



security|zone
PLATTFORM FÜR INFORMATIONSSICHERHEIT

keyon

Next Generation Corporate PKI

- ▶ Modernes Smartcard Management
- ▶ Device- und Webserverzertifikate
- ▶ Zertifikate für mobile Devices (iPhone, etc.)
- ▶ Email Verschlüsselung
- ▶ Subordinierung von öffentlichen CAs

Praxisberichte

- ▶ **Swiss Re:** Sichere Devicezertifikate in Hardware (TPM)
- ▶ **Manor:** Zertifikate für mobile Datenerfassungsgeräte (MDE)
- ▶ **Migros-Genossenschafts-Bund:** Subordinierung öffentliche CA

Über Keyon

keyon

- Experten im Bereich IT-Sicherheit und Software Engineering

information security?

just relax.

plan
implement
enforce
control



keyon for security reasons
www.keyon.ch / info@keyon.ch

Corporate PKI • Identity & Access Management • Software Engineering • Legal Archiving • ISMS - ISO 27001

Über Keyon

keyon

Erstklassige Referenzen im Bereich PKI



Credit Suisse

SNB

Coop

Sulzer

RUAG

SIX Group

Swiss Re

MGB

USZ

Bund (ePass)

Glencore

VRSG

Manor

ZKB

ESTV (EIDI-V)

Agenda

keyon

Einführung PKI

Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)

Integriertes Token Management

Zertifikate für mobile Devices (iPhone, etc.)

Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

Einführung PKI

keyon

■ Definition Public Key Infrastructure (keyon)

Eine PKI umfasst die Hardware, Software, Personen, Prozesse, Richtlinien und Methoden, die daran beteiligt sind, auf asymmetrische Kryptographie beruhende Zertifikate zu erzeugen, zu verwalten, zu archivieren, zu verteilen und zu sperren.

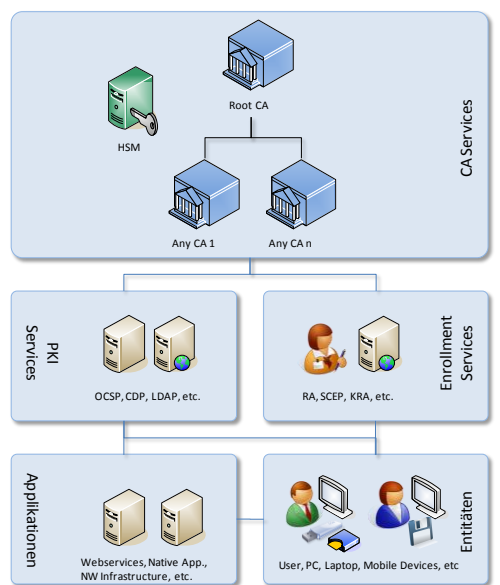
Sie werden von Zertifizierungsinstanzen (CA's) an Entitäten (Personen oder Systeme) ausgegeben, die zuvor nach einem festgelegten Prozess durch Registrierstellen (RA's) identifiziert wurden.

