

Heute über:

PKI – Aufbau und  
Betrieb einer  
sicheren MS PKI

*by*

TEMS SECURITY SERVICES



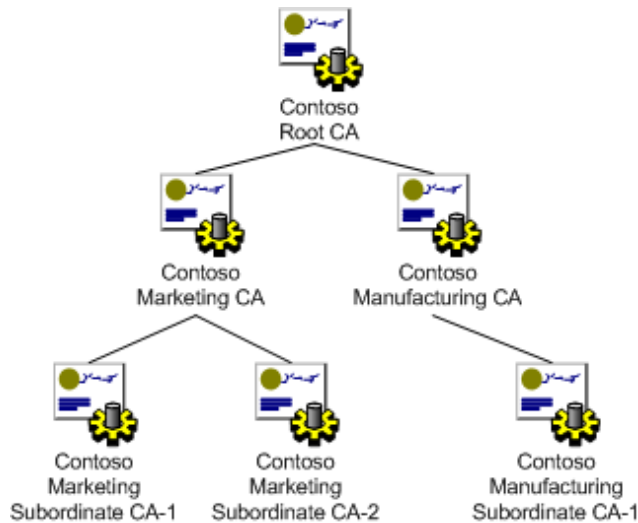


PHILIP BERGER

MICHAEL MEIXNER

# Agenda

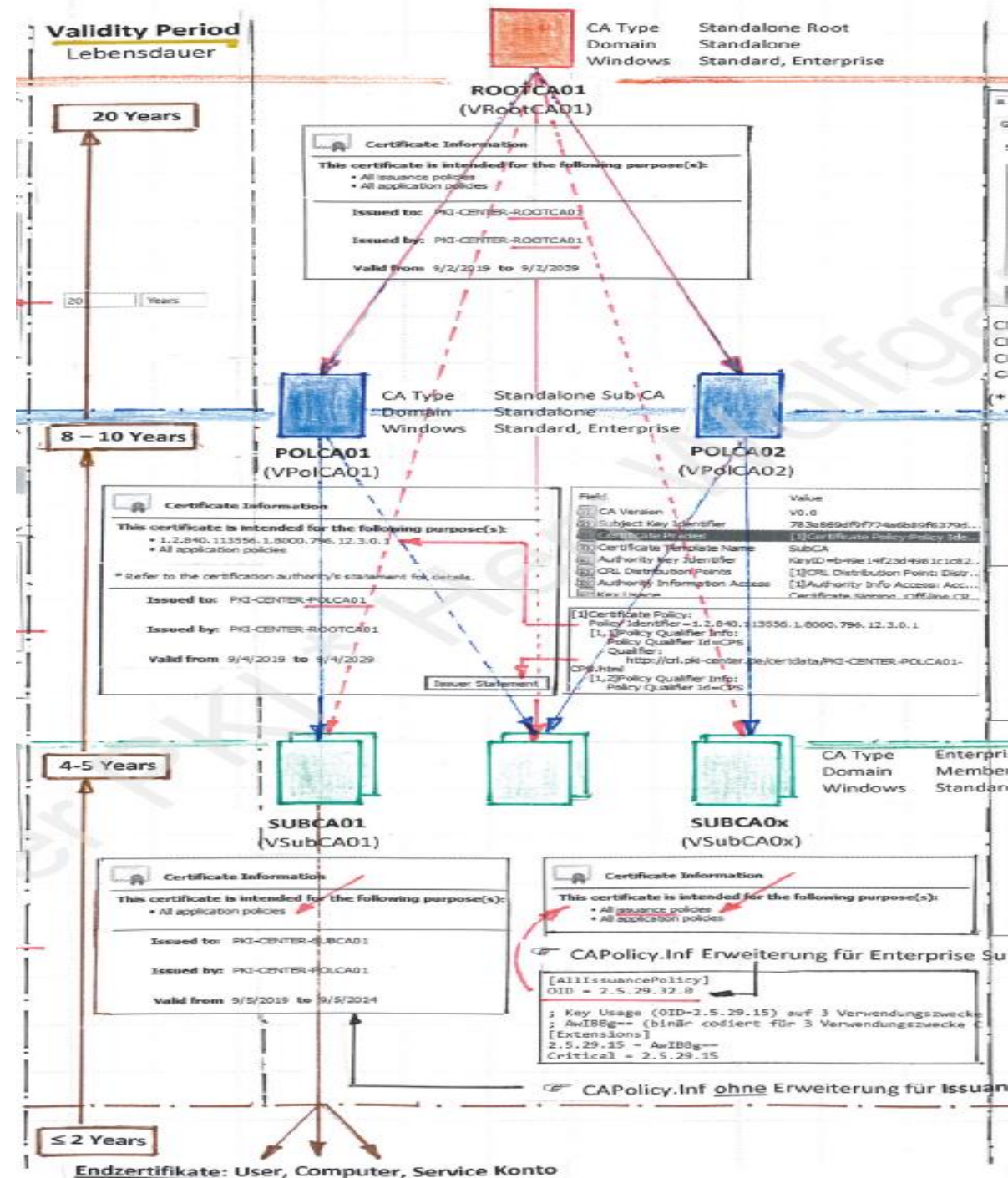
## PKI – Aufbau und Betrieb einer sicheren Microsoft PKI Umgebung



- Warum eine PKI?
- Aufbau einer PKI
- Grundlagen zur Verschlüsselung von “Nachrichten”
- Zertifikate X.509 Standard
- Lab?
- Lesson learned

