



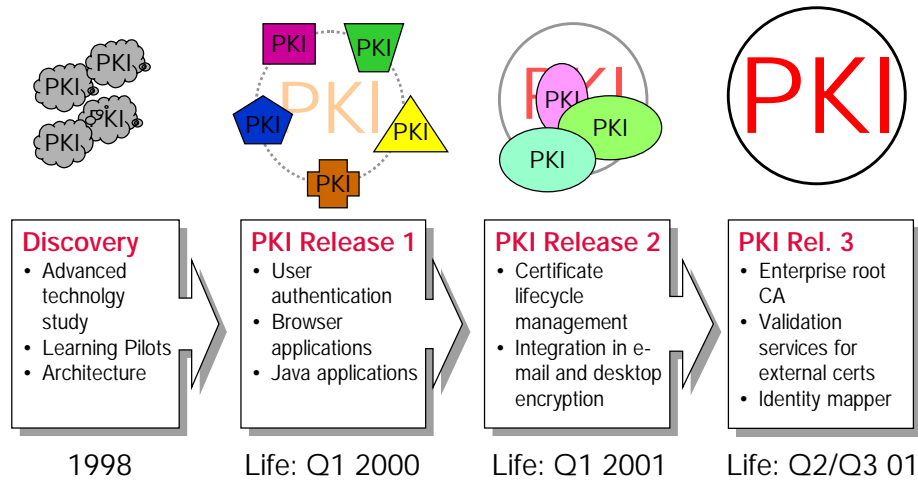
Key management is key!  
Fachtagung FGSec, 28.03.2001

Martin Achermann  
Leiter IT Security Engineering

## Index

• CSFS PKI Roadmap - gestern, heute und morgen	3
• Ausgangslage mit PKI Release 1	4
• Beschränkungen von PKI Release 1	5
• Ziele des Projekts PKI Release 2	6
• Applikationsintegration mit "Full Service" PKI-Client	7
• Browser-basierende Applikationsarchitektur mit PKI	8
• Vorgehen im Projekt	9
• Challenge No. 1 – 4	10
• Fazit	16

## CSFS PKI Roadmap - gestern, heute und morgen



## Ausgangslage mit PKI Release 1

- CS Banking, CS e-Business, CS Private Banking, TaS
  - 8'000 Web-Zertifikate für Mitarbeiter
  - 45 Maschinen-Zertifikate
  - 65 Webserver-Zertifikate
  - 1'000 Test-Zertifikate (SW-Entwicklung)
- 12 produktive Browser-basierende Applikationen
  - Architektur gemäss CSFS-Applikationsframework
- 9 produktive weitere Applikationen
  - Standardsoftware (Packages)
  - Legacy-Applikationen mit massgeschneiderten PKI-Schnittstellen

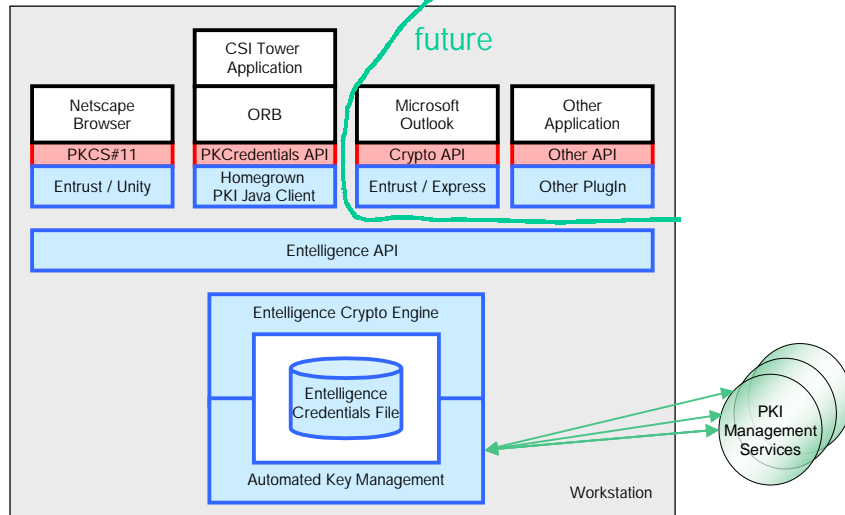
## Beschränkungen von PKI Release 1

- Fehlende Standardschnittstellen für PKI-Anwendungen
  - Middleware unterstützt(e) noch keine PKI-Schnittstelle
- Key management
  - Instabiles key generation applet führte zu undefiniertem Status während Schlüsselgenerierungsprozess
  - Zertifikatserneuerung vor Ablauf der Gültigkeitsdauer nicht technisch sichergestellt
  - Netscape Browser "verliert" CA-Zertifikat
- Verfügbarkeit CA
  - Kein Monitoring
  - Defunct Process