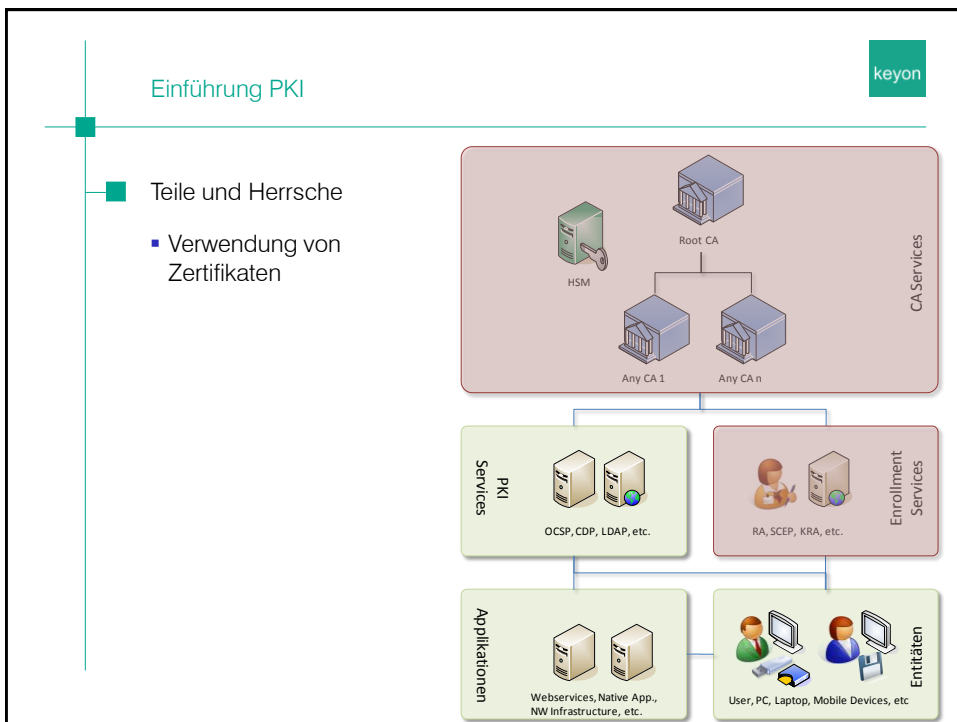
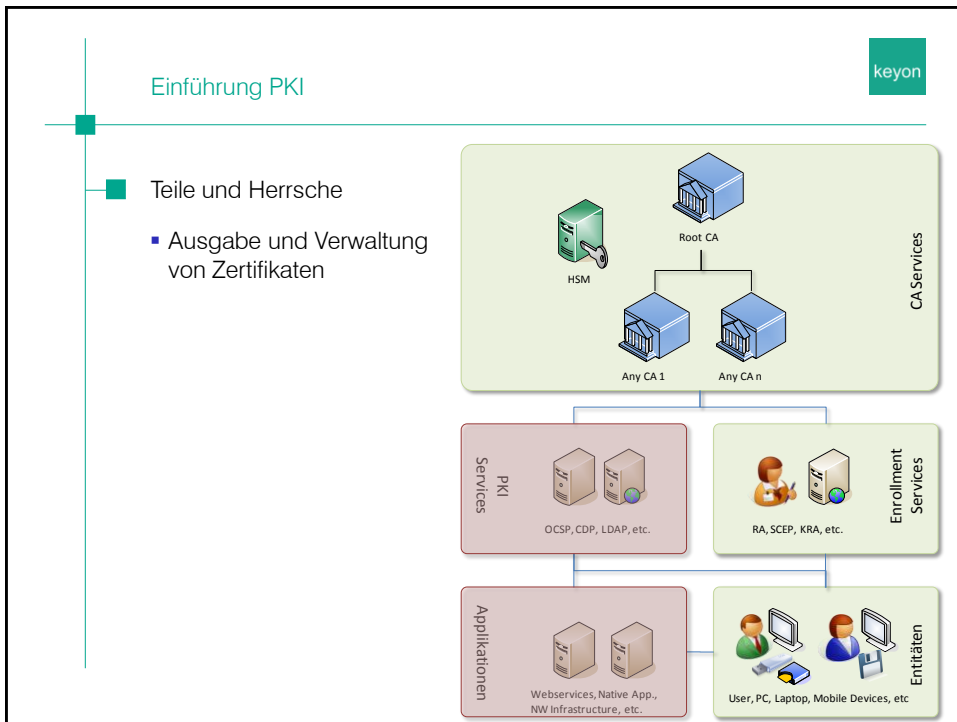
Einführung PKI

keyon

■ Teile und Herrsche

- CA Services
- PKI Services
- Enrollment Services
- Applikationen
- Entitäten





Einführung PKI

keyon

- Güte einer elektronischen Identität (Zertifikat)
 1. Registrierung: Identifizierung der Entität
 - HR Prozesse
 - Lichtbildausweis und persönliches Vorsprechen (SuissELD)
 - etc.
 2. Qualität und Sicherheit des privaten Schlüssels
 - Software-, Hardware Token
 - Schlüssellänge, Algorithmen
 3. Nutzungsbestimmungen
 - Geheim halten des PIN / Passwort
 - Verantwortungsbewusstes Verhalten (Dubiose Webseiten, Attachments, etc.)
 - Virenschutz, Firewall, physischer Schutz, etc.

