

Organisatorische Aspekte in PKI-Projekten

Elena Jent-Dellis
PayNet AG

Dr. Marcus Holthaus
IMSEC GmbH

28. März 2001

FGSec PKI

Inhalt

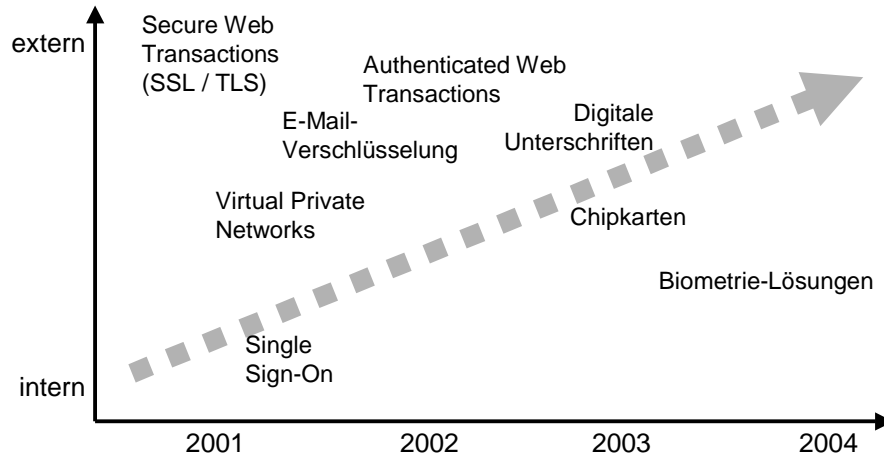
- PKI als Entwicklung
- Organisatorische Aspekte von
 - Secure Web Transactions
 - Virtual Private Networks
 - E-Mail-Verschlüsselung
 - Digitale Signaturen
- PKI-Rahmenorganisation
- Wieviele Zertifikate / Schlüsselpaare
- Verschlüsselte Malware
- Authenticated Services
 - Notwendige Dienstleistungen
 - Registrierungsprozess
 - Single Sign-On
 - Chipkarten
- Key Management
- PKI-Projekte:
 - Aufwand
 - Realitäten
 - Initialisierung
 - Implementation
- Now or never?
- Erwartete Verbreitung

28. März 2001

2

FGSec PKI

PKI: Akzeptanz heute und morgen



28. März 2001

3

FGSec PKI

PKI heute: Technologien im Vergleich

- Alle Technologien sind heute verfügbar!
- Organisatorische Anforderungen steigen durch Einbezug externer Parteien und Beziehung zum inhaltlichen Geschäft
- „Relativ“ einfach:
 - SSL / TLS
 - VPN*
 - SSO mit Speicherkarten*
 - Biometrielösungen*
- „Mittelschwer“
 - E-Mail-Verschlüsselung
 - PKI-Chipkartenverwendung
 - Intern gültige Digitale Signaturen (Closed User Groups)*
- Relativ schwierig:
 - Authenticated Web Transactions
 - Extern gültige Digitale Signaturen

* wird hier nicht näher ausgeführt, da keine PKI-spezifischen Technologien, sondern im erweiterten Umfeld

28. März 2001

4

FGSec PKI

Secure Web Transactions (SSL / TLS)



- Technisch-Organisatorisch auf Anbieterseite:
 - Protokoll: Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS)
 - Generieren eines Schlüsselpaars und Lösen eines Server-Zertifikats
 - Installation in entsprechend vorbereiteten Server, Aktivierung
 - Sicherung des Server-Betriebs mit Mitteln der Informatik-Sicherheit (Verfügbarkeit, Schutz vor Integritätsverlust des Zertifikats etc.)
 - Minimales Key Management:
 - Sicherstellung der Gültigkeit des Zertifikats (läuft nach bestimmter Periode ab), Ersatz und Austausch
 - Verwendung parallel gültiger Zertifikate?

