1234 5678

uid    Vorname Nachname <vorname.nachname@example.org>
sig    0x12345678      Vorname Nachname <vorname.nachname@example.org>
sig    0x87654321      Zertifizierer <zertifizierer@example.org>

uid    Vorname Nachname (Geschäftsführer der Beispiel GmbH) <vorname.nachname@example.net>
sig    0x12345678      Vorname Nachname <vorname.nachname@example.org>
sig    0x87654321      Zertifizierer <zertifizierer@example.org>

sub    2048R/0x51B279FA 2010-03-04 [verfällt: 2013-03-03]
sig    0x12345678      Vorname Nachname <vorname.nachname@example.org>
```

X.509

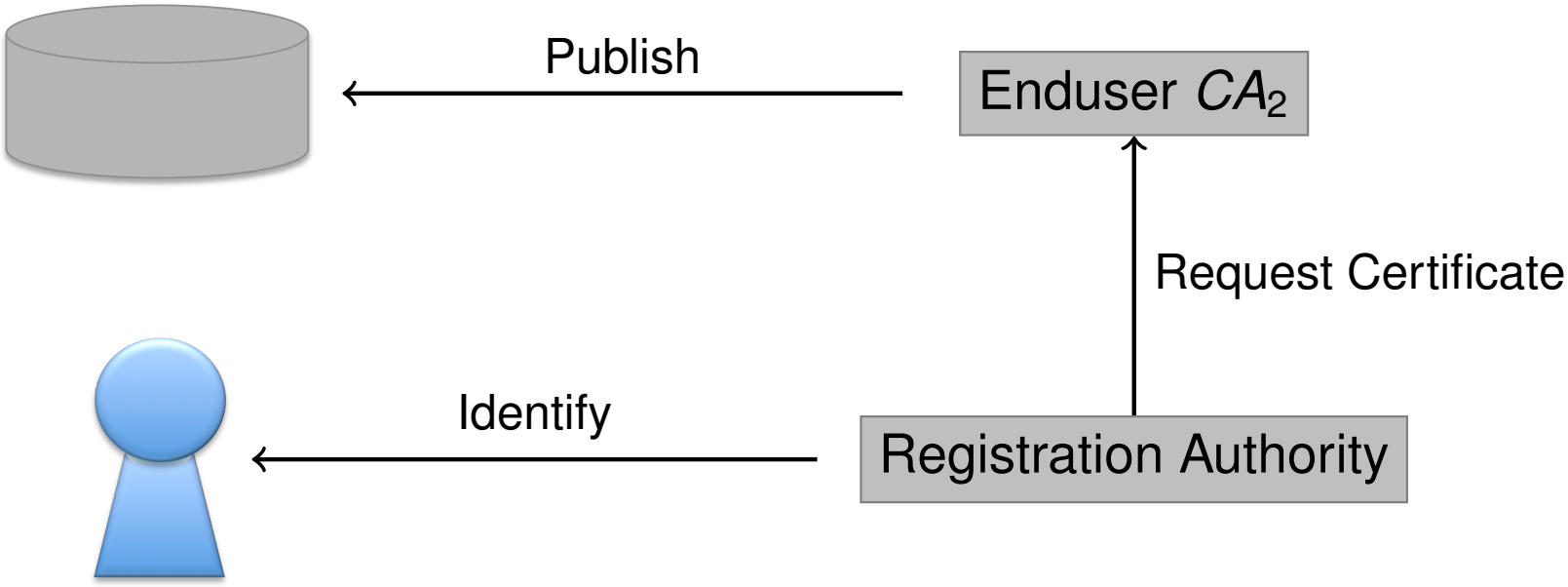
- Hierarchische Struktur:



X.509

- Hierarchische Struktur:
  - Eine root CA (Wurzel CA) steht zu Beginn und ein selbst-signiertes Wurzelzertifikat (root certificate) bildet die Basis des Vertrauens für alle Entitäten in der Hierarchie.
  - Die Wurzel CA zertifziert $0 \ldots N$ CAs unter ihr.
  - Diese CAs wiederum zertifizieren CAs die unter ihnen stehen
  - Auf der vorletzen Stufe zertifizieren die CAs End-User.