Einführung PKI

keyon

- PKI Komplexitätsstufen (keyon)
 1. Microsoft Autoenrollment (Auth., Sign., Enc.)
 - Software basierte Zertifikate für Benutzer und Systeme
 - 802.1X Port Authentifizierung / VPN Authentifizierung, etc.
 2. Nicht Microsoft Autoenrollment von Systemzertifikaten (Auth., Sign.)
 - Applikationsspezifische Enrollment Services
 3. Nicht Microsoft Autoenrollment von Benutzerzertifikaten (Auth., Sign.)
 - Token Management Systeme
 4. Nicht Microsoft Autoenrollment von Benutzerzertifikaten (Auth., Sign., Enc.)
 - Schlüssel hinterlegung (key recovery)
 5. Multifunktionskarte
 - Physische Abhängigkeiten
 - Integration der Personalisierung RFID / Magnetkarten

Einführung PKI

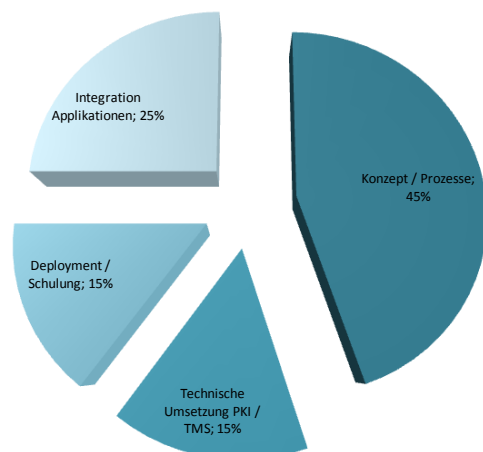
keyon

- Warum „Next Generation PKI“?
 - Breite Unterstützung von Zertifikaten in Applikationen
 - Integrierte und automatisierte Enrollment-Prozesse
 - Ausgereifte und kostengünstige Technologien (Token Management, Smartcards)
 - Rasche und pragmatische technische und organisatorische Integration
 - Hohe Sicherheit und Benutzerakzeptanz
 - Kosteneffizienz (Helpdesk, SSO, etc.)
 - Gesetzgebung / Compliance

Einführung PKI

keyon

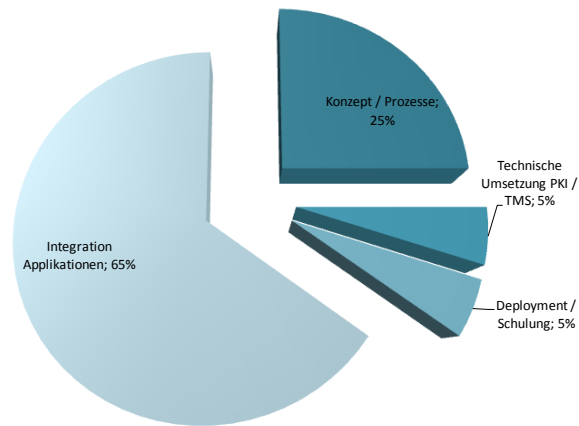
- Projektaufteilung – Initialphase



Einführung PKI

keyon

Projektaufteilung – Integration weiterer Applikationen



Agenda

keyon

Einführung PKI

Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)

Integriertes Token Management

Zertifikate für mobile Devices (iPhone, etc.)

Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

Swiss Re

keyon



Die Präsentation der Swiss Re finden Sie im File [security-zone_TPM-certificates_20100920.pdf](#)

Agenda

keyon

Einführung PKI

Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)

Integriertes Token Management

Zertifikate für mobile Devices (iPhone, etc.)

Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Ausgangslage und Ziele

- Sicherer Netzwerkzugang für mobile Datenerfassungsgeräte (802.1X)
- Effiziente Sperrung der mobilen Datenerfassungsgeräte bei Verlust
- Einfache, kostengünstige und sichere Verwaltung der Sicherheitselemente
- Dezentrale Ausgabe und Verwaltung der mobilen Datenerfassungsgeräte