28. März 2001

5

FGSec PKI

Secure Web Transactions (2)



- Vertrauen
 - Server identifiziert sich und kann vom Kunden authentisiert werden
 - Datenverkehr ist verschlüsselt
 - Organisatorisch auf Kundenseite:
 - Kunde muss Aussteller des Server-Zertifikates akzeptieren
 - Kunde muss Server-Zertifikat prüfen (Authentisierung)
- ⇒ Risiko für die Transaktionen i.d.R. beim Anbieter
⇒ blindes Vertrauen in die Identität des Kunden

28. März 2001

6

FGSec PKI

E-Mail-Verschlüsselung (1)

- Wahl / Anerkennung einer Zertifizierungsstelle
-> Frage des Trust Levels
- Regelungen, wann E-Mails zu verschlüsseln sind
 - Z.B. auf Basis von Klassifizierungsprozess
 - Immer, wenn mit dem Partner möglich
- Gesamten Lebenszyklus einer E-Mail betrachten!
- Eintritt eines Mitarbeiters:
 - Kein vertrauliche E-Mail vor Verfügbarkeit des Zertifikats
- Verlust des privaten Schlüssels: Recovery-Prozess
 - Zentrales Key-Management und / oder
 - Mit-Verschlüsselung für „Nachschlüssel“ und / oder
 - Rollenbasierte Verschlüsselung

28. März 2001

7

FGSec PKI

E-Mail-Verschlüsselung (2)

- Revokation des Zertifikats
 - Bei Kompromittierung des Schlüssels oder
 - bei Austritt des Mitarbeiters
- Bei Archivierungsnotwendigkeit:
 - Sicherstellung der mittel- und langfristige Verfügbarkeit des privaten Schlüssels zur Entschlüsselung der Korrespondenz dieses Mitarbeiters - oder
 - Unverschlüsselte Archivierung und / oder
 - Re-Encryption mit allgemeinem Firmenschlüssel
- Nebenwirkung: Verschlüsselte Malware

28. März 2001

8

FGSec PKI

PKI mit Chipkarten

- Logistik der Verbreitung und verteilten Installation der Kartenlesegeräte
- Unterschiedliche Kartenschnittstellen (nicht jeder Leser liest jede Karte und umgekehrt)
- Ausstellungsprozess: Personalisierung
 - Intern vs. extern
 - Frequenz
 - Kurzfristige Nicht-Verfügbarkeit einer Karte („zu Hause vergessen“)
- Verlust von Karten -> Sperrungs- und Neuausstellungsprozesse
- Kurzfristige nicht-Kontrolle über Karten kann genügen zur Kompromittierung

28. März 2001

9

FGSec PKI

Extern gültige digitale Signaturen

- Allgemein: Wenn bestehendes organisatorisches Wissen konsequent adaptiert wird, entstehen keine aussergewöhnlichen rechtlich verbindlichen Verpflichtungen
 - Prokura, Freigabe, Disclaimers...-> Organisationshandbuch
- Haftung für Missbrauch von Signaturen
 - Beweisumkehr
 - Widerruf
- Achtung vor
 - Inkompetenz
 - Kompetenzüberschreitung
 - Betrug

28. März 2001

10

FGSec PKI

Digitale Signaturen: Vision

- E-Mail-Client als „verlängerter Arm“ des Nutzers
 - Vertrauenswürdige Devices
 - Mobile / handheld Systeme
 - Öffentliche Stationen
- Verschiedene Zertifikate für verschiedene Rollen (Prokura als temporäres Anhängsel zur Grundzertifizierung)
- Mehrere Schlüsselpaare
 - Vertraulichkeit, Signierung, rollenbasiert, etc.

