Aufbau einer Zertifizierungsinstanz (CA) an einer Hochschule

Vorgehen, juristische Aspekte und Software-Unterstützung

Motivation

- Studentenzahlen steigen:
  - Effektive Kommunikation nötig
- Ohne Verschlüsselung keine Vertraulichkeit / Verbindlichkeit:
  - Authentizität: rektor@tu-ilmenau.de
  - Integrität: "Glückwunsch zu Ihrem Diplom"
- Know-How an *Forschungs*einrichtungen:
  - Public Key Kryptographie
  - digitale Signaturen

Ziele

- Know-How in wichtigen Teilbereichen:
  - Recht
  - Organisation
  - Technik
- Vorgehen beim Aufbau einer CA
  - insbesondere: X.509v3
- Vergleich von und mit Alternativen
  - Registrierungsinstanz (Registration Authority: RA)

So wird's laufen

- Grundlagen (Schnelldurchlauf):
  - (Public Key) Kryptographie im Internet
- Einblicke in:
  - Juristische Aspekte
  - Organisatorische Aspekte
  - Technische Aspekte
- Varianten: Aufbau einer CA
- Ausblick

Kryptographie im Internet

- Internet (IP) i.A. unverschlüsselt
- ↷ Bedarf an sicherer Datenübertragung
  - ssh: Sicherer remote Zugriff
  - https: Sichere Webseiten
  - PGP: Sichere Emails
- Ursprünglich primäres Ziel:
  - Vertraulichkeit: sicherer Datentransfer
  - Verbindlichkeit (Integrität): meist implizit
- Email / mission-critical Applikationen:
  - Verbindlichkeit (diesmal explizit)

Verbindlichkeit

- Authentizität:
  - War er's, der das gesagt hat?
- Aber auch (¬Authentizität):
  - War der das wirklich NICHT?
  - Gerade juristisch bedeutsam!
- Integrität:
  - War's das, was er gesagt hat?

Public Key Kryptographie

- 1976: Diffie und Hellman:
  - "New Directions in Cryptography"
- Symmetrisch:
  - ein Schlüssel: Ver- und Entschlüsselung
- Asymmetrisch (Public Key):
  - Öffentlicher Schlüssel: Verschlüsselung
    - Absender verschlüsselt
  - Privater Schlüssel: Entschlüsselung
    - Empfänger entschlüsselt

Signaturen

- Manche Public Key Algorithmen: **kommutativ:**
  - Öffentlicher Schlüssel verschlüsselt / Privater entschlüsselt
  - Privater Schlüssel verschlüsselt / Öffentlicher entschlüsselt

  statt Verschlüsselung auch: Hashwerte

  Authentizität:

  ➡ Signatur
  - bekannt: RSA
    - Ronald **R**ivest Fiat **S**hamir, Leonard **A**dleman

Authentizität

- Ist das der Öffentliche Schlüssel von Hans?

Schlüsselverteilungsproblem:
  - trivial: persönliche Übergabe
  - viele Personen:
    Public Key Infrastructure (PKI)

Trust Infrastructure  CA
  - » Signaturen, Widerrufslisten
  - » Zertifizierungsrichtlinien

Begriffsbestimmung

- Schlüssel (Key)
  - **Verschlüsseln** von Dokumenten:
    Öffentlicher Schlüssel: Lesen darf's nur Hans
  - **Signieren** von Dokumenten:
    Privater Schlüssel: Hans hat's geschrieben
- Zertifizierungs-Schlüssel
  - Spezieller Schlüssel
  - **Zertifizieren**: Signieren von Schlüsseln:
    Der Schlüssel gehört wirklich Hans
  - Zertifikat mit dem Öffentlichen Schlüssel verbunden

Widerrufslisten

Insbesondere im Hinblick auf eine CA:

- Falsche Angaben bei Ausstellung
- Kompromittierung des Privaten Schlüssels
- ...

➡ Rücknahme eines Zertifikats
  - Widerrufsliste
  - Sperrliste
  - Certificate Revocation List: CRL

Zertifizierungsrichtlinien

- Wer zertifiziert?
- Wer zertifiziert den Zertifizierer?
- Nach welchen Regeln / Richtlinien?
- Was wird zertifiziert?
  - Auf jeden Fall: Bindung Person-Schlüssel

  aber evtl. auch:
  - Schlüsselqualität? Einhaltung Regeln? Zugriffsrechte?
  - Widerruf? Speicherung? Garantien? Haftung?

