Swiss Open Systems User Group

PKI – die Wunderwaffe zur Vertrauensbildung ? !

iT_SEC iT_Security AG

Daniel A. Pfenninger
Manager Sales
Tel. direkt 01/ 404 82 55
daniel.pfenninger@it-sec.com

Technopark Zürich
30. Januar 2002

ITSEC

Agenda

- **Einleitung**
- Einsatz
- Technik
- Interoperabilität
- Markt
- Wirtschaftlichkeit
- Projektorganisation
- Rechtslage

2

Was ermöglicht das Internet?

- Elektronische Post und Dokumente ersetzen Briefe und Formulare
- Kommunikation über das Internet beschleunigt und vereinfacht die Abwicklung von Geschäftsprozessen
- Verteilte Arbeitsgruppen arbeiten in virtuellen Teams

3

Wir brauchen ein elektronisches Äquivalent

Physikalische Welt	Digitale Welt
 Authentisierung	Digitale Zertifikate
 Beweisbarkeit	Digitale Signaturen
 Vertraulichkeit	Verschlüsselung

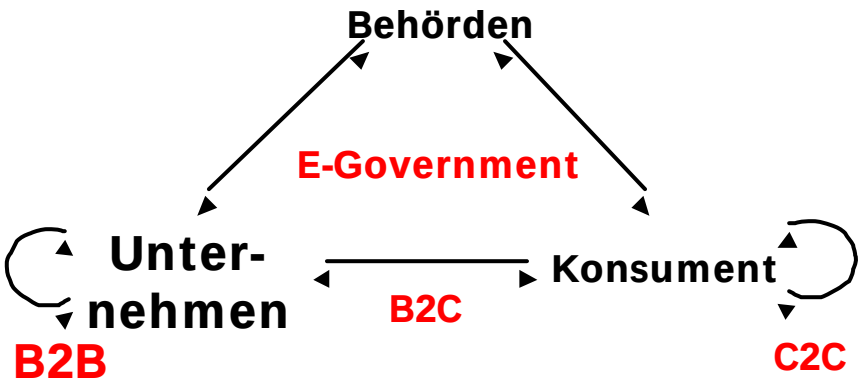
4

Agenda

- Einleitung
- **Einsatz**
- Technik
- Interoperabilität
- Markt
- Wirtschaftlichkeit
- Projektorganisation
- Rechtslage

5

Geschäftsbeziehungen



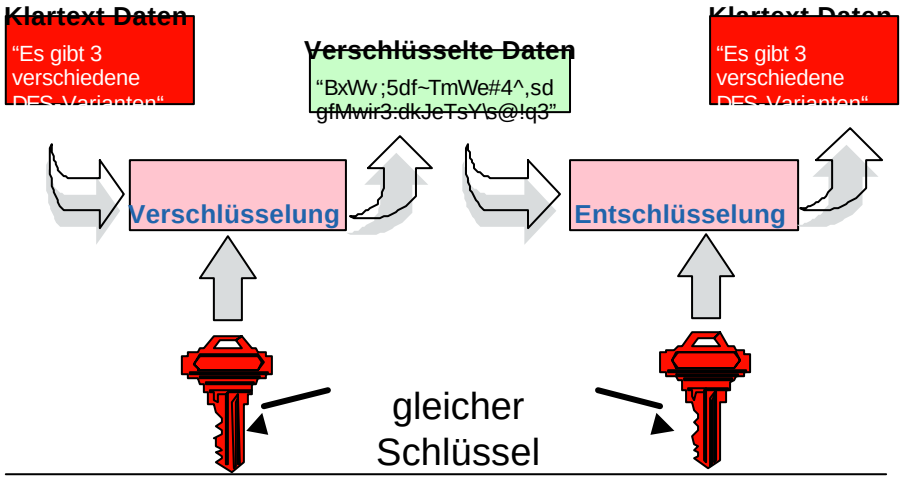
6

Agenda

- Einleitung
- Einsatz
- **Technik**
- Interoperabilität
- Markt
- Wirtschaftlichkeit
- Projektorganisation
- Rechtslage

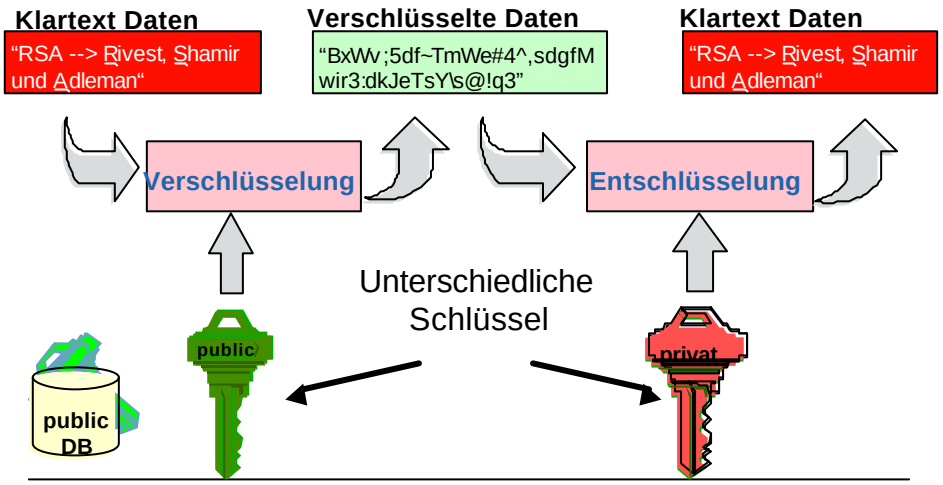
7

Symmetrische Algorithmen



8

Asymmetrische Algorithmen



9

Hash Funktionen

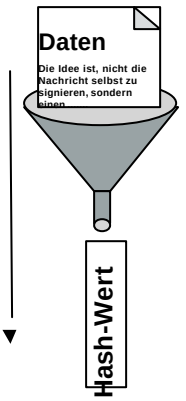
HASH ist eine Einweg-Funktion, welche eine Nachricht (Datenfile) in einer „quasi" Checksumme abbildet.

