

PKI: Ein Tanz um das goldene Kalb?



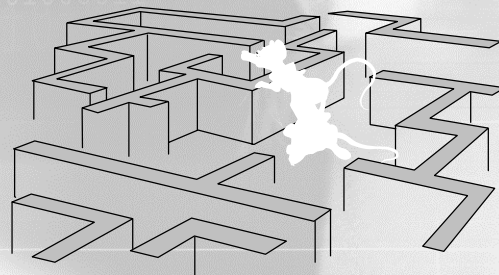
© 1634 Nicolas Poussin

PD Dr. Rolf Oppliger
Informatikstrategieorgan Bund (ISB)
Holzikofenweg 8, 3003 Bern
Tel. +41 (0)31 325 96 96, Fax. +41 (0)31 322 45 66, E-Mail: rolf.oppliger@isb.admin.ch

Inhaltsübersicht



1. PKI
2. Rolle des Staates
3. Rechtliche Rahmenbedingungen
4. PKI-Markt
5. Schlussfolgerungen
6. Ausblick



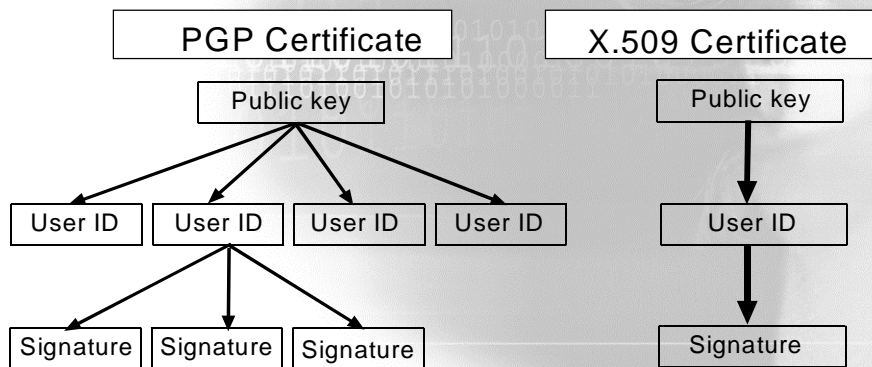
© 2001 Rolf Oppliger

28. März 2001

Folie 2

1. PKI 1/6

- Ein **Zertifikat** wird von einer vertrauenswürdigen Stelle ausgestellt und ausgegeben, um eine bestimmte Eigenschaft (Attribut) einer Entität zu beglaubigen
- Ein **Public Key Zertifikat** hat die Zugehörigkeit eines öffentlichen Schlüssels zu einer (oder mehreren) User ID(s) zu beglaubigen



© 2001 Rolf Oppliger

28. März 2001

Folie 3

PKI 2/6

- Die meisten heute im Einsatz stehenden Public Key Zertifikate sind konform zu **ITU-T X.509** Version 3
- Leider lässt der Standard so viele Erweiterungen zu, dass in jedem Anwendungsbereich eine spezifische **Profilierung** erforderlich ist
- Für das Internet findet diese Profilierung im Rahmen der **IETF PKIX WG** statt
- Im Rahmen der **IETF SPKI WG** werden alternative Ansätze untersucht und diskutiert

Version
Certificate serial number
Signature algorithm identifier
Issuer
Validity period
Subject
Subject public key information
[Issuer unique information]
[Subject unique information]
[Extensions]
CA's digital signature

