T-Systems Solutions for Research.

DFN Sicherheits-Workshop, PKI Services auf Basis der DFN PKI

18.03.09; Hamburg; Frank Fiedler; T-Systems SfR GmbH

T · · Systems

PKI-Services auf Basis der DFN PKI

Inhalt

- Hintergrund und Herausforderung
- Regelungen /Sicherheitsmaßnahmen der DLR PKI
- Technische Lösung
  - Komponenten
  - RA Prozesse mit Softwareunterstützung
  - Zertifikats Provisionierung
  - Nutzenbetrachtung
- Organisatorische Prozesse am Beispiel von Festplattenverschlüsselung
- Ausblick

PKI-Services auf Basis der DFN PKI

Hintergrund und Herausforderungen

- Wachsender Bedarf nach PKI-Services beim DLR
  - Sichere interne und unternehmensübergreifende Kommunikation
    - Email-Signatur / Email-Verschlüsslung
  - Elektronische Unterschrift
    - Dokumentensignatur
  - Festplattenverschlüsselung
- Projekt zur Einführung unter Beteiligung von
  - DLR
  - T-Systems SfR
  - DFN/DFN-CERT
- Aufbau eines PKI Testlab s

PKI-Services auf Basis der DFN PKI

Hintergrund und Herausforderungen

- Rollout von Benutzerzertifikaten ausschließlich auf kryptografischen Geräten
- Gewährleistung der Sicherheit von Zertifikatsinhalten (Welche Informationen sollen/dürfen veröffentlicht werden?)
- Verbindung von Festplattenverschlüsselung mit zertifikatsbasierter Prebootauthentifizierung (Mobilität?)
- Wiederherstellbarkeit von Verschlüsselungsschlüsseln zur Vermeidung von Datenverlusten
- Anbindung an das DLR Identity Management (Corporate Metadirectory, AD)
- Softwaregestützte RA-Prozesse (Vermeidung von fehlerhaften Zertifikatsinhalten, CPS Konformität)
- Zukunftssicherheit (Erweiterbarkeit ohne erneuten Zertifikatsrollout)

PKI-Services auf Basis der DFN PKI

Regelungen / Sicherheitsmaßnahmen der DLR PKI

- Benutzerzertifikate auf eToken 64k USB der Fa. Aladdin (Token)
- Elektronische Beantragung von Zertifikaten über SfR Auftragsmanagementsystem
- Ausstellung nur für Personen mit
  - SAP Personalnummer
  - Active Directory Account
  - DLR Emailadresse
- 3 Zertifikate pro Benutzer / Token
  - Authentifizierungszertifikat
  - Signaturzertifikat
  - Verschlüsselungszertifikat

PKI-Services auf Basis der DFN PKI

Regelungen / Sicherheitsmaßnahmen der DLR PKI

Zertifikatstyp	Einsatzzweck	Merkmale
Authentifizierungs-zertifikat	• SmartCard Logon • Prebootauthentifizierung für Festplattenverschlüsselung • Clientauthentifizierung an Webservices	• Veröffentlichung: **nein** • Schlüsselgenerierung: **auf dem Token** • Sensible Daten: **UPN (User Principal Name)** • Schlüsselbackup: **nein**
Signaturzertifikat	• Email-Signatur • Dokumentensignatur	• Veröffentlichung: **nein** • Schlüsselgenerierung: **auf dem Token** • Sensible Daten: **nein** • Schlüsselbackup: **nein**
Verschlüsselungs-zertifikat	• Email-Verschlüsselung • Dokumentenverschlüsselung • Ordner/Dateiverschlüsselung	• Veröffentlichung: **ja** • Schlüsselgenerierung: **in der RA-Middleware** • Sensible Daten: **nein** • Schlüsselbackup: **ja**