Einige bekannte Hash-Funktionen:

MD 5 (Message Digest 5) 128 bit

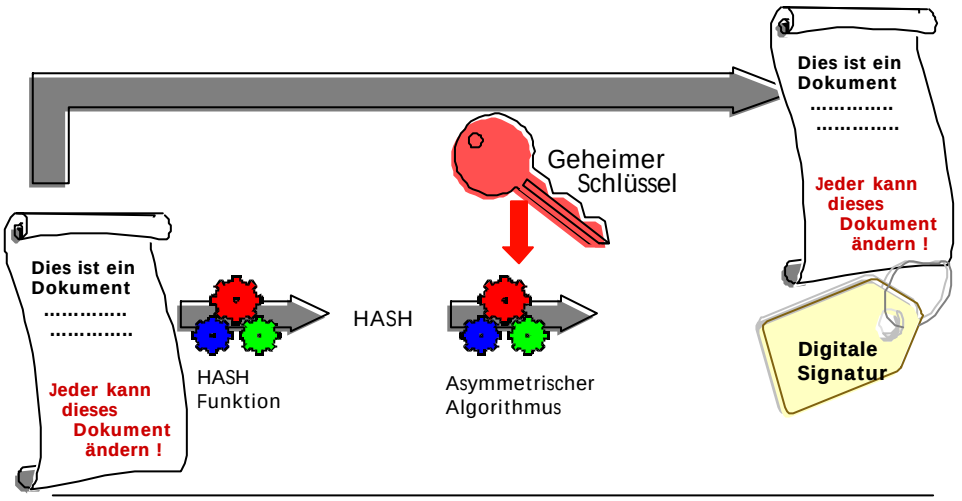
SHA (Secure Hash Algorithm) 160 bit

RIPEMD 160 (Race Integrity Primitives Evaluation) 160 bit



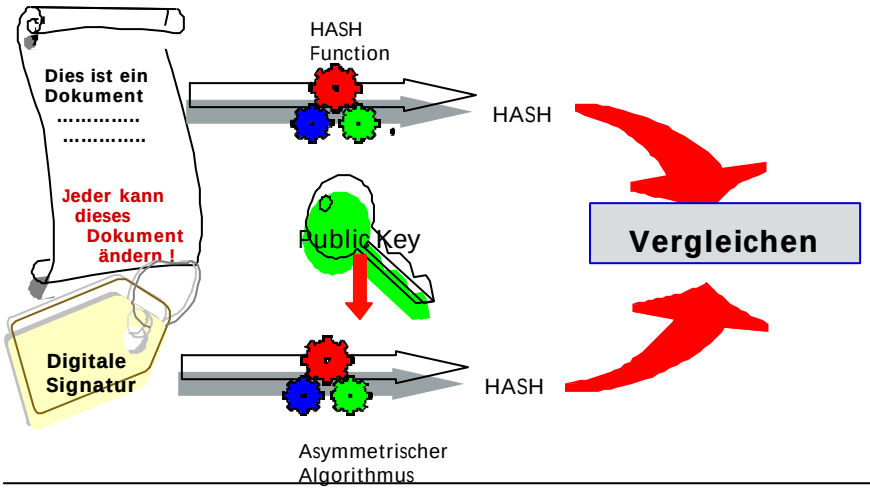
10

Digitale Signatur --> Generierung



11

Digitale Signatur --> Verifizieren



12

Zertifikate

- Ein Zertifikat ist eine untrennbare Verbindung zwischen dem Public-Key eines Anwenders und seiner Identität (z.B. E-Mail Adresse)
- Die Daten des Zertifikats werden von einer höheren Instanz (Certification Authority = CA/ Trust Center) unterschrieben.
- Ein Zertifikat dient zum sicheren Übermitteln der Identität und des Public Keys eines Partners
- Zertifikate können wieder zertifiziert werden (Hierarchie)

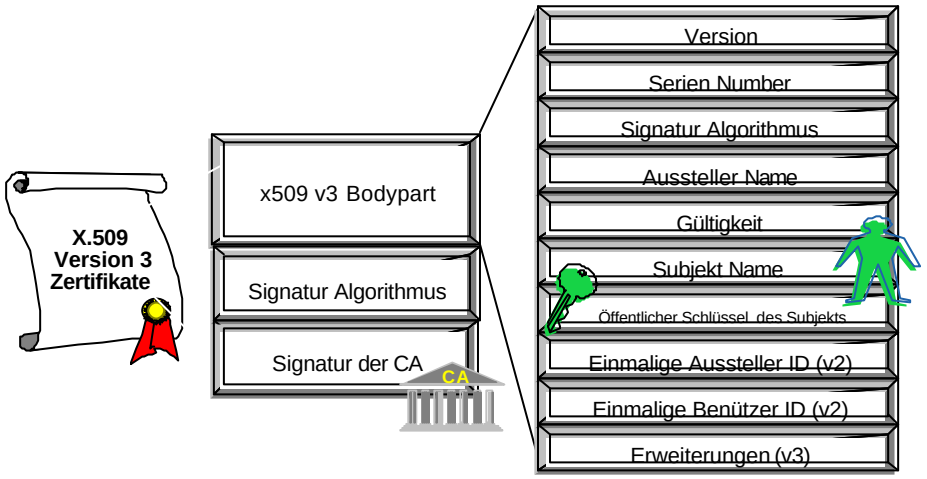
13

X.509

- Authentication Framework von X.500
- Erste Version in 1988
- Der Standard für PKI
- Heute Version 3 verfügbar (‘95, ‘97)
- Andere Standards benützen X.509 z.B. PKIX, SET, S/MIME,.....