- Public key Zertifikate

Registrierung



- RA erstellt und verifiziert die Identität eines Individuums, zusätzlich kann sie:
  - Schlüsselmaterial generieren
  - Life-cycle-Management für Schlüssel und Zertifikate

Zertifikatsmanagement

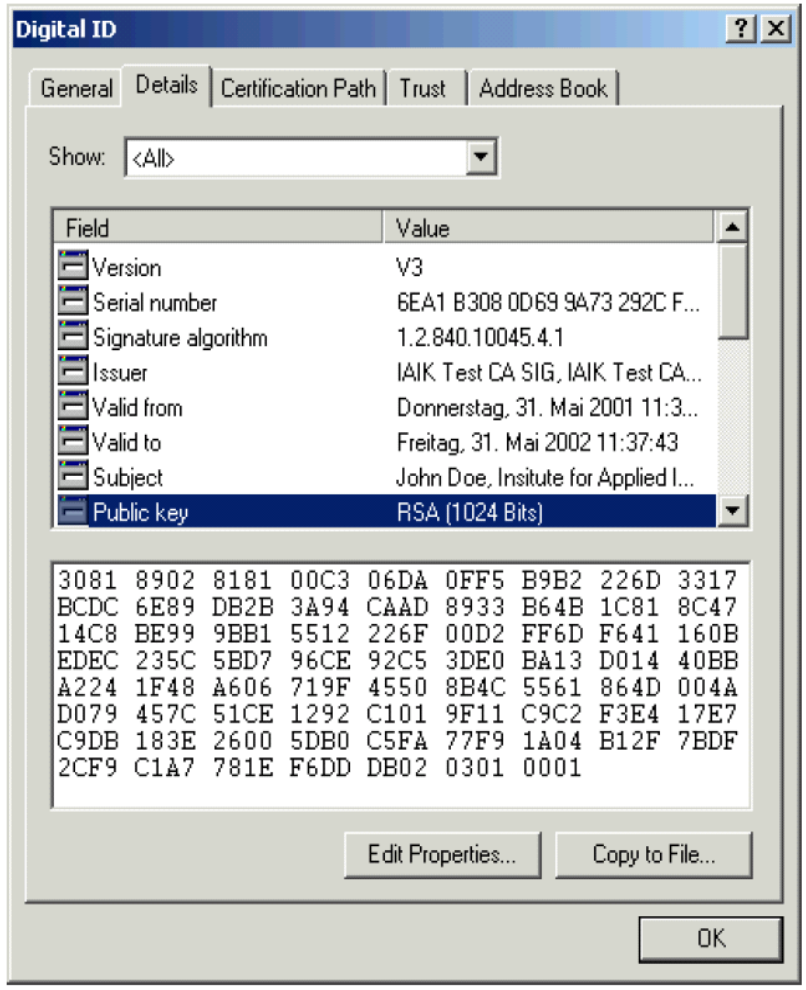
- Certificate Repository:
  - Zumeist ein LDAP server
  - Public read access
  - Such Features
    - Name
    - E-Mail Adresse
- Widerruf (Revocation):
  - Widerruf eines Zertifikats (noch nicht standardisiert)
  - Überprüfen eines Widerrufs:
    - CRLs
    - Online Protokolle OCSP

CAs

- Certificate Policies:
  - Gültigkeitsbereich des Zertifikats
  - Inhalt des Zertifikats
  - Andere Services (OCSP, CRLs)
- Certificate Practice Statement:
  - Organisation der CA (non-technical)
  - Lebenszyklus des Zertifikats

X.509 Certificate

- Version Number
- Serial Number
- Issuer Name
- Validity Period
- Subject Name
- Issuer/Subject Unique IDs
- Public Key Info
- Extensions
- Signature of the CA



X.509 Certificate Extensions

- In Version 3:
  - Key identifiers:
    - Authority Key Id
    - Subject Key Id
  - Key Usage:
    - Digital signature
    - Key encipherment
    - Key agreement, . . .
  - CRL Distribution Point
  - Certificate Policies
  - Basic Constraints:
    - Path length constraint
  - Extended Key Usage:
    - TLS server authentication
    - Code signing, . . .

X.509 Certificate Extensions

- Eine Extension die als kritisch markiert ist muss bearbeitet werden.