PKI-Services auf Basis der DFN PKI

Regelungen / Sicherheitsmaßnahmen der DLR PKI

- Schlüsselhinterlegung und –wiederherstellung
  - Nur Verschlüsselungszertifikat/schlüssel
  - Verschlüsselung/Entschlüsselung der Verschlüsselungsschlüssel mittels Keybackup Rollenzertifikat
  - Privater Schlüssel des Keybackup-Rollenzertifikats ausschließlich auf Token
  - 4 Augen-Prinzip bei Wiederherstellung
    - Nutzung der PIN des Keybackup-Tokens
    - Kenntnis der PIN verteilt auf RA-Mitarbeiter und PIN-Geber
- Ereignisse für Schlüsselwiederherstellung
  - Tokenverlust oder –defekt
  - Sicherstellung von Daten, veranlasst durch Datenschutzbeauftragten

PKI-Services auf Basis der DFN PKI

Regelungen / Sicherheitsmaßnahmen der DLR PKI

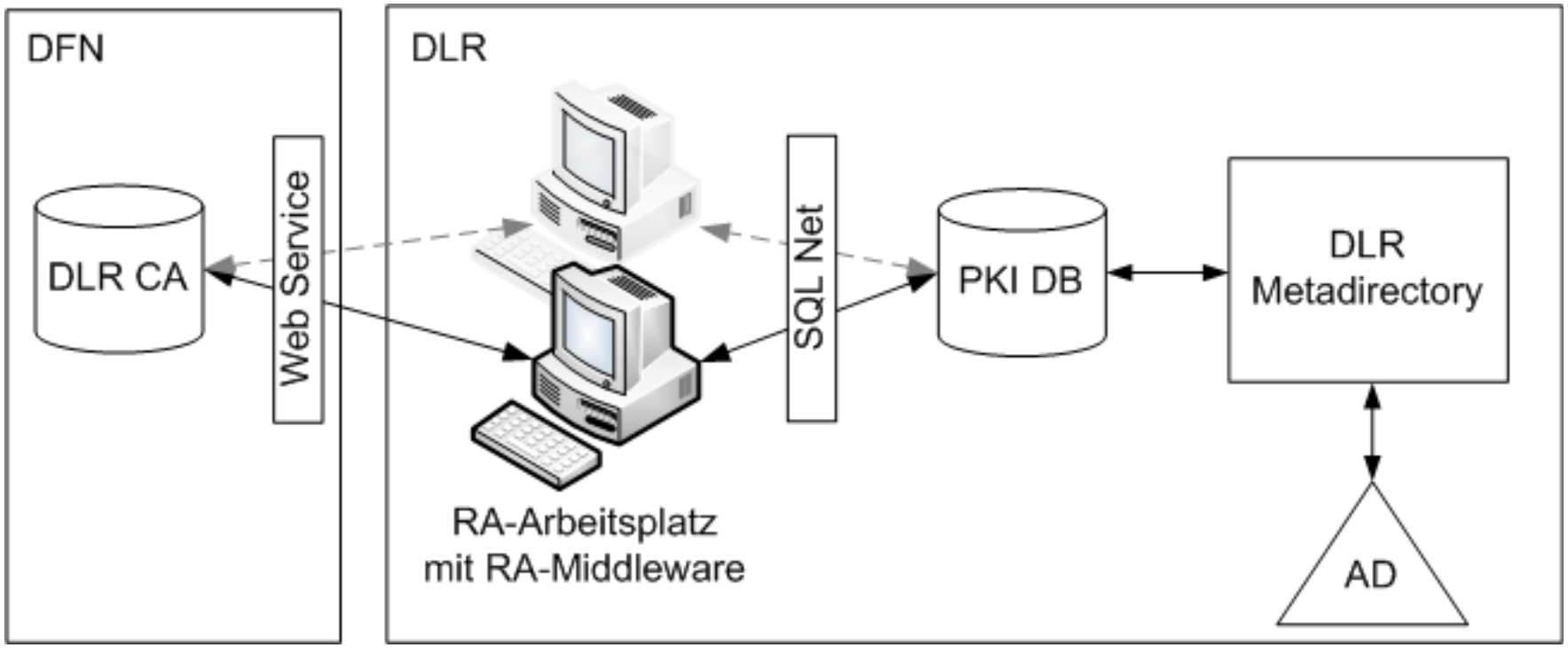
- Weitere Sicherheitsmaßnahmen
  - PIN- Briefe
  - Zertifikatsinformation zur Überprüfung der Authentizität des Tokens bei Postversand
  - Token/PIN- Briefversand zeitversetzt
  - Zeitlimit für Empfangsbestätigung Token und PIN-Brief
  - RA-Logbuch
  - RA-ID s: Zuweisung von Rechten entsprechend des RA-Zertifikats
  - Passwort Policy für PIN Nummern (zentraler Rollout von vorkonfigurierter Clientsoftware)