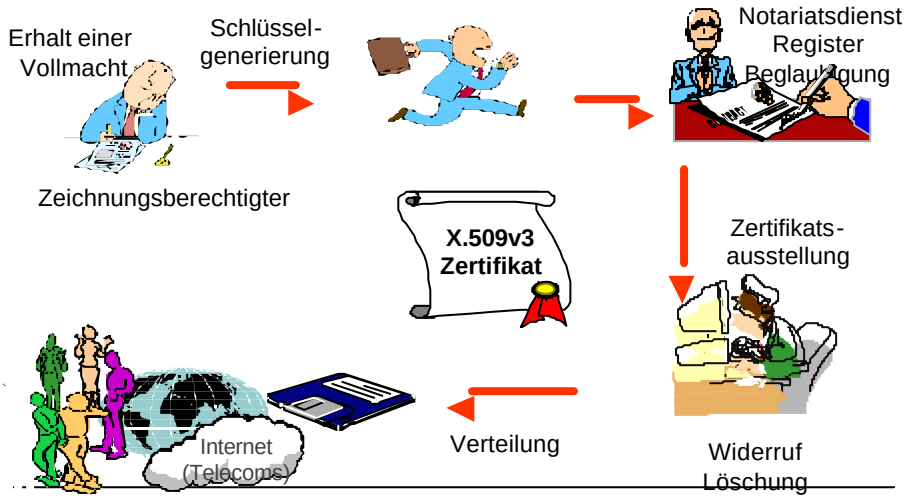
14

Struktur von Zertifikaten



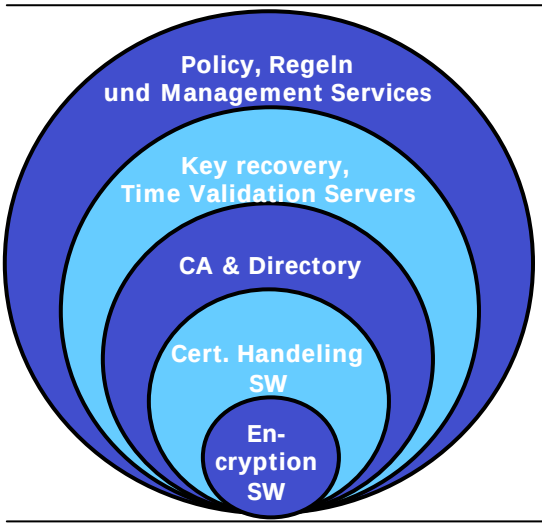
15

Erzeugung eines Zertifikates



16

Was ist eine PKI ?

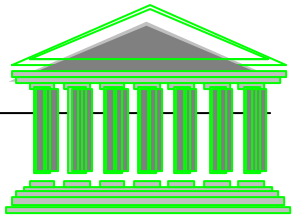


Eine Ansammlung von Applikationen, Regeln, Standards und Gesetzen, welche sich aus einer Public Key Technologie ergeben.

Source : iWord, Hambrecht and Quist, 1998 und RSADSI, 1999

17

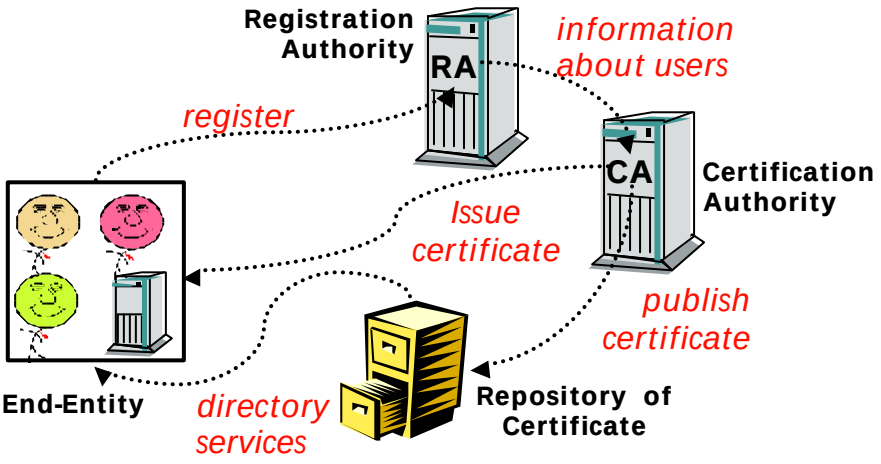
PKI Merkmale



- Unterstützung von Standards PKIX, X.509, PKCS, X.500
- Flexible Schlüssel Policy
- Skalierbarkeit
- Verfügbarkeit/Fehlertoleranz
- Interface zu anderen PKIs
- Unterstützung von Hardware Optionen