- Eine nicht-kritische Extension soll wenn möglich bearbeitet werden

Signaturen – Rechtliche Aspekte

- Direktive 1999/93/EC des Europäischen Parlaments und des Rats vom 13 December 1999 über

  Community framework for electronic signatures

  “Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”

Fortgeschrittene Elektronische Signatur

(Advanced Electronic Signature)

- Ist eindeutig verbunden zum Unterzeichner.
- Ist in der Lage, den Unterzeichner zu identifizieren.
- Wird mit Mitteln erzeugt, die der Unterzeichner unter seiner alleinigen Kontrolle behalten kann.
- Steht zu den zugehörigen Daten derart in Verbindung, dass nachträgliche Veränderung dieser detektierbar ist.

Nützliche Terminologie

- Unterzeichner (Signatory)
  - eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt;
- Signaturerstellungsdaten
  - einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden;

Nützliche Terminologie

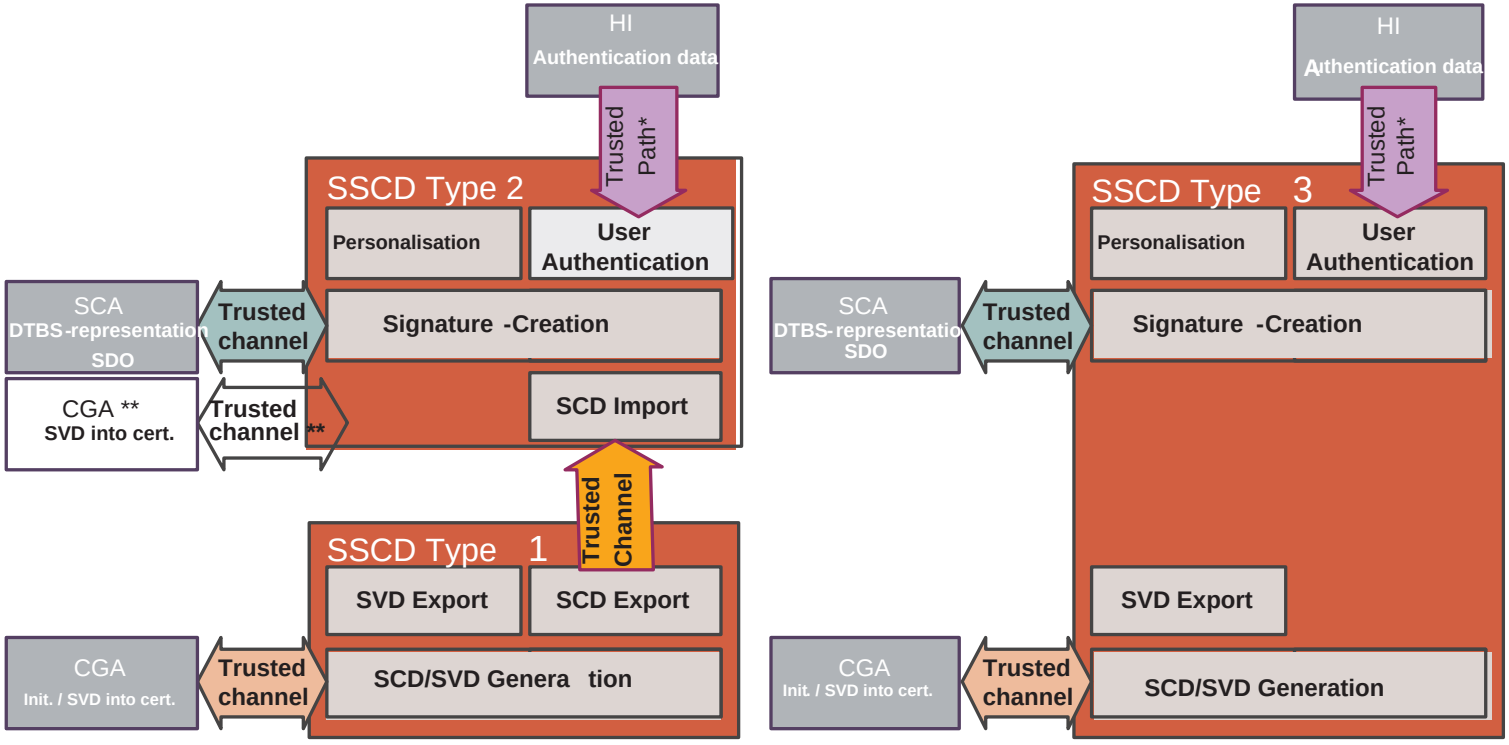
- Signaturerstellungseinheit
  - eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird;
- Sichere Signaturerstellungseinheit
  - eine Signaturerstellungseinheit, die gewisse zusätzliche Anforderungen erfüllt

Qualifizierte elektronische Signatur

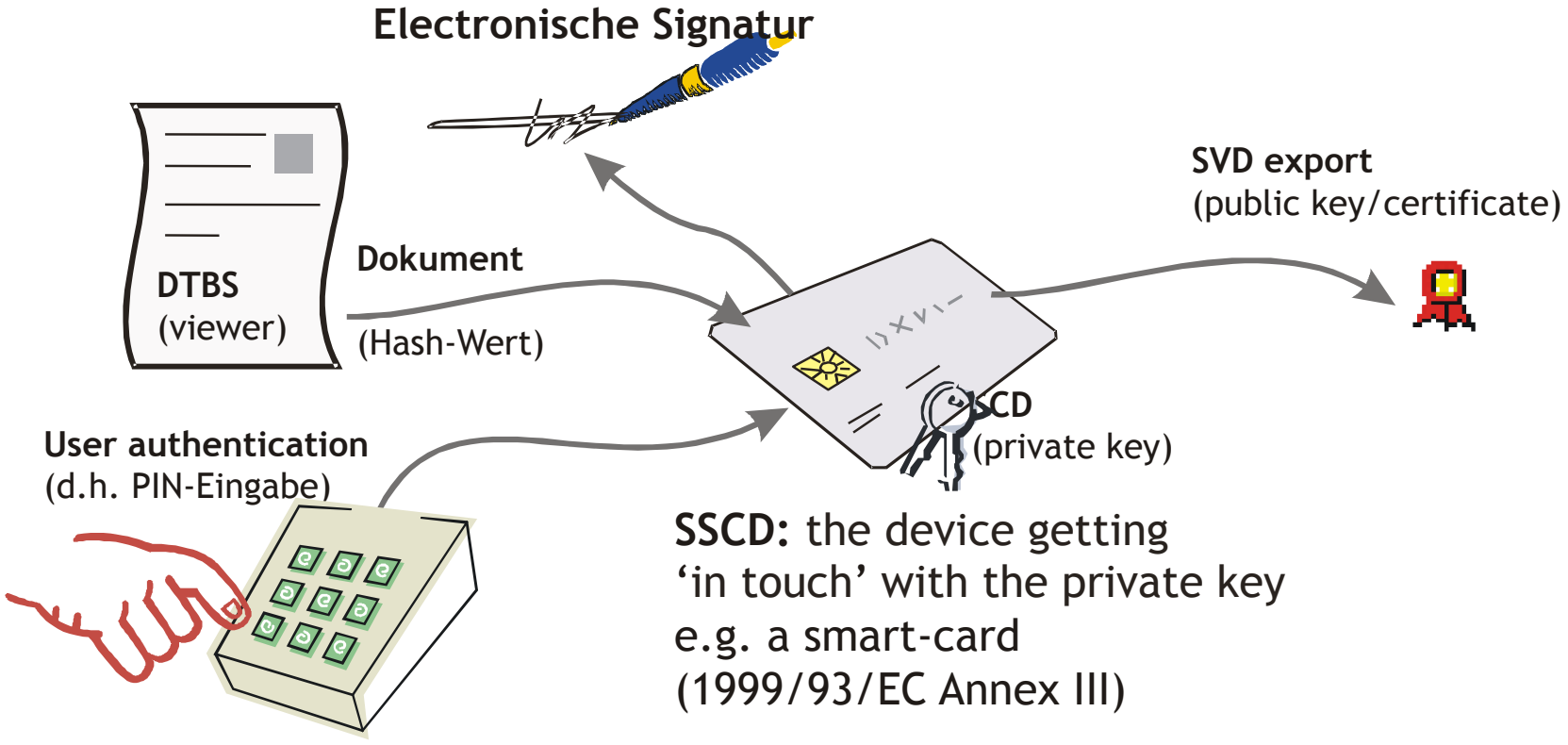
(ehemals sichere elektronische Signatur)

- Ist eine fortgeschrittene elektronische Signatur die auf einer
- sicheren Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat basiert. Es muss
- sichergestellt werden, dass die Signaturersttellungsdaten (z.B. der private Schlüssel) nur einmal existiert und geschützt sind
- durch den Benutzer vor Missbrauch durch andere.