PKI-Services auf Basis der DFN PKI

- Technische Lösung
  - Komponenten
  - RA Prozesse mit Softwareunterstützung
  - Zertifikats Provisionierung
  - Nutzenbetrachtung

PKI-Services auf Basis der DFN PKI

Komponenten



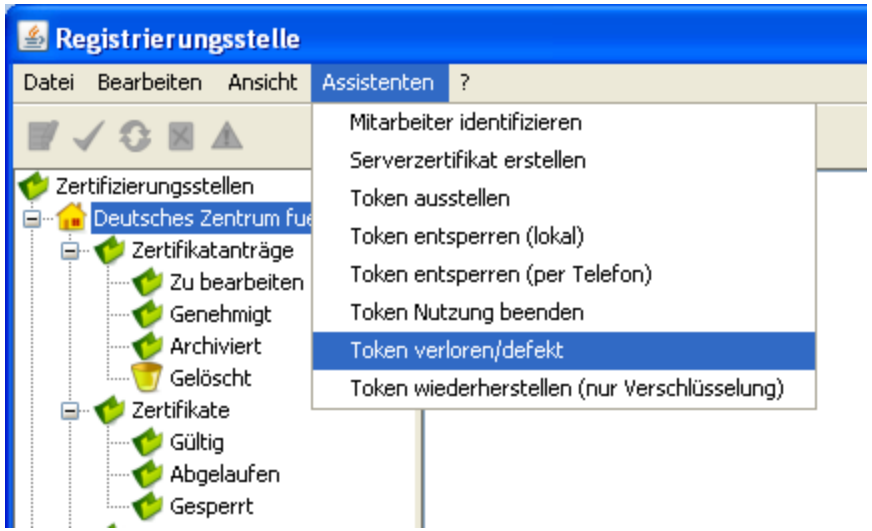
PKI-Services auf Basis der DFN PKI

RA-Prozesse mit Softwareunterstützung

- Identifizierung von Mitarbeitern
- Ausstellung von Zertifikaten auf Tokens
- Entsperrung von Tokens (PIN-Reset)
- Neuausstellung von Zertifikaten im Fall verlorener oder defekter Tokens
- Erstellung eines Notfalltokens zur Entschlüsselung von Daten
- Beenden der Nutzung von Zertifikaten