18

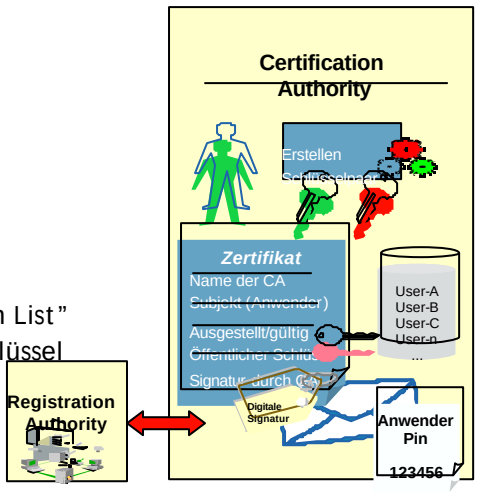
Basis-Elemente einer PKI



19

Certification Authority (CA)

- Trust
- Merkmale (Aufgaben)
  - Anwender ID bestätigen
  - Zertifizierung Anwender-Schlüssel
  - PIN Code Erstellung
  - PIN Mailer
  - Run "Certificate Revocation List"
  - Ev. erstellen Anwender-Schlüssel



20

Registration Authority (RA)

- Das effektive User Interface der PKI
- Merkmale
  - Anwender ID Erstellung
  - Anwender-Schlüssel Abfrage
  - Anwender-Schlüssel Aufbewahrung (SmartCard, KeyFile)
  - Aufhebung des Anwender-Schlüssels
  - Aufbewahrung CRL
  - Anwender-Schlüssel Erneuerung/ Aktualisierungsaufforderung

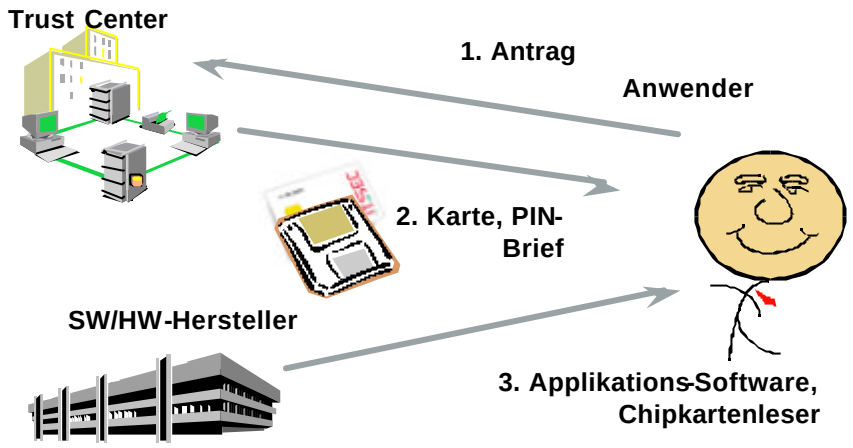
21

Ergänzende PKI Module

- Secure Communication
- Secure Time Stamping
- Notarization
- Validation
- Automatic Key Update
- Key Recovery and History Management
- Cross-Certification
- Client Software
- Hardware Support

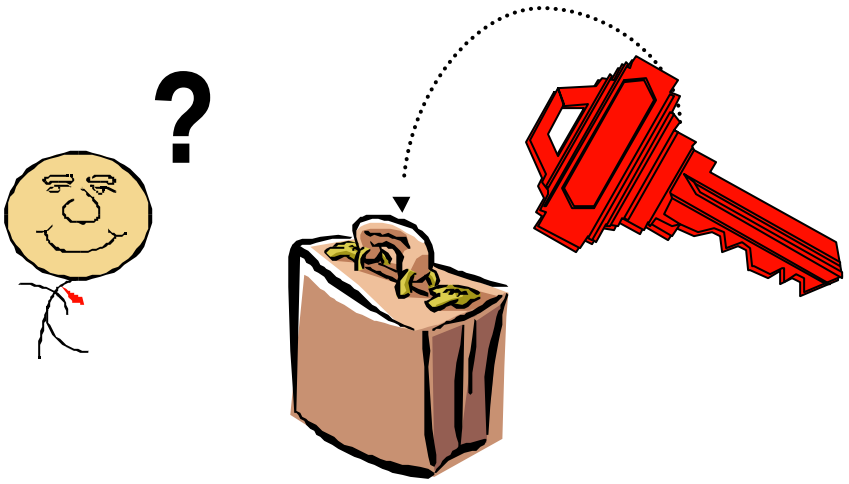
22

Generierung eines Zertifikates (vereinfachte Darstellung)



23

Wo werden die privaten Schlüssel gespeichert ?



24

Soft Token / Hard Token

Hard Token

Geheimnisse verlassen nie die Karte – alle sicherheitsrelevanten Operationen werden auf der Karte durchgeführt

Soft Token

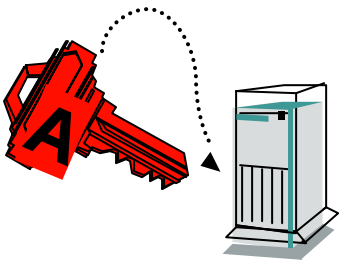
sicherheitsrelevanten Operationen können nicht auf der Karte durchgeführt werden

25

A: Hard Disk

- Einfache Lösung
  - Jeder Computer hat eine Festplatte
- Diese Sicherheit basiert auf dem Windows Passwort