28. März 2001

11

FGSec PKI

Authenticated Web Transactions

- Voraussetzungen: Vgl. Secure Transactions
- Zusätzlich: Authentisierung von Client-System (=dahinterliegende Identität) durch den Server mittels Zertifikat
- Abweisung von Transaktionen bei Zweifeln an Echtheit und Gültigkeit des Zertifikats
- Registrierung von Externen (Kunden, Partnern)
 - Selbst zertifizieren
 - „Einkaufen“ von Zertifikaten einer spezifischen Klasse bei einer öffentlich anerkannten CA

28. März 2001

12

FGSec PKI

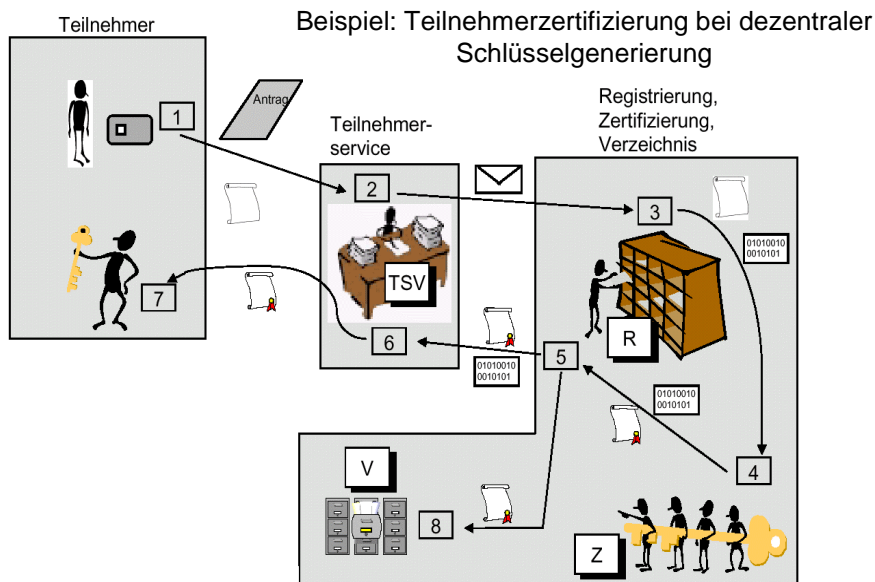
PKI-Rahmenorganisation

- Zertifizierung
 - Leitungsorganisation
 - Organisator Registrierung
 - Technologiemanager
 - Zertifizierer
 - Personalisierer
- Registrator
- Verzeichnispfleger
- Teilnehmerdienste
 - Hotline / Service
 - Schulung
- Übergeordnete / parallele Rollen
 - Sicherheitsbeauftragter
 - Revision
 - Datenschutzbeauftragter
 - Technischer Administrator
 - Krisenmanagement-Team

28. März 2001

13

FGSec PKI



• (aus: SPHINX PKI Organisationshandbuch V3.8, Nov. 1999, S. 45)

28. März 2001

14

FGSec PKI

Instanzen, Rollen, Stellen: Make or buy?

Dienst	Make	Buy
Teilnehmerservice	+++	+
Registrierung	+++	++
Zertifizierung	+	+++
Verzeichnis	+	+++
Sperrdienst	+	+++
Namensraumvergabe	(+)	+++

28. März 2001

15

FGSec PKI

Registrierungsprozess

- RA: Bezeichnete Stelle innerhalb der Unternehmung
 - Mit Personalkompetenz
 - Mit Authentisierungsmöglichkeit
- Möglicherweise separierbare Funktionen
 - Ausstellung des Zertifikats
 - Personalisierung von Zertifikatsspeichern (Chipkarten etc.)
- Registrierungs- und Revokationsprozess muss in normalen Personalmanagement-Prozess integriert werden

28. März 2001

16

FGSec PKI

Key Management

Key-Management ist eine Kernkompetenz der PKI-Beherrschung

- Zugriffsregelungen
- Archivierung der Schlüssel
- Schlüssel-Ersatz und -Austausch
- Über die Nutzungsdauer entstehen VIELE Schlüssel
- Schlüsseltypen
 - Server
 - Code
 - Personen / Mitarbeiter
 - Rollen
 - Partner (nur public key)
 - Tests
 - Besondere Anwendungen und Prozesse
 - Symmetrische
- Anwendung
 - Web (1/2seitig)
 - VPN
 - Vertr. E-Mail
 - Signaturen
 - Besondere Anwendungen und Prozesse
- Schlüsselgültigkeit
 - (Beantragt)
 - Gültig
 - Abgelaufen
 - Revoziert
 - Suspendiert