Sichere Signaturerstellungseinheiten



SSCD und Umgebung



SSCD: the device getting ‘in touch’ with the private key
e.g. a smart-card
(1999/93/EC Annex III)

Zertifizierungsdiensteanbieter

(Certificate Service Providers)

- Muss vertrauenswürdig sein!

- Sichere Verzeichnisse (LDAP) und unverzügliches Widerrufsservice.
- Verifikation der Identitäten der Benutzer.
- Qualifiziertes und vertrauenswürdiges Personal.
- Einsatz von vertrauenswürdigen (zertifizierten) Produkten und Systemen.

Zertifizierungsdiensteanbieter

(Certificate Service Providers)

- Muss über genügend finanzielle Reserven verfügen.
- Aufzeichnung aller relevanten Informationen.
- Darf auf keinen Fall private Schlüssel kopieren oder speichern.
- Muss die Benutzer mit einem dauerhaften Kommunikationsmittel über die genauen Bedingungen für die Verwendung des Zertifikats informieren.

Anwendungen von elektronischen Signaturen

- E-Government:
  - §2 (10) EGovG: “Bürgerkarte”:

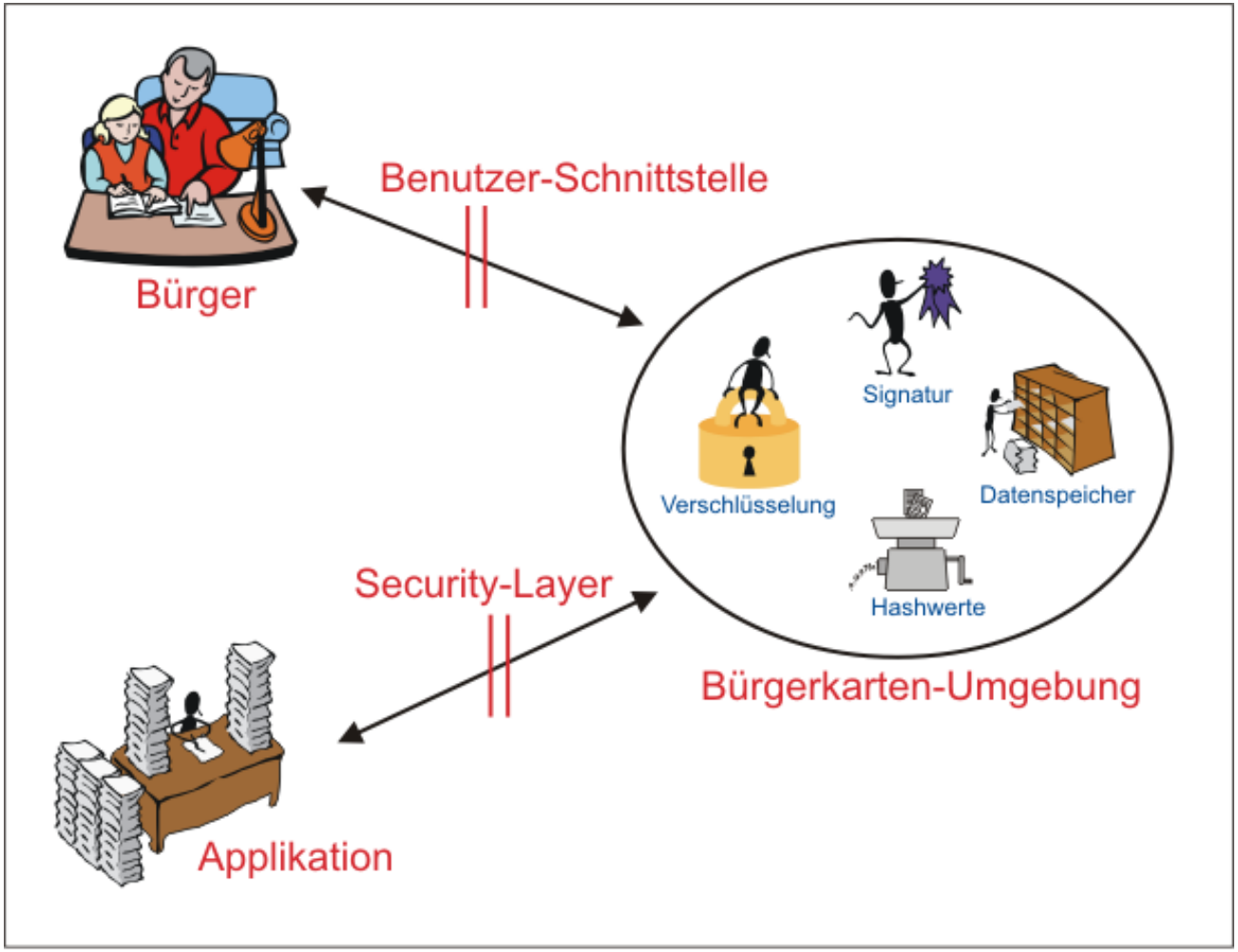
    die unabhängig von der Umsetzung auf unterschiedlichen technischen Komponenten gebildete logische Einheit, die eine elektronische Signatur mit einer Personenbindung (§4 Abs. 2) und den zugehörigen Sicherheitsdaten und -funktionen sowie mit allenfalls vorhandenen Vollmachtsdaten verbindet.
  - Technische Realisierung:

    - Smart card
    - Mobile Phone
    - Handheld, USB stick, etc.
- E-Business

Österreichisches Konzept: Bürgerkarte

- Definiert die allgemeinen Minimalanforderungen:
  - Sichere elektronische Signaturen
    - d.h. rechtlich äquivalent der handschriftlichen Signatur,
  - Zusätzliche Schlüsselpaare
    - ‘Allgemeine Signaturen’, Verwaltungssignatur, Verschlüsselung