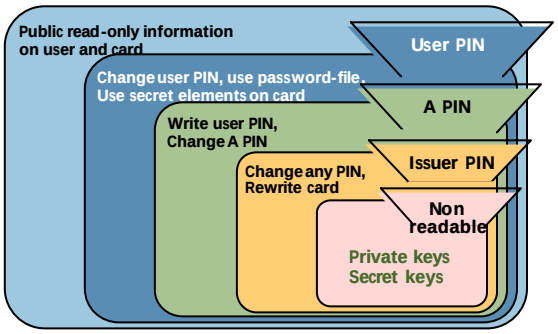
⇒ Provide low security



26

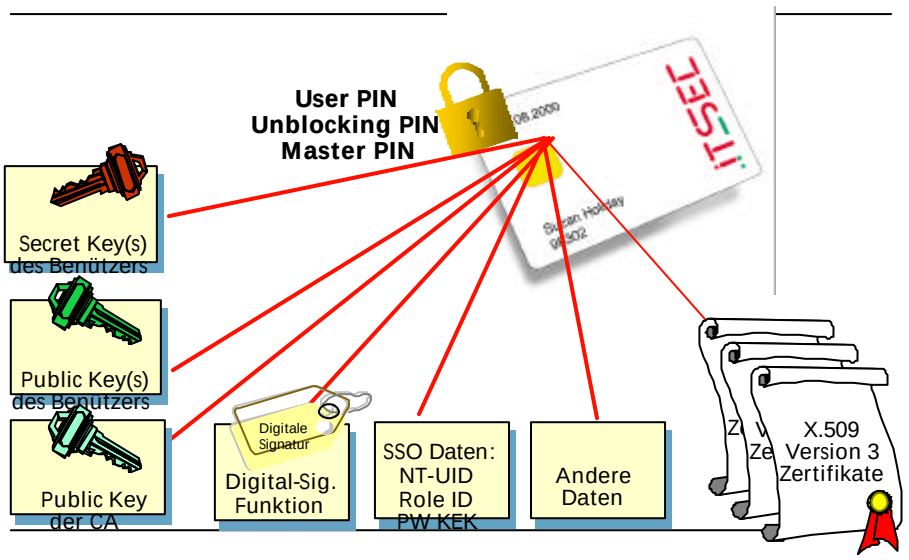
B: Smartcard

Security Shells einer "tamper-protected" Smartcard



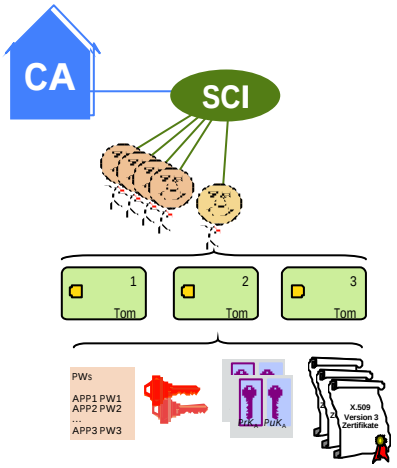
27

SmartCard -- Gespeicherte Information & Funktionen



28

Smart Cryptocard Infrastructure

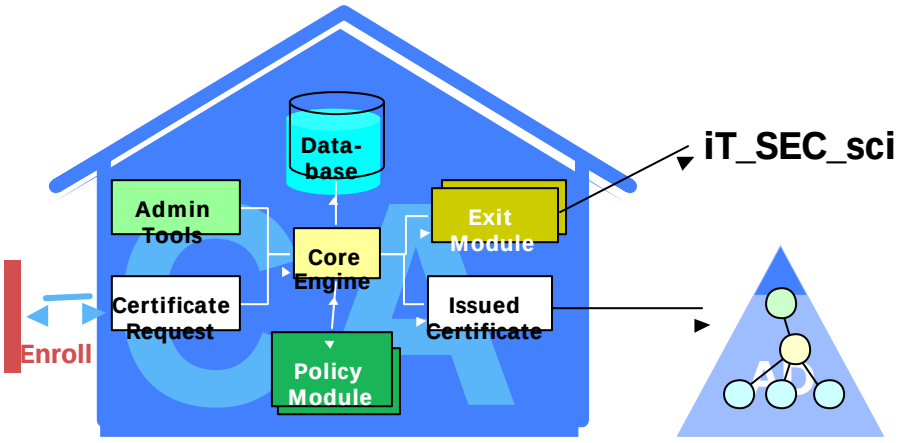


- Smartcard Management
- Key Management
- Assistent Funktionen
- Dezentralisierte Kartenaustellung
- User Management

- Mehrere Karten pro User
- Pro Karte
  - Passwort Container
  - Symmetrischen Schlüssel Container
  - Public Key Paar
    - Zertifiate