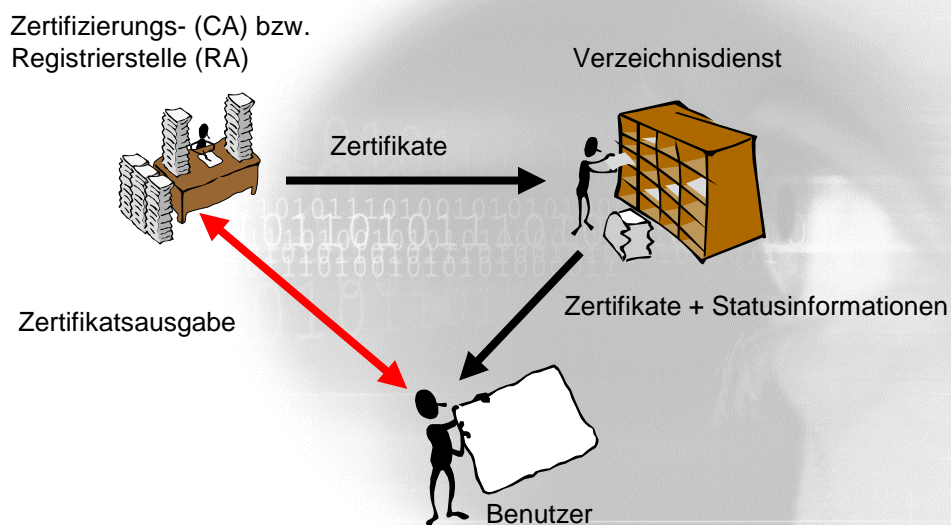


© 2001 Rolf Oppliger

28. März 2001

Folie 4

- Eine **Public Key Infrastruktur (PKI)** stellt eine Infrastruktur für die Verwaltung von Public Key Zertifikaten dar
- Public Key Zertifikate werden von **Certification Authorities (CAs)** ausgegeben und im Rahmen von Verzeichnisdiensten verwaltet
- Gemäss RFC 2828 („Internet Security Glossary“) ist eine PKI folgendermassen definiert:
 - „A system of CAs [...]
 - that perform some set of certificate management, archive management, key management, and token management functions
 - for a community of users
 - in an application of asymmetric cryptography.“



- Ansätze für die Vermittlung von Statusinformationen:
 - Certificate Revocation Lists (CRLs)
 - Delta-CRLs
 - Online Certificate Status Protocol (OCSP)
 - Certificate Revocation System (CRS)
 - Certificate Revocation Trees (CRTs)
 - ...
- Grundsätzlich macht die Möglichkeit zur **Revozierung** von Zertifikaten eine Online-Komponente erforderlich
- Die Möglichkeit zur **Suspendierung** von Zertifikaten macht die Situation (in bezug auf die Validierbarkeit der Zertifikate zu einem beliebigen Zeitpunkt) sehr schwierig

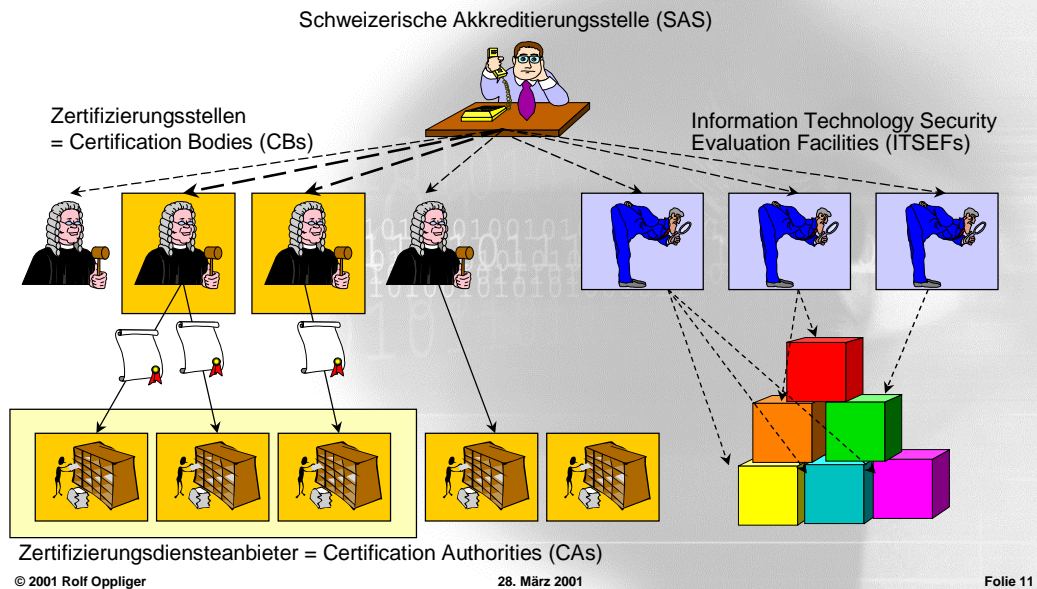
- Primäre Einsatzgebiete:
 - Sicherheit von Web-basierten Applikationen mit Hilfe von **Secure Sockets Layer (SSL)** bzw. **Transport Layer Security (TLS)**
 - Austausch von kryptographisch abgesicherten elektronischen Nachrichten mit Hilfe von **Secure MIME (S/MIME)** oder **PGP** bzw. **OpenPGP**
 - Virtuell private Netze und gesicherte Netzanbindungen mit Hilfe von **IPSec**
- Primäre Motive für den Einsatz von asymmetrischen Kryptosystemen und PKIs sind **Skalierbarkeit** (insbesondere effiziente Schlüsselverwaltungsverfahren) und **Verbindlichkeit** (z.B. mit Hilfe von digitalen Signaturverfahren)
- Für digitale Signaturen ist eine PKI zwingend erforderlich