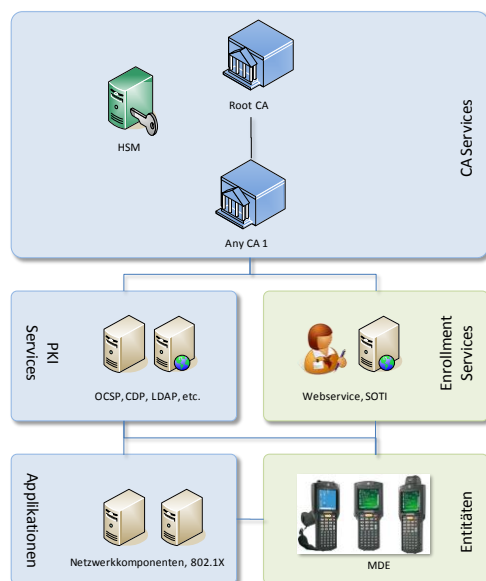


Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Design und Umsetzung

- CA Services
 - Microsoft PKI inkl. HSM
- Enrollment Services
 - Keyon / Enrollment Service
 - Keyon / RA / Helpdesk
 - SOTI MobiControl (MDE Management)
- Entitäten
 - Motorola/Symbol MC3190
- Applikationen
 - 802.1X fähige Netzwerkkomponenten
- PKI Services
 - CDP

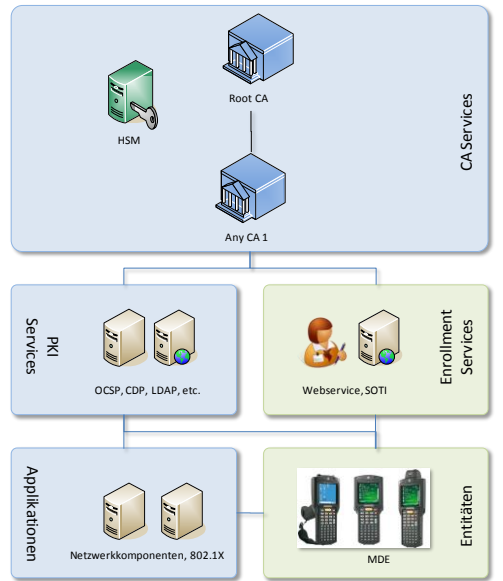


Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



■ Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passwörter / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat



Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



■ Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passwörter / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat



Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passwörter / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passwörter / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat



Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passworte / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat



Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)



Enrollment-Prozess

1. Bootstrap
 - MDE Profile
2. Barcode Scannen
 - Enrollment URL
 - Passworte / Secrets
3. Zert Enrollment
 - MDE - Webservice
4. Aktivierung Zertifikat



keyon


Agenda

- Einführung PKI
- Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)
- Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)
- Integriertes Token Management**
- Zertifikate für mobile Devices (iPhone, etc.)
- Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

keyon

Integriertes Token Management

- Fokus auf benutzerspezifische Prozesse
 - Ausgabe von Zertifikaten
 - Erneuerung von Zertifikaten
 - Sperrung von Zertifikaten
 - Ausgabe von temporären Hardware-Tokens
 - [Setzen / Zurücksetzen von PIN / PUK eines Hardware-Tokens](#)
 - Notfallprozesse, falls ein Travelling User seinen Hardware-Token verliert und keine Möglichkeit hat, einen Ersatz zu bekommen
 - Zentrale oder dezentrale Personalisierung



Integriertes Token Management

keyon

- Live Demo mit Microsoft Forefront Identity Manager 2010
 1. Benutzer hat PIN gesperrt auf seiner Smartcard
 - Windows Logon möglich
 - Kein *Secure Kiosk Account* nötig
 2. Start Windows 7 basierter Offline PIN Unblocking Prozess
 3. Kontaktaufnahme mit dem Helpdesk
 - Challenge
 - Identifikation des Benutzers
 - Response
 4. Eingabe eines neuen PIN
 5. Windows Logon



Integriertes Token Management

keyon

- Live Demo mit Microsoft Forefront Identity Manager 2010



Integriertes Token Management

keyon

- Next Generation Token Management
 - Nahtlose Integration in die Client Systeme
 - Keine Middleware (Smart Card Minidriver)
 - Unterstützung von unterschiedlichen Enrollment Prozessen
 - Zentral / Dezentral
 - Renewal / Revocation
 - Reporting, etc.



Agenda

keyon

Einführung PKI

Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)

Integriertes Token Management

Zertifikate für mobile Devices (iPhone, etc.)

Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

Zertifikate für mobile Devices (iPhone, etc.)

keyon

Ausgangslage und Ziele

- Sichere Datensynchronisation (Exchange, etc.)
- Mobile Device wird zum „Token“
- Zentrale und Over-the-Air Verwaltung von Profilen und Zertifikaten
- Effiziente Sperrung / Löschung der Mobile Devices
- Einfache, kostengünstige und sichere Verwaltung der Sicherheitselemente

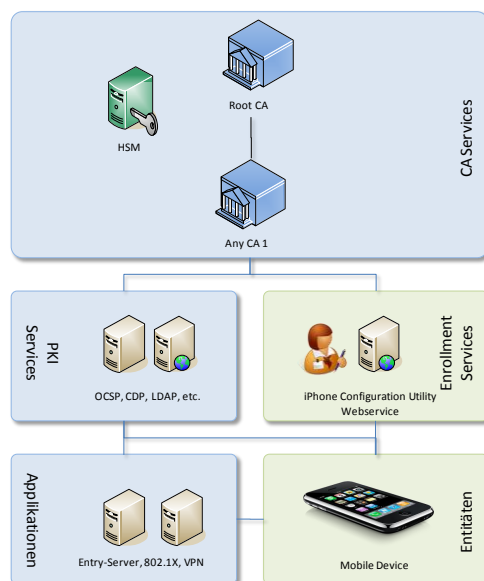


Zertifikate für mobile Devices (iPhone, etc.)

keyon

Design und Umsetzung

- CA Services
 - Microsoft PKI inkl. HSM
- Enrollment Services
 - iPhone Configuration Utility
 - Microsoft Network Device Enrollment Service (NDES)
 - Keyon / Webservice
- Entitäten
 - iPhone
- Applikationen
 - Entryserver
 - Mobile Iron
 - Keyon / true-Tunnel
- PKI Services
 - CDP



Zertifikate für mobile Devices (iPhone, etc.)

keyon

■ Enrollment-Prozess – SCEP

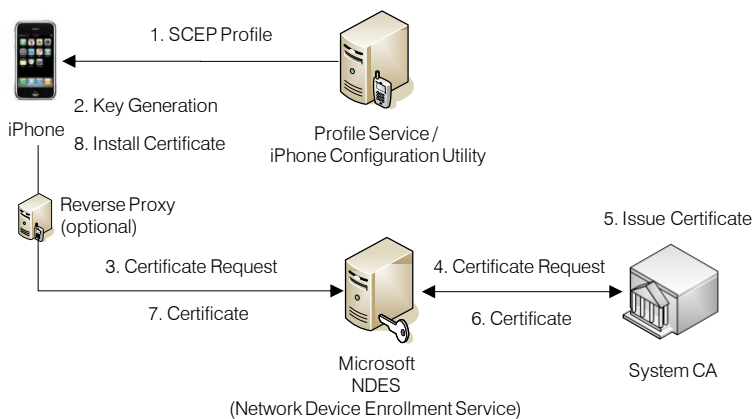
- Installation eines benutzerspezifischen SCEP Profils
 - Benutzerspezifischer Challenge / Subject DN
 - Wired oder Over-the-Air (secure logon)



Zertifikate für mobile Devices (iPhone, etc.)

keyon

■ Enrollment-Prozess – SCEP



Zertifikate für mobile Devices (iPhone, etc.)

keyon

Enrollment-Prozess – SCEP

1. Download Profile (secure)



2. Install Profile



3. Done (Over-the-Air)



Zertifikate für mobile Devices (iPhone, etc.)

keyon

Enrollment-Prozess – weitere Profile

- Installation weiterer Profile
 - Einschränkungen (Kamera, Apps, etc.)
 - Kommunikationsparameter (Exchange Server, Username, etc.)
 - Wi-Fi Parameter
 - etc.



Zertifikate für mobile Devices (iPhone, etc.)

keyon

Enrollment-Prozess – Zertifikatsmanagement

- Verwalten der Zertifikate und Zertifikatsprofile über Keyon / RA / Helpdesk

The screenshot displays the 'Registration Authority' web interface. The main area is titled 'Certificate Search and Administration'. It features several search filters: 'Certificate Status' (All Certificates, Valid Certificates, Expired Certificates, Revoked Certificates, Let Expire Certificates) and 'Certificate Validity' (Between start and end dates). Below these filters is a table with 77 certificates found. The table columns include Serial Number, Web Name, Status, Valid To, Requested By, and Application ID. To the right, a detailed view for a specific certificate 'webapp.pkidemo.net' is shown, including its Issuer Name, Subject Name, Valid From, Valid To, and Certificate Template.