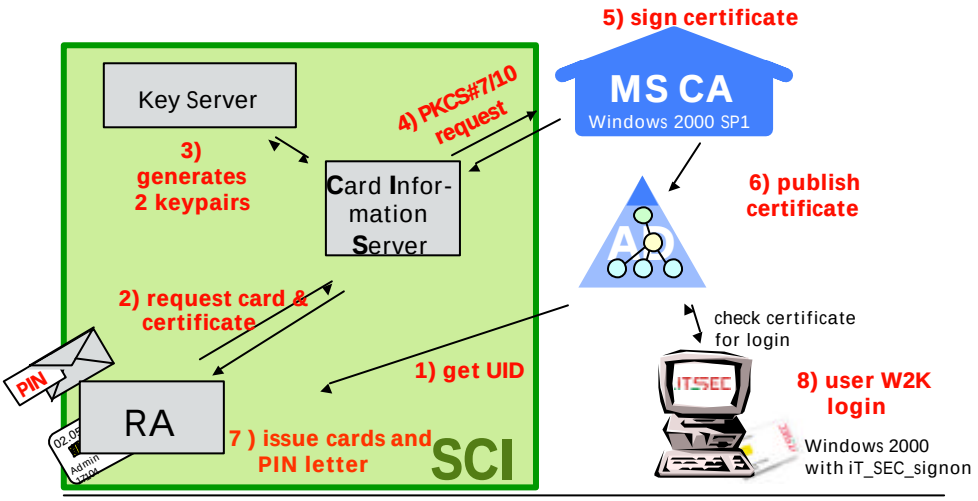
29

Windows 2000 Enterprise CA Components



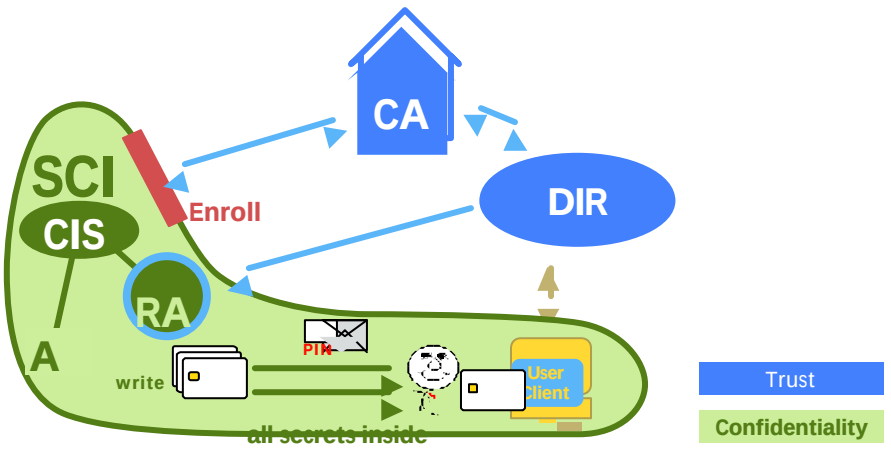
30

iT_SEC_sci mit Windows 2000



31

The Concerns Trust and Confidentiality



32

Agenda

- Einleitung
- Einsatz
- Technik
- **Interoperabilität**
- Markt
- Wirtschaftlichkeit
- Rechtslage

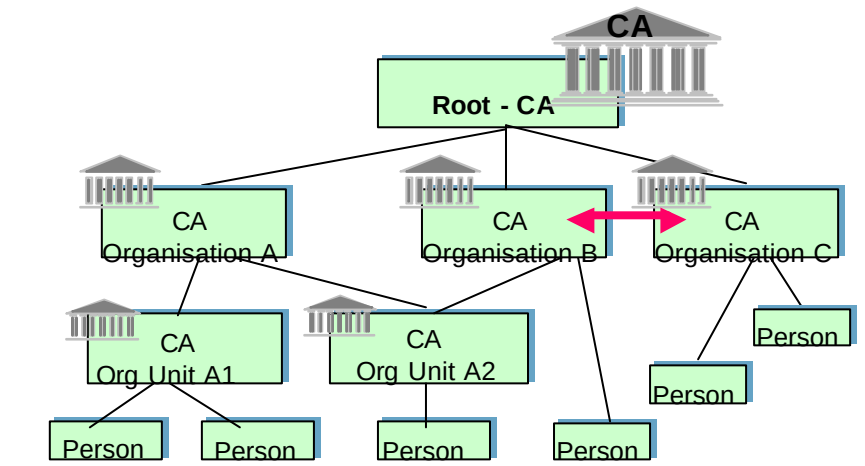
33

PKIX Topics

- IETF Arbeitsgruppe seit 1995
- Fokus auf X.509-based public-key infrastructure für Internet Applikationen
- Profiles für X.509 V3 Zertifikate und V2 CRL
- Policy Guidelines
- Management Protocols
  - registration; certificate request; initialisation; distribution
  - recovery
  - key-pair/certificate update
  - cross-certify
  - CRLs

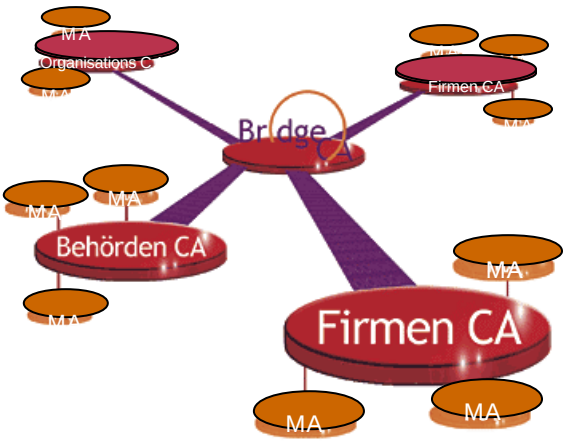
34

X.509 Hierarchie und "Cross Certification"



35

Interoperabilität mittels Bridge-CA



Bridge-CA als organisations-übergreifende PKI-Lösungen.

36

Agenda

- Einleitung
- Einsatz
- Technik
- Interoperabilität
- **Markt**
- Wirtschaftlichkeit
- Projektorganisation
- Rechtslage

37

Was für Lösungen benötigen PKIs ?

- Secure Mail
- VPN Solutions
- RAS solutions
- Browsers;
  - Mail
  - SSL
- Access Control
- SET Applikationen
- WEB Servers
- Banking Applikationen
- Und viele mehr ...

38

Swiss Trust Center: WISeKey

EuroTrust lands its largest e-security transaction ever with closing of $525,000 sale to WISeKey of Switzerland

EuroTrust to deliver 100,000 digital certificates to WISeKey and its clients, along with a full OnSite PKI Solution from VeriSign

In addition, WISeKey has purchased one VeriSign's full OnSite solutions through EuroTrust that will be used in WISeKey's Certification Services.