  - Infoboxen um Daten zu speichern
    - Personenbindung, Zertifikate
    - Zugangskontrolle zu Infoboxen
  - DH Schlüsselaustausch
    - Session-Key Zertifikate

Security Layer



Das Modell der Bürgerkarte

Aktueller Status

- Security layer
  - Generallizenz der Bürgerkarten-Software durch die Regierung
- Die österreichische Bürgerkarte (http://www.buergerkarte.at) ist fertig erhältlich:
  - A-TRUST (Österr. CSP für qualifizierte Zertifikate)
  - E-Card
  - Maestro
  - etc.

Aktueller Status

- E-Government Anwendungen
  - Versicherungszeitenauszug
  - Registrierung eines Gewerbes in Wien
  - Online Steuerausgliech
  - Signierte Unterschriftenaktionen an die Regierung
  - Strafregisterauszug
  - Elektronische Zustellung (z.B. RSa-Briefe)
  - Online Meldezettel
  - ...

Seit 2009: Relaunch Mobile Signatur

- Wichtigste Aspekte:
  - Betrieben von Ceritifcation Service Provider (CSP) für qualifizierte Zertifikate
  - Signaturerstellungsdaten (kryptographische Schlüssel) bleiben beim CSP, aber die Kontrolle ist beim Unterzeichner

    - 2-Faktor Authentfizierung (Wissen & Besitz)
  - Sichere Signaturerstellungseinheit:

    - 1999/93/EC Annex III, bestätigt von einer Zulassungsstelle

Zusammenfassung

- Die Verteilung von authentischen öfftentlichen Schlüsseln ist ein nicht-triviales Problem.
- PKIs können nur manche der Probleme lösen, andere, wie Authorisierung, Vertrauen, allgemein richtiges Verhalten kann nicht durch PKI gelöst werden.
- State-of-the art Lösungen sind eher komplex.
- Unterschiedliche elektronische Unterschriften sind anerkannt, qualifizierte elektronische Unterschriften sind sogar äquivalent zu handschriftlichen Signaturen.

Vielen Dank für Ihre Aufmerksamkeit!