2. Rolle des Staates

- Man kann sich fragen, ob der Aufbau und Betrieb einer PKI eine staatliche Aufgabe sei (z.B. Finnland)
- In der Schweiz ist diese Frage im Rahmen einer interdepartementalen Arbeitsgruppe untersucht worden
- Dabei ist man zum Schluss gekommen,
 - dass der Aufbau und Betrieb einer PKI nicht zwingend eine staatliche Aufgabe ist,
 - dass aber die Definition eines Gütesiegels für qualitativ hochwertige Anbieter von Zertifizierungsdiensten eine staatliche Aufgabe ist (auch aus Eigeninteresse der Bundesverwaltung)
- Dieser Grundsatzentscheid hat die bisherigen Aktivitäten im PKI-Bereich innerhalb der Bundesverwaltung geprägt

3. Rechtliche Rahmenbedingungen ^{1/4}

- Seit dem 1. Mai 2000 ist eine **Verordnung über Dienste der elektronischen Zertifizierung (ZertDV)** in Kraft (vgl. <http://www.admin.ch/ch/d/sr/7/784.103.de.pdf>)
- Der Entwurf eines **Bundesgesetzes über die elektronische Signatur (BGES)** befindet sich in der Vernehmlassung
- Für eine Umsetzung der ZertDV und BGES sind **Ausführungsvorschriften** und entsprechende Kriterien zur Prüfung von Zertifizierungsdiensteanbietern erforderlich
- Ein erster Entwurf ist vom BAKOM und von der SAS erarbeitet worden (vgl. <http://www.bakom.ch/eng/subsubpage/document/309/1576>)
- Dieser Entwurf befindet sich ebenfalls in der Vernehmlassung



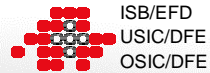
- Am 30.11.99 hat die EU eine **Richtlinie** über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen verabschiedet
- Die Richtlinie verlangt,
 - dass die EU-Mitgliedstaaten ein freiwilliges Akkreditierungssystem für Zertifizierungsdiensteanbieter aufbauen
 - dass die rechtliche Anerkennung der elektronischen Signaturen, die im Rahmen dieses Systems ausgegeben werden, geregelt wird
- Im Rahmen der **European Electronic Signature Standardization Initiative (EESSI)** werden Vorgaben für die Umsetzung der EU-Richtlinie im Rahmen von nationalen Signaturgesetzen erarbeitet
- Einzelne EU-Mitgliedstaaten haben entsprechende Gesetze bereits erlassen oder sind daran, solche zu erlassen
- ZertDV und BGES scheinen mit der EU-Richtlinie konform zu sein