28. März 2001

17

FGSec PKI



PKI-Projekte (1)

- Kombiniertes Informatik-Organisation-Projekt
- Grundsätzlicher Ablauf analog zu herkömmlichen Projekten (Phasen, Meilensteine, etc.)
- Zum Teil komplexe Technologien
- Hohe Qualitätsanforderungen
- Geschäftskritische rechtliche Fragestellungen

28. März 2001

18

FGSec PKI

PKI-Projekte (2)

- Empfehlungen zum Vorgehen
 - Auswahl eines einzelnen, gut separierbaren Business-Cases
 - Start direkt mit Zertifikaten eines externen Ausstellers
- Motivation offen legen
- Verständnis, Vertrauen, Erfahrung entwickeln sich langsam
- PKIs benötigen sichere Grundlage
 - Traditional vs. Security Engineering
 - Client als Identitätsträger des Benutzers -> Vertrauenswürdiges Device?
- Prinzipielle „online“-Philosophie

28. März 2001

19

FGSec PKI

PKI-Projekte (3)

- Erwarten Sie Probleme in folgenden Bereichen
 - Unterschiedlich qualifiziertes und teures Personal
 - Inkonsistente und unzuverlässige Produkte, Inkompatibilitäten, Versteckte Mängel
 - Intransparenzen und Unmöglichkeit des Nachvollzugs einzelner Vorgänge, d.h. Nichtverfügbarkeit notwendiger Qualitätssicherungswerkzeuge
 - Performance-Probleme
 - Skalierungs-Problematiken
- Echtes Vertrauen beruht weiterhin auf persönlicher Erfahrung und Empfehlung

28. März 2001

20

FGSec PKI

PKI: Now or never?

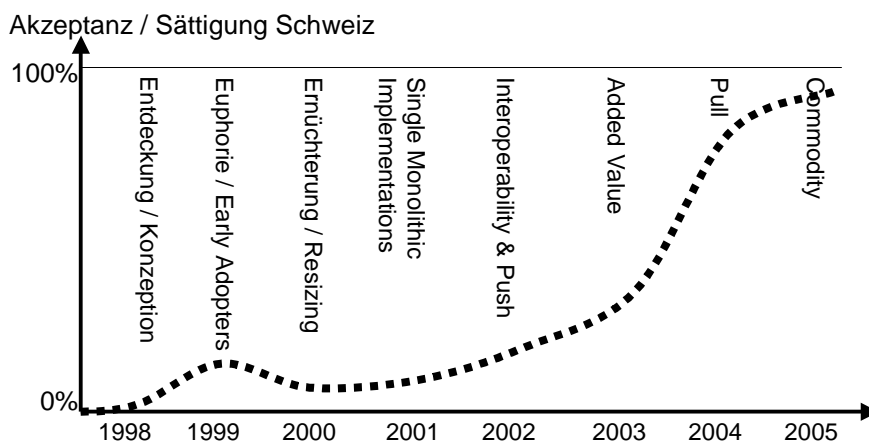
- Jetzt realisieren (intern & extern):
 - Jeder mit Marktinteresse im Fernabsatz
 - Grosse Finanzdienstleister
 - Mittlere bis grosse Unternehmen
- Genau evaluieren und probieren:
 - Kleinere Finanzdienstleister
 - Juristische Dienstleister
 - Öffentliche Organisationen mit starkem Publikumsverkehr
 - Insourcer und Dienstleister mit enger Kundenbindung
 - Unternehmen mit vertraulichem E-Mail-Verkehr
- Evaluieren:
 - Mittlere Unternehmen
 - Unternehmen mit EDI, Fernabsatz, starkem Extranet
 - Unternehmen mit WANs
- Abwarten:
 - Private
 - Kleine Unternehmen
- Never? No!
PKI kommt definitiv.

28. März 2001

21

FGSec PKI

PKI: Unsere Prognose



28. März 2001

22

FGSec PKI