➡ Policy (Certification Practice Statement – CPS)
  - Information Dritter
  - Absicherung der Zertifizierungsinstanz

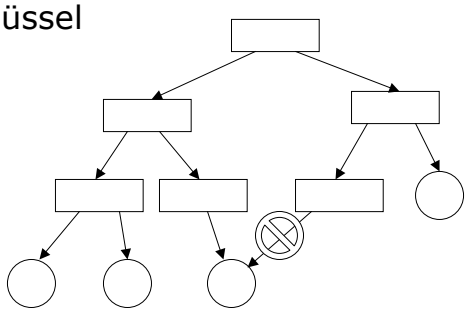
Infrastruktur

PGP: Web of Trust

- Jeder Schlüssel kann zertifizieren
  - Richard sagt: Ja, das ist Hans
  - Andy sagt: Ja, das ist Hans
  - Lutz sagt: Ja, das ist Andy
  - Mario kennt und vertraut Lutz...
    ... und weiß damit, daß Hans auch wirklich Hans ist
- Jeder kann Identität von jedem bestätigen
  - jeder kann jedem vertrauen ...
  - ... oder auch nicht

Infrastruktur

- X.509: Trust-Hierarchie
  - Zertifizierungs-Schlüssel
  - Schlüssel



i.A. KEINE
Doppelzertifizierung

Juristische Aspekte – SigG

Signaturgesetz (SigG)

Legaldefinitionen
- (einfaches) Zertifikat: (einfache) Signatur
- fortgeschrittenes Zertifikat: fortgeschrittene Signatur
- **qualifiziertes Zertifikat: qualifizierte Signatur**
  - Neusignierung von Dokumenten
- Zertifizierungsdiensteanbieter

- Anzeigepflicht
- Veröffentlichungspflicht für Zertifikate
- Freiwillige Akkreditierung akkreditierter Zertifizierungsdiensteanbieter

Juristische Aspekte - SigG

- sichere Signaturerstellungseinheit / Signaturanwendungskomponenten
  - Signieren von Dokumenten
  - stellt ab auf Chipkarten etc.
- technische Komponenten für Zertifizierungsdienste
  - Zertifizieren von Schlüsseln
- Haftung
  - Versagen der technischen Produkte
  - Versagen von Sicherheitseinrichtungen
- Deckungsvorsorge
  - Sicherung von Ansprüchen Dritter aus der Haftung
- etc.

Juristische Aspekte – SigV

Signaturverordnung (SigV)

- Regelung der Anzeige:
  - Führungszeugnisse, Fachkundenachweis, Sicherheitskonzept
- Regelungen zum Zertifikatverzeichnis
- Sicherheitsvorkehrungen
- Sperrung von qualifizierten Zertifikaten
- Regelung der Deckungsvorsorge
  - Haftpflichtversicherung (≥2.5Mio € pro Schadensfall)
  - Gewährleistungsverpflichtung Kreditinstitut
- Anforderungen Produkte, Datensicherung
- etc.

Juristische Aspekte: Hinweis

- Problem: DFN-PCA Handbuch von 2000
  - bezieht sich auf SigG/SigV von 1997
- Aber: 2001: SigG/SigV Neufassung
  - **dramatisch** überarbeitet

➡ DFN-PCA Handbuch veraltet

  - insbesondere:
    - keine Lizenzpflicht mehr: "genehmigungsfrei"
  - dafür:
    - Anzeigepflicht
    - Aufsicht durch zuständige Behörde
    - u.U. Untersagung des Betriebs (teilweise, ganz)
- Hier: SigG/SigV von 2001

Organisatorische Aspekte

- Im Vorfeld des Aufbaus einer CA:
  - Erstellung eines CA-Arbeitskonzepts
    - enthält: Sicherheitskonzept, Notfallkonzepte ("Tag X")
    - beschreibt im Wesentlichen, wer was wann tut
  - Erstellung einer CA-Policy
- Im Betrieb einer CA:
  - Ausstellen von Zertifikaten
  - Veröffentlichung, Datensicherung, Wartung
- Wer macht die Arbeit?
  - Literatur:
    - kleine CA's: 1 Stelle: ½ Organisation, ½ Technik
    - große CA's: 3 Stellen: 2 Organisation, 1 Technik

Technische Aspekte nach DFN-PCA

- Zertifizierungsrechner
  - empfohlen: Laptop (leicht wegzuschließen)
  - Standalone! Insbesondere kein Internet ☺
- Veröffentlichungsplattform
  - Zertifikate: zertifizierte Öffentliche Schlüssel
  - CRL's
- Datensicherung
- Zugriffsschutz
- Zugangskontrolle