Rechtliche Rahmenbedingungen ^{4/4}



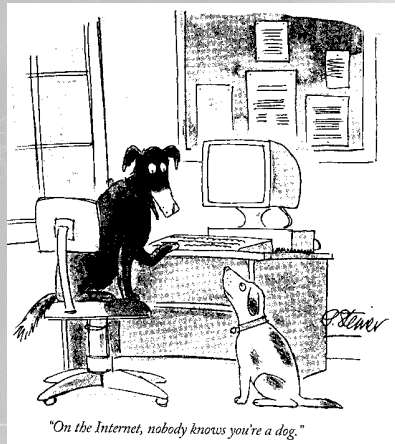
- Die Ausarbeitung der Vorgaben für **Signaturgesetze** ist eine schwierige Gratwanderung zwischen zu anspruchsvollen und zu unverbindlichen Anforderungen:
 - Sind die Anforderungen zu anspruchsvoll, kann Konformität auf der Produkte- und Dienstleistungsebene nur schwer erreicht werden
→ das entsprechende Gesetz erhält dann kaum praktische Bedeutung (z.B. SigG/SigV in Deutschland)
 - Sind die Anforderungen zu unverbindlich, verliert Konformität an juristischem Wert → das entsprechende Gesetz erhält dann ebenfalls kaum praktische Bedeutung (z.B. Signaturgesetz in den USA)
- Vor diesem Hintergrund erscheint die langfristige Entwicklung der Signaturgesetze offen

4. PKI-Markt ^{1/4}



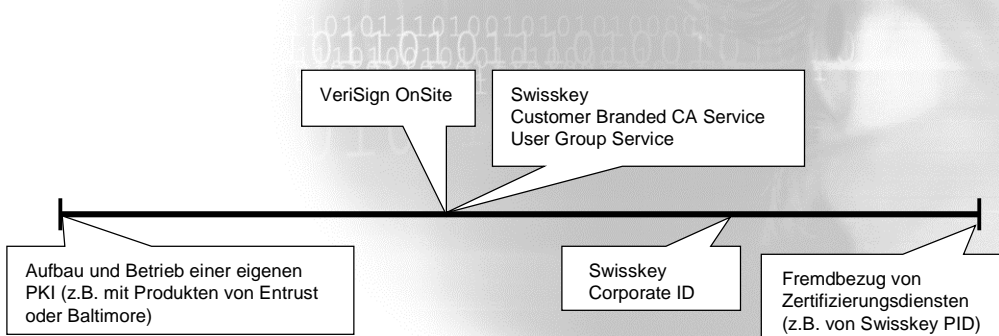
- Informatiksicherheit ist als Fachgebiet
 - komplex
 - schwer zu messen
 - schwer zu kommunizieren
- Entsprechend gesucht und aggressiv vermarktet werden auf dem Informatiksicherheitsmarkt einfache und einfach zu kommunizierende Lösungen
- Die jüngsten Beispiele sind Firewalls, „Intrusion Detection“-Systeme (IDS), virtuell private Netze (VPN) und PKIs
- Eine grosse Zahl von Firmen bieten PKI-Produkte (z.B. Entrust, Baltimore Technologies, ...) und -Dienstleistungen an (z.B. VeriSign, Swiskey, ...)

- Die Informatiksicherheitsindustrie hat lange Zeit argumentiert, dass die Existenz einer PKI eine notwendige Voraussetzung für den **elektronischen Handel (E-Commerce)** sei (vgl. Cartoon)
- Diese Kausalität muss hinterfragt werden
- Im elektronischen Handel geht es nur vordergründig um Authentizität (in erster Linie geht es um Autorisierung)
- Dabei stellt die Authentifikation oft eine notwendige aber in keinem Fall eine hinreichende Bedingung für die Autorisierung dar



- Autorisierungsmöglichkeiten:
 - Codierung von Autorisierungsinformation in Public Key Zertifikaten (z.B. im Rahmen von X.509 Extension Fields)
 - Verwendung von spezialisierten Attributzertifikaten
 - Verwaltung von Autorisierungsinformation in Datenbanksystemen
- Letztendlich geht es um die Bereitstellung von Infrastrukturen für die Behandlung von Authentifizierungs- und Autorisierungsfragen
- Neue Begriffe:
 - Authentication and Authorization Infrastructure (AAI)
 - Privilege Management Infrastructure (PMI)
 - ...