→ RA-Middleware des DFN / Assistenten

→ Individuelles Assistentenmenü für jede RA-ID



PKI-Services auf Basis der DFN PKI

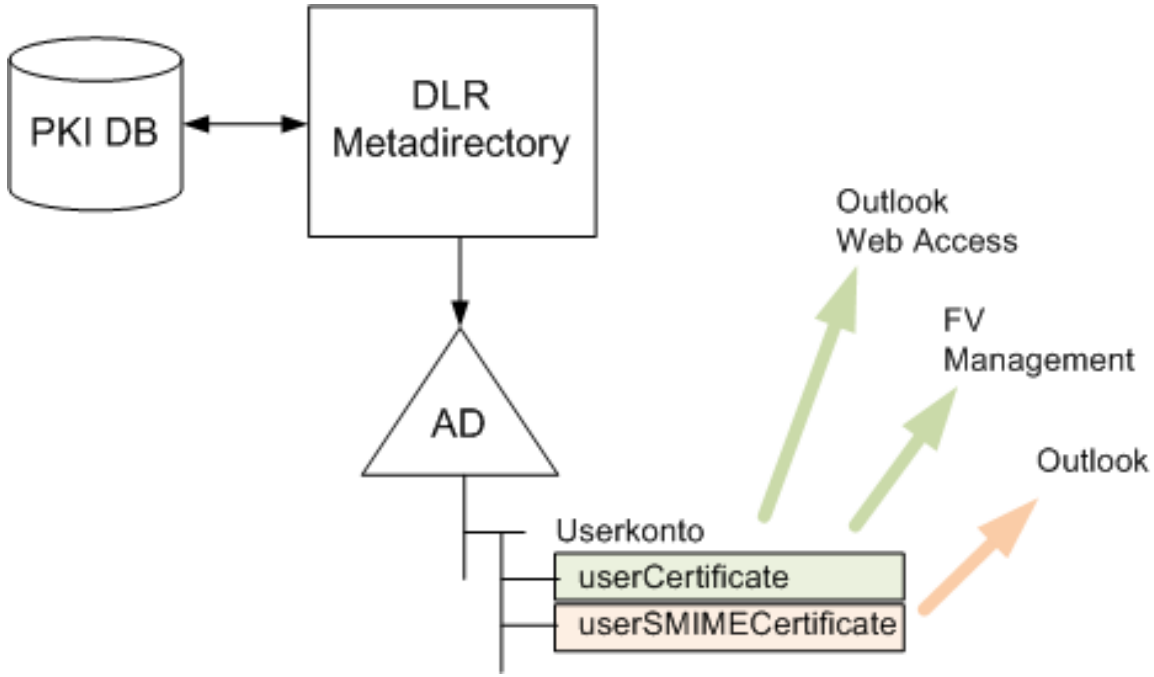
RA-Prozesse mit Softwareunterstützung am Beispiel Tokenverlust/defekt

- Tokeninitialisierung
- Generierung und Speicherung einer Admin-PIN in der zentralen PKI Datenbank
- Schlüsselpaargenerierung
- Versand der Zertifikatsrequests (Auth, Sign, Encr) an das CA-System beim DFN
- Versand der Sperranträge und Genehmigung der Sperranträge für die (alten) Zertifikate
- Zertifikatsausstellung durch die CA und Übermittlung der Zertifikate an die RA-Middleware
- Verschlüsselung und Speicherung des (neuen) Verschlüsselungszertifikats in der PKI -DB
- Entschlüsselung aller hinterlegten Verschlüsselungszertifikate des Benutzers
- Speicherung der neuen Zertifikate, aller wiederhergestellten Verschlüsselungszertifikate sowie aller CA-Zertifikate der Zertifizierungshierarchie auf dem Token
- Ausdruck von PIN-Brief, Zertifikatsinformation und Empfangsbestätigung
- Löschung aller gesperrten Authentifizierungs- und Signaturzertifikate aus der PKI-DB

PKI-Services auf Basis der DFN PKI

Zertifikats Provisionierung

- Provionierung von
  - Authentifizierungs-Zertifikat für Festplattenverschlüs-selung
  - Verschlüsselungs-zertifikat für Globale Adressliste (Exchange)
- Täglicher Synclauf



PKI-Services auf Basis der DFN PKI

Nutzenbetrachtung

- Sicherheit durch 2 Faktor Authentifizierung
- Vermeidung von Fehlern bei Zertifikatsinhalten
- Angepasstes Sicherheitsniveau / angepasste Verwendungszwecke von Zertifikaten
- Zertifikatsausstellung technisch nur für Mitarbeiter möglich, die die Kriterien erfüllen
  - SAP-Personalnummer, AD-Account, Email-Adresse
  - Identifizierung liegt vor
- kritische Ereignisse wie Tokenverlust, PIN-Vergessen werden durch Supportprozesse „entschärft“
- In die existierende Maillösung integriertes zentrales Verzeichnis für Verschlüsselungszertifikate