Zertifikate für mobile Devices (iPhone, etc.)

keyon

Enrollment-Prozess – PKCS#12

- Installation eines benutzerspezifischen Profils
 - PKCS#12 File aus dem Windows User Store
 - Vollständiger Setup über das USB Kabel
 - Nur beschränkt für eine grosse Anzahl Benutzer geeignet

The screenshot shows the 'iPhone Configuration Utility' application. A 'Personal Certificate Store' dialog box is open, prompting the user to select certificate(s) to use. The dialog lists certificates with columns for Issued to, Issued by, Intended..., Friendly..., Expiration, and Location. In the background, the main configuration window is visible, showing fields for 'Email Address', 'Password', 'Mail Sync' (set to 3 days), and 'Authentication Credential Name'.

Agenda

keyon

Einführung PKI

Swiss Re: – Sichere Devicezertifikate in Hardware (TPM)

Manor: Zertifikate für mobile Datenerfassungsgeräte (MDE)

Integriertes Token Management

Zertifikate für mobile Devices (iPhone, etc.)

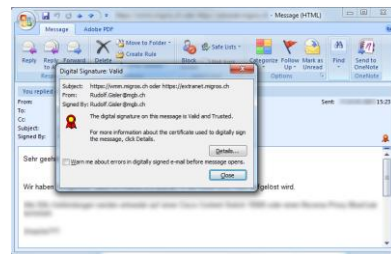
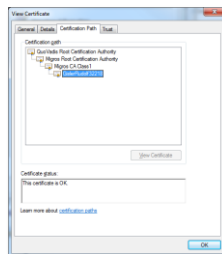
Migros-Genossenschafts-Bund: Subordinierung öffentliche CA

MGB: Subordinierung öffentliche CA

MIGROS keyon

Ausgangslage und Ziele

- Globaler Trust durch vorinstallierte CA Zertifikate in gängigen Applikationen
- Sicherer Datenaustausch ohne vorgängige Etablierung eines Trusts (Email, Webapplikationen)
- Flexible Ausgabe eigener Public-Corporate Benutzer- und Serverzertifikate
- Definierte Sicherheitsanforderungen gemäss Richtlinien der CA

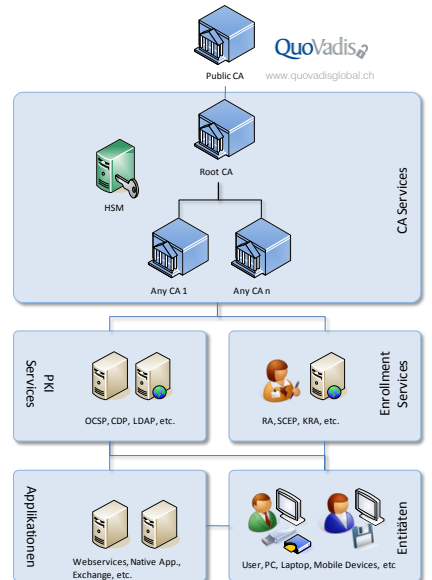


MGB: Subordinierung öffentliche CA



- Design und Umsetzung

- CA Services
 - Microsoft PKI inkl. HSM
- Enrollment Services
 - Keyon / Enrollment Service
 - Keyon / RA / Helpdesk
 - Aladdin „TMS“
 - Key Recovery Agents
- Entitäten
 - Benutzer / Server
- Applikationen
 - Outlook / Exchange
 - Webapplikationen / Services / WES
- PKI Services
 - CDP



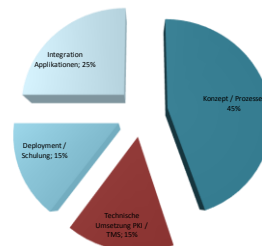
MGB: Subordinierung öffentliche CA



- Corporate PKI vs. Outsourced PKI

- Eine eigene Corporate PKI sichert einem Unternehmen die Flexibilität die es braucht, um Applikationen und Prozesse rasch integrieren zu können.

Ein Outsourcing einer Corporate PKI ist wenig sinnvoll, da die zentralen Prozesse wie die Registrierung von Benutzern und Systemen oder die Integration von PKI basierten Applikationen nur durch das Unternehmen selbst durchgeführt werden können.



Vielen Dank für Ihre Aufmerksamkeit



Bei Fragen stehen wir Ihnen gerne zur Verfügung.



Aus Gründen Ihrer Sicherheit