Source: http://www.eurotrust.dk/news/largestsale.php; PR 18.12.2001

39

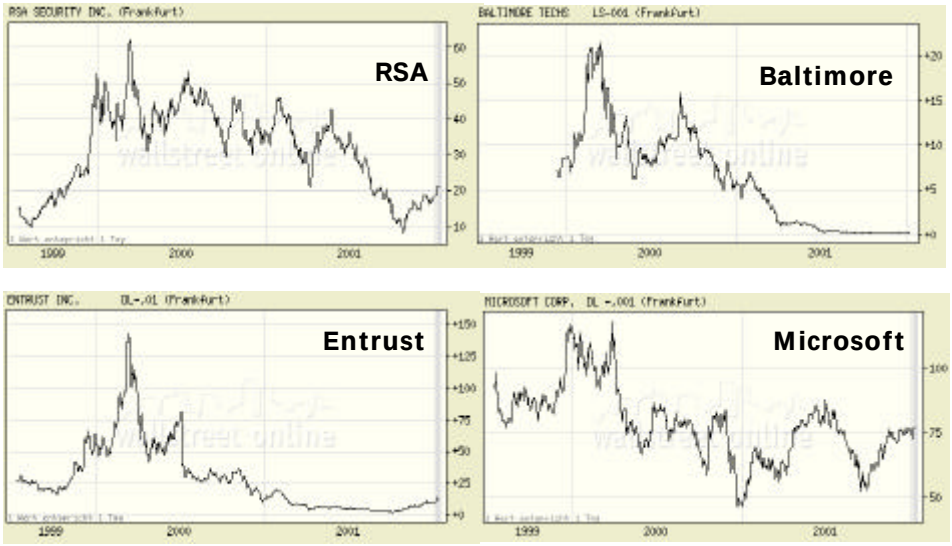
Verschiedene PKI Hersteller

BALTIMORE GTE Cybertrus
RSA Data Security. SecurityDynamics
xcert international inc.
swisscert
SwissSign
GlobalSign
Microsoft
VeriSign
GEMPLUS Celo
SPYRUS
THAWTE
EuroTrust
iTSEC
CertCo
Entrust
SSE
PHAOS TECHNOLOGY
sonera
Smart
iD2

40

PKI's an der Frankfurter Börse

(per 8.1.2002)



41

Agenda

- Einleitung
- Einsatz
- Technik
- Interoperabilität
- Markt
- **Wirtschaftlichkeit**
- Projektorganisation
- Rechtslage

42

Ausgewählte Branchenstatistik

Dell Computer (Revenue 2000: 31‘888 Mio US$)

- ca. 50 % des Umsatzes via Internet.
- > 40 Mio US $/pro Tag per Internet

Cisco (Revenue FJ 2001: 22‘200 Mio US$)

Einsparungen im 2000:

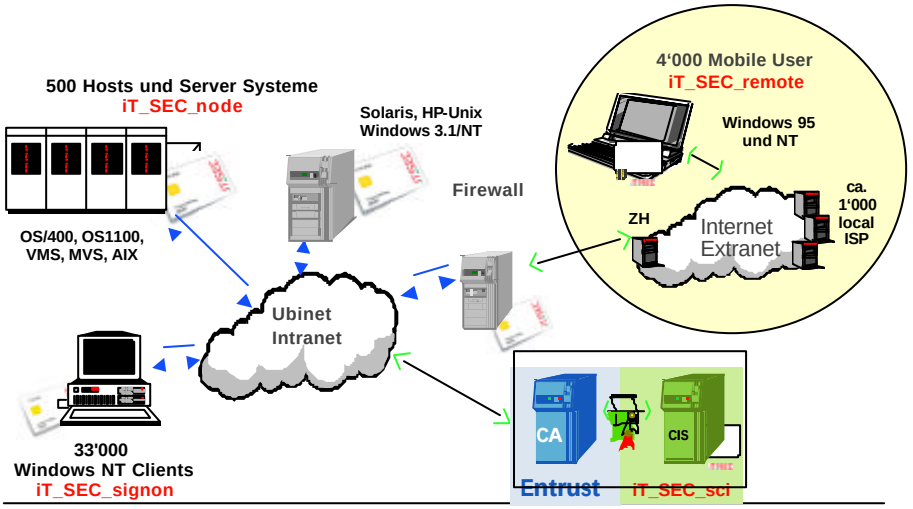
- 30 Mio US$ Kundenbetreuung
- 40 Mio US$ Online-Publikation
- 250 Mio US$ Software Downloads

43

iT_SEC Information Security

basierend auf Smartcards und allg. Sicherheitsdiensten (GSS)

UBS



ITSEC

44

Der Stand der Dinge

UBS

- Ca. 33‘000 PCs sind mit einem Kartenleser ausgestattet, Laptops haben einen PCMCIA-Kartenleser
- Ca. 30‘000 Benutzer haben eine persönliche Smartcard
- Ca. 20‘000 Personen nutzen die Smartcard (freiwillige Nutzung!)
- Für den „Remote“-Zugriff auf die IT-Ressourcen der Bank (ca. 4‘000 Laptop Benutzer) ist Nutzung der Smartcard obligatorisch
- Werbekampagne von Februar bis Mai 2001: ca. 150 IT-Berater geben jeder Benutzerin/jedem Benutzer eine 7-minütige Instruktion
- Heute ist der Login von 40 der wichtigsten Anwendungen automatisiert. 20 davon mit automatisierter Passworteingabe, 20 mit zertifikatsbasiertem Login

45

UBS Statements

UBS

Nutzen durch Einführung einer zertifikatsbasiernden Single-Sign-On Lösung mit dazugehörigem Smartcardmanagement:

- Eine PKI muss mit einer SCI komplementiert werden
- Erhöhte Sicherheit durch Besitz und Wissen
- Akzeptanz der Anwender (weniger Passwörter)
- Eine Produktivitätsteigerung von ca. 60 Minuten pro Mitarbeiter. Dies ergibt bei 30.000 Anwendern:
  - eine "Zeitersparnis" von 30.000 Stunden
  - oder 18 Mann-Jahre
  - eine jährliche Kostenersparnis von ca. CHF 4 Mio.