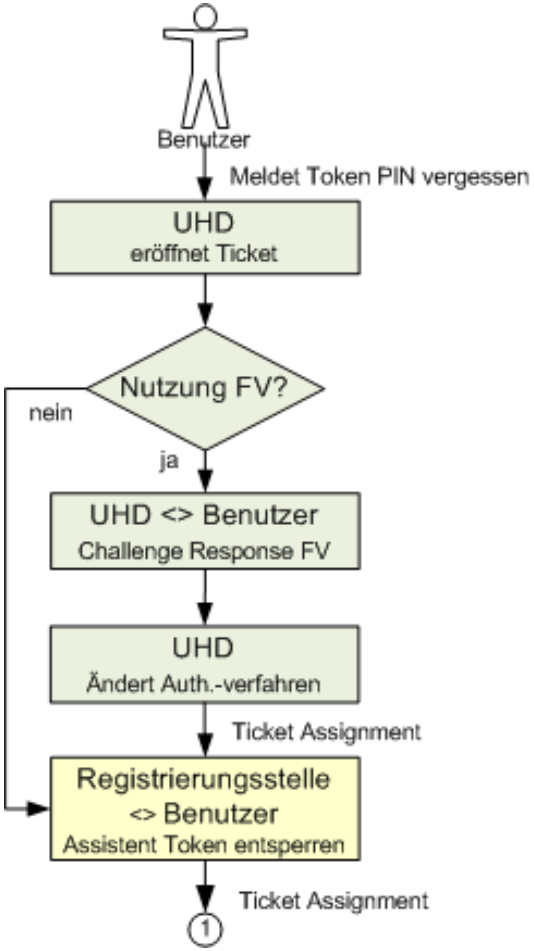
PKI-Services auf Basis der DFN PKI

Organisationsprozesse am Beispiel Festplattenverschlüsselung

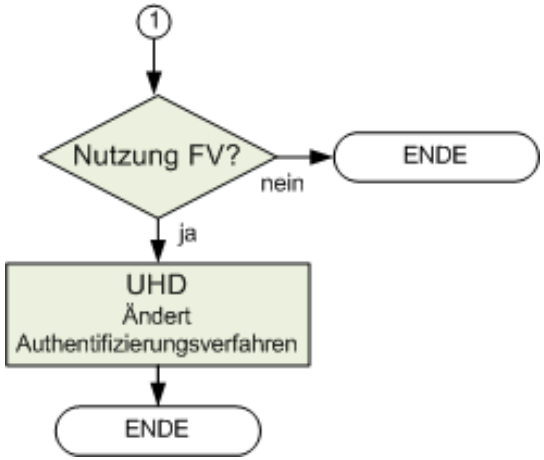
- Festplattenverschlüsselungs Service für Notebooks
- Basis: McAfee Endpoint Encryption
- PKI- Einsatz zur zertifikatsbasierten Prebootauthentifizierung
- Zentrales Managementsystem zur
  - Zertifikatssynchronisation aus dem AD
  - Vorgabe zentraler Policies (z.B. Anmeldeverfahren)
  - Zentrales Schlüsselmanagement
  - Challenge-Response- Verfahren