- Viele Unternehmen stehen heute vor der Frage, ob sie eine PKI selbst aufbauen und betreiben sollen, oder ob sie entsprechende Dienstleistungen fremdbeziehen sollen
- Dabei wird diese Frage leider meist nur an den Endpunkten eines ganzen Spektrums von Möglichkeiten diskutiert



5. Schlussfolgerungen ^{1/3}

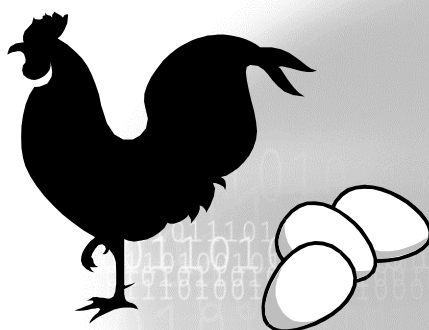
- Eine PKI ist eine **Infrastruktur**, d.h. eine PKI erzeugt selbst keine Sicherheit
- Eine PKI kann allenfalls eingesetzt werden, um Sicherheitslösungen zu realisieren, die
 - skalierbar sind,
 - resistent gegenüber „Man-in-the-middle“-Angriffen sind und
 - von digitalen Signaturen Gebrauch machen
- Allerdings müssen Applikationen und entsprechende Applikationsprogramme angepasst werden, um von einer PKI Gebrauch zu machen (d.h. sie müssen „PKI-enabled“ werden)
- Diese Anpassungen sind in der Regel kostspielig und nicht immer möglich (z.B. bei proprietären Applikationen)

Schlussfolgerungen ^{2/3}



- Das finnische Beispiel zeigt, dass nur wenige Bürger(innen) bereit sind, ein Public Key Zertifikat zu erwerben (6'045 Chipkarten bis im September 2000)
- Entsprechend wird der Aufbau und Betrieb einer PKI getragen (und finanziert) werden müssen von den Applikationen, die von dieser PKI Gebrauch machen
- Für die entsprechenden Applikationsbetreiber ist die Wahl zwischen PKI-basierten Sicherheitstechnologien und alternativen Technologien in erster Linie wirtschaftlich zu begründen (d.h. PKI-basierte Sicherheitstechnologien müssen effizienter sein)
- Diese Begründung kann nicht immer gegeben werden (z.B. Benutzerauthentifizierung im Internet-Banking)

Schlussfolgerungen ^{3/3}



- Der Aufbau und Betrieb einer PKI stellt ein „**Huhn-Ein**“-Problem dar:
 - Applikationen können auf keine existierende PKI zurückgreifen
 - Der Aufbau und Betrieb einer PKI lässt sich - aufgrund fehlender Applikationen - kaum begründen

6. Ausblick

- In der **digitalen Welt** wird sich eine ähnliche Situation ereignen, wie in der **realen Welt**
- In der realen Welt ...
 - ... haben wir viele Ausweise
 - ... wäre es grundsätzlich auch möglich, nur einen (multifunktionalen) Ausweis zu verwenden
 - ... gibt es nur wenige amtlich beglaubigte Ausweise (mit in der Regel nur einer Qualitätsstufe, nur statischer Information und keinen Haftungsregelungen)
 - ... geben viele Organisationen - aufgrund dieser amtlich beglaubigten Ausweispapiere - eigene Ausweispapiere aus (z.B. Mitgliederausweise)
 - ... dienen diese Ausweise in erster Linie der Autorisierung

Fragen und Antworten