46

Betriebsaufwand 4 Vollzeitstellen (VZS)

- 0,5 VZS für Kartenproduktion
- 1,0 VZS für Help-Desk
- 2,0 VZS für Centre of Competence PERSAUTH
- 0,5 VZS für Produktintegration Systemtechnik

- „Versteckt“
  - Betrieb des SCI-Servers, Betrieb des CA-Services, Betrieb des Directory-Services
  - ca. 200 Ersatzkarten pro Monat (200*12*20=48‘000): ca. 50‘000.- CHF/ Jahr

47

Agenda

- Einleitung
- Einsatz
- Technik
- Interoperabilität
- Markt
- Wirtschaftlichkeit
- **Projektorganisation**
- Rechtslage

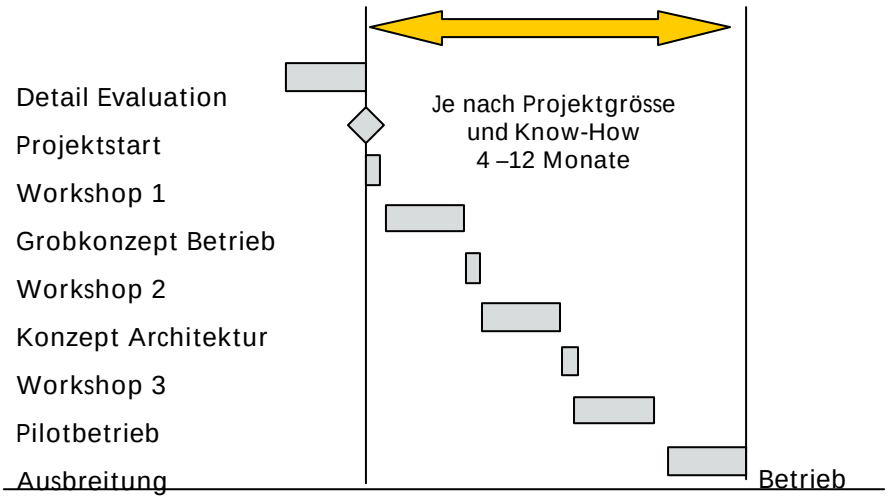
48

Zielsetzungen

- Prozesse, d.h. Definition der Prozesse um eine PKI/SCI zu betreiben (z.B. Registrierung von Benutzern, Ausstellen von Zertifikaten/Karten, Ersatz von Karten, PIN Rücksetzung).
- Architektur , d.h. welche Komponenten werden benötigt, um eine PKI/SCI zu betreiben und wie funktionieren diese Komponenten zusammen (Schnittstellen, Informationsfluss).
- Integration
  - mit Applikationen (z.B. Windows 2000 Logon)
  - In bestehende Prozesse/Abläufe (Zutritt/Berechtigung)
  - In bestehende Architekturen/Komponenten (z.B. Active Directory)

49

Zeitplan



50

Agenda

- Einleitung
- Einsatz
- Technik
- Interoperabilität
- Markt
- Wirtschaftlichkeit
- Projektorganisation
- **Rechtslage**

51

Neues D-Signaturgesetz nach EU-Recht, 22. 5. 01

Inkraft seit 22. Mai 2001 mit Unterscheidung von

- Stufe 1: dig. Signaturen zur Authentifizierung, ohne besondere Anforderungen
- Stufe 2: fortschrittliche dig. Signatur
  eindeutige Identifizierung des Inhaber des Signaturschlüssel
- Stufe 3: qualifizierte dig. Signaturen mit qualifiziertem Zertifikat und Smartcard
  (Zertifikate durch akkreditierte Trust Center.
  Nur diese Stufe entfaltet unmittelbare Rechtswirkung und werden von den Mitgliedsstaaten der handschriftlichen Unterschrift gleichgestellt)

52

CH Bundesgesetz über die elektronische Signatur

Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

Vernehmlassungsvorlage

Fahrplan

17. Januar 2001	Start Vernehmlassung
Mai 2001	Ende Vernehmlassung
Herbst 2001	Parlament
1. Quartal 2002	Umsetzung

Ablösung der Zertifizierungsdiensteverordnung;ZertDV; SR 784.103 (2009)
in Kraft seit 1. Mai 2000

53

Schleppende Akkreditierung

- Akkreditierte Trust Center in Deutschland
  - Telecom/Telesec
  - Deutsche Post/Sign Trust
- Akkreditierte Trust Center in Schweiz
  - Keines
- KPMG als 1. Schweizer Akkreditierungsstelle
  - Durch **metas** – Bundesamt für Metrologie und Akkreditierung, vormals Eidgenössisches Amt für Messwesen (EAM)

54

Schlusswort

- Für sehr viele Probleme (Vertrauen, Sicherheit, Schlüssel-Management) eine technisch gute Lösung
- Es ist heute verfügbar
- PKI ist ein komplexes Projekt mit Management Attention
- Es ist eine Infrastruktur und kein Allheilmittel für Security.
- Eine Killerapplikation ermöglicht der PKI den Durchbruch

55

.iTSEC

manage your secrets

Vielen Dank für Interesse!

Daniel A. Pfenninger
Tf: 01/ 404 82 55
www.it-sec.com
daniel.pfenninger@it-sec.com