PKI-Services auf Basis der DFN PKI

Organisationsprozesse am Beispiel Festplattenverschlüsselung

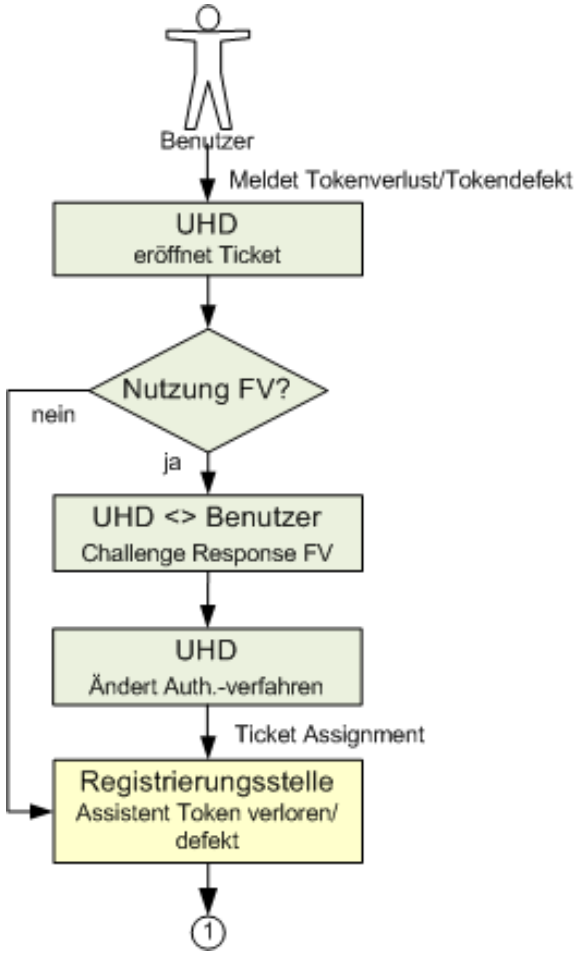


Workflow beim Ereignis
„Token PIN vergessen/ Token blockiert

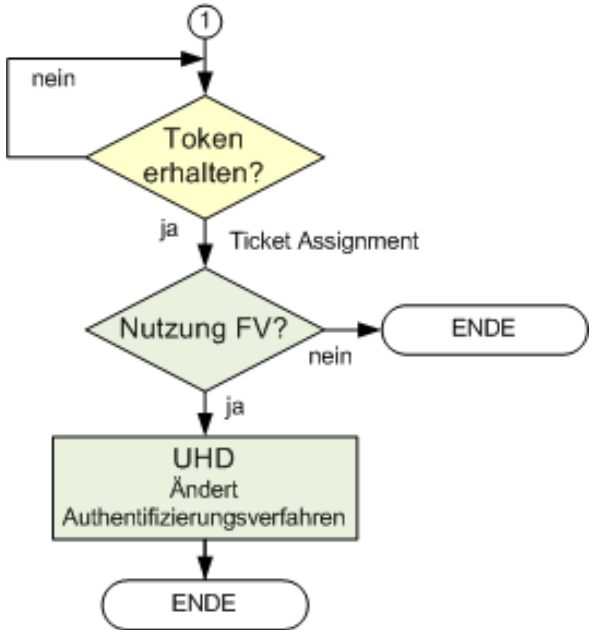


PKI-Services auf Basis der DFN PKI

Organisationsprozesse am Beispiel Festplattenverschlüsselung



Workflow beim Ereignis
„Token verloren/Token defekt“



PKI-Services auf Basis der DFN PKI
Ausblick

- In der kurz- bis mittelfristigen Planung beim Kunden DLR
  - Erweiterung der FV-Lösung für Datei und Ordnerverschlüsselung
  - Einführung SmartCard Logon
  - Zertifikatsbasierte Authentifizierung von clientless und client based SSL VPN
  - Einsatz MicroSD Cards für Windows Mobile Systeme (Emailverschlüsselung)

- In der langfristigen Planung
  - SmartCard s als ergänzendes Angebot zu Tokens
  - Gerätezertifikate für 802.1x Authentifizierung

PKI-Services auf Basis der DFN PKI
Fazit

- Deployment von PKI-Services in Unternehmen ist flächendeckend für eine Vielzahl von Einsatzzwecken möglich
- Kritische Einsatzszenarien wie Verschlüsselung lassen sich durch Technik und Organisationsprozesse beherrschen
- Die DFN PKI Angebote erlauben durch ihre Flexibilität und Innovationsfähigkeit den Aufbau individuell zugeschnittener PKI-Services bei den Anwendern

Vielen Dank für Ihre Aufmerksamkeit.