## Ziele des Projekts PKI Release 2

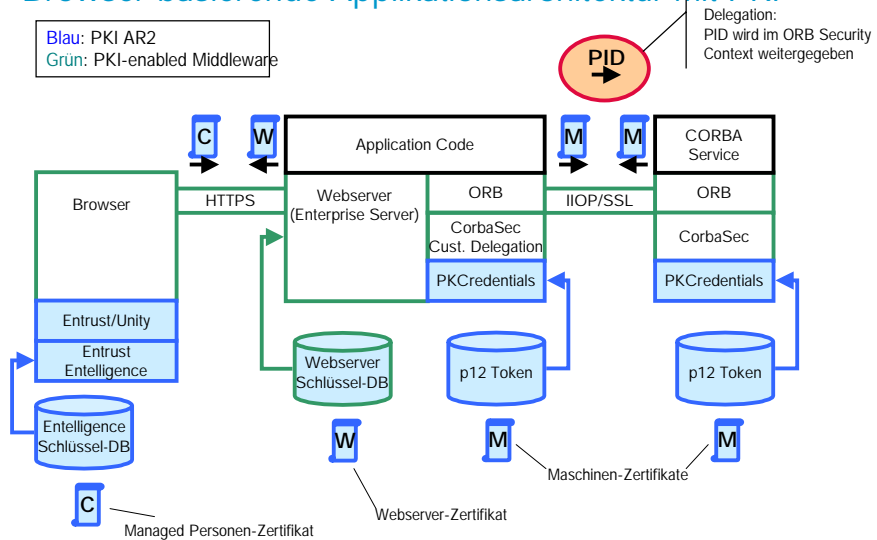
- Verwaltete Zertifikate auf dem Client
  - Key recovery, key renewal, DN changes, etc.
- Vereinfachung / Stabilisierung der Zertifikatsgenerierung
  - Einsatz von Standard PKI-Software
- Verwaltung und Prüfen von Sperrlisten (CRL)
- Bereitstellung Standard PKI Client Interface für Applikationen
  - S/MIME, PKCS#11, etc.
- Verbesserter Schutz der Credentials
  - Die Schlüssel sind durch ein PSE (Personal Security Environment) besser geschützt
  - Basis für den Einsatz von Smartcards geschaffen

## Applikationsintegration mit "Full Service" PKI-Client



## Browser-basierende Applikationsarchitektur mit PKI

Blau: PKI AR2  
Grün: PKI-enabled Middleware



## Vorgehen im Projekt

- Divide et impera!
  - Team PKI Server
  - Team PKI Client
  - Team Schulung / Dokumentation
  - Team Prozesse
  - Quality Assurance
  - Einführungscoordination
- Intensive Kommunikation
  - Infoveranstaltung und individuelle Ausbildung für Supporter
  - Ausbildung Sicherheitsadministration
  - etc.

## Challenge No. 1: Upgrade CA

- Aufgabe: Upgrade Entrust Authority auf Release 5.0
- Probleme:
  - Directory Interoperabilität
    - LDAP Version 2 und 3, Probleme mit Schema
  - Directory Design
    - Architektur des DIT (directory information tree)
    - Separate Trees für Zertifikate des Projekts PKI Release 2 und Secure E-Mail Pilotprojekt notwendig
- Lessons learned
  - Nur unterstützte Konfigurationen nutzen
  - Dediziertes Directory (DIT oder DIB) für PKI erforderlich

## Challenge No. 2: RA-Prozesse

- Aufgabe: Definition und Implementierung der RA-Prozesse
- Probleme:
  - Zeitaufwändig
  - „Sicherheitskultur“ der dezentralen RA-Personen muss entwickelt werden
- Lessons learned
  - Organisation und Prozessdesign absorbieren signifikante Anteile des Budgets in einem PKI Projekt
  - Ausbildung der RA-Personen ist essentiell

## Challenge No. 3: Low-impact Softwareverteilung

- Aufgabe: Konzipierung der Softwareverteilung für 25'000 PC
  - minimale Auswirkungen auf den Benutzer
  - robuste, fehlertolerante Installation (Support!)
- Probleme:
  - Installationsprozedur PKI Client
    - Unterstützung für PKI user und Non-PKI user erforderlich
  - Aktivierung PKI Client zum richtigen Zeitpunkt für enrolment Prozess (Transition Non-PKI user zum PKI user)
  - Anpassung PKI-Komponenten der Browser
- Lessons learned
  - Der Browser ist eine strategische Applikation!

## Challenge No. 4: Migration Release 1 nach Release 2

- Aufgabe: Migration bestehender PKI Release 1 Benutzer
  - erneute Registration bestehender Rel. 1 Benutzer vermeiden
  - alle Benutzer sind auf dem selben PKI Release (Release 2)
- Probleme:
  - Modaler Dialog zum Zeitpunkt der Softwareinstallation
    - Benutzer kann Zeitpunkt der Migration nicht wählen
  - Einführung sicherer Passwörter
    - Komponieren und Einprägen von sicheren Passwörtern ist anspruchsvoll
- Lessons learned
  - Benutzerakzeptanz frühzeitig testen

## Passwort-Reset "Selbstbedienungsprozess"

### Passwort-Recovery

- autom. Neugenerierung anhand von UserId, Single Sign-On Passwort und SecurID-Nummer
- Passwort kann sofort neu gewählt werden
- Kein Umweg über Support mehr nötig

### ... more lessons learned!

- Gestaffelte Softwareverteilung mit Pilotierung
  - Dank Pilotierung der Softwareverteilung konnte während des Roll-Out des PKI Clients ein gravierender Fehler im Installationspaket entdeckt werden.
- Pilotierung Secure E-Mail
  - Dank der Pilotierung von Secure E-Mail (Learning Pilot) konnten frühzeitig Fehler im PKI Client entdeckt werden.
  - Auswirkungen zu diesem Zeitpunkt gering, da erst ca. 30 Benutzer aufgeschaltet.

### Fazit

- Key management is key!
  - Ein effizientes key management ist eine notwendige Voraussetzung für die Nutzung von PKI im Unternehmen.
  - Ein grosser Teil der PKI-Supportfälle kann durch ein robustes key management verhindert werden.
- Testen, testen und noch einmal testen!
  - Benutzerakzeptanz
  - Integrationstest
  - Produktionstest
  - Pilotierung!



Besten Dank für Ihre Aufmerksamkeit!

Key management is key!  
Fachtagung FGSec, 28.03.2001

Martin Achermann (KTXS)  
Leiter IT Security Engineering