Software

- bei Authority **und** Client abhängig von:
  - gewählter CA-/RA-Form
    - unterhalb einer SigG-CA / SigG-konform
      - abhängig von übergeordneter CA
      - RegTP-Bestätigung: http://www.regtp.de/
    - unterhalb der DFN-PCA / nicht SigG-konform:
      - OpenSSL
      - OpenCA
      - Client-seitig: Standard-Software (Netscape, IE, etc.)
- Siehe nächste Folien: Aufbau einer CA

Aufbau einer CA

- Grundlegende Frage:
  Eigene Root-CA oder unter einer anderen CA?
- Notwendige Frage:
  Wozu sollen die CA und die von ihr zertifizierten Schlüssel dienen?
  Im Wesentlichen:
  - Rechtssicherheit benötigt? Wie herstellbar?
- Im Folgenden Varianten:
  - Eigene Root-CA
  - unterhalb der DFN-PCA
  - unterhalb einer CA nach SigG

Eigene Root-CA

- Insellösung
- Vorteil: Unabhängigkeit
- Nachteil: Unabhängigkeit
- Cross-Zertifizierung i.A. später möglich
- Variante 1:
  - Eigene Root-CA mit "einfachem" Zertifikat
  - Unterschied zu unterhalb der DFN-PCA marginal
- Variante 2:
  - Eigene Root-CA nach SigG
  - Unterschied zu unterhalb einer SigG-CA marginal

Unterhalb der DFN-PCA

- **einfache** Zertifikate
- DFN-PCA ist **kein** Zertifizierungsdienste-anbieter nach SigG
- kein Geltungsbereich des SigG, insbesondere:
  - keine Anzeigepflicht nach SigG
  - keine Haftung nach SigG
  - keine Deckungsvorsorge nach SigG
- juristische Bedeutung:
  - nach DFN-PCA Policy: keine
  - Im Zweifel: Sachverständige, Gutachten, Gerichte
- Rechtssicherheit durch Vertrag/Satzung?

Unterhalb einer SigG-CA

- Rechtssicherheit nach SigG
- Vorschriften des SigG / der SigV gelten und sind zu beachten, insbesondere:
  - Anzeigepflicht
  - qualifizierte Zertifikate / Schlüssel
  - Haftung
  - Deckungsvorsorge
  - sichere Signaturerstellungseinheiten

↷ hohe Kosten

Registrierungsinstanz (RA)

- Unterhalb der DFN-PCA nicht möglich
- Unterhalb einer CA nach SigG:
  - qualifizierte Schlüssel mit allen Vor- und Nachteilen:
    - Rechtssicherheit
    - Neusignierung von Dokumenten
    - etc.
  - CA trägt sämtliche Verantwortung für alle Schlüssel, insbesondere auch Haftungsverantwortung, daher:
    - Kosten werden auf RA umgelegt, üblich:
    - Kosten pro zertifiziertem Schlüssel

Wie nun?

- Ernstzunehmende Alternativen:
  - SigG-konform:
    - Unterhalb einer SigG-CA
    - Als Registrierungsinstanz (RA) einer SigG-CA
      - in diesem Fall IMHO die bevorzugte Alternative
  - SigG-unkonform:
    - Unterhalb der DFN-PCA

Alternative: SigG-konform

- Rechtssicherheit automatisch (SigG)
- Kosten auf Authority-Seite:
  - CA:
    - technische Komponenten für Zertifizierungsdienste
    - Deckungsvorsorge
    - qualifiziertes (teures) Personal
  - RA:
    - fixe Kosten pro zertifiziertem Schlüssel
- Kosten auf Benutzer-Seite:
    - sichere Signaturerstellungseinheiten
    - Signaturanwendungskomponenten

Alternative: SigG-unkonform

- Rechtssicherheit muß "irgendwie" hergestellt werden
- Kosten auf CA-Seite:
  - Hardware mit Standard-Software
  - Personal
- Kosten auf Benutzer-Seite:
  - Hardware mit Standard-Software

Zusammenfassung

- Wahl der CA-/RA-Form: nicht trivial
- abhängig von verschiedenen Faktoren:
  - Zweck: Wozu sollen die Schlüssel dienen?
  - Zweck: Benötigte Rechtssicherheit?
  - Investierter Arbeitsaufwand: **Personal**!
  - last, but not least: **Kosten**!
- Wahl der Software:
  abhängig von der CA-/RA-Form

Ausblick

- Realer Aufbau einer CA
  - vermutlich unterhalb DFN-PCA
  - Personal!
- Erfahrungen sammeln:
  - Know-How: organisatorisch, technisch
  - juristisch

- WENN Bedarf:
  - Entweder CA, aber vermutlich eher RA nach SigG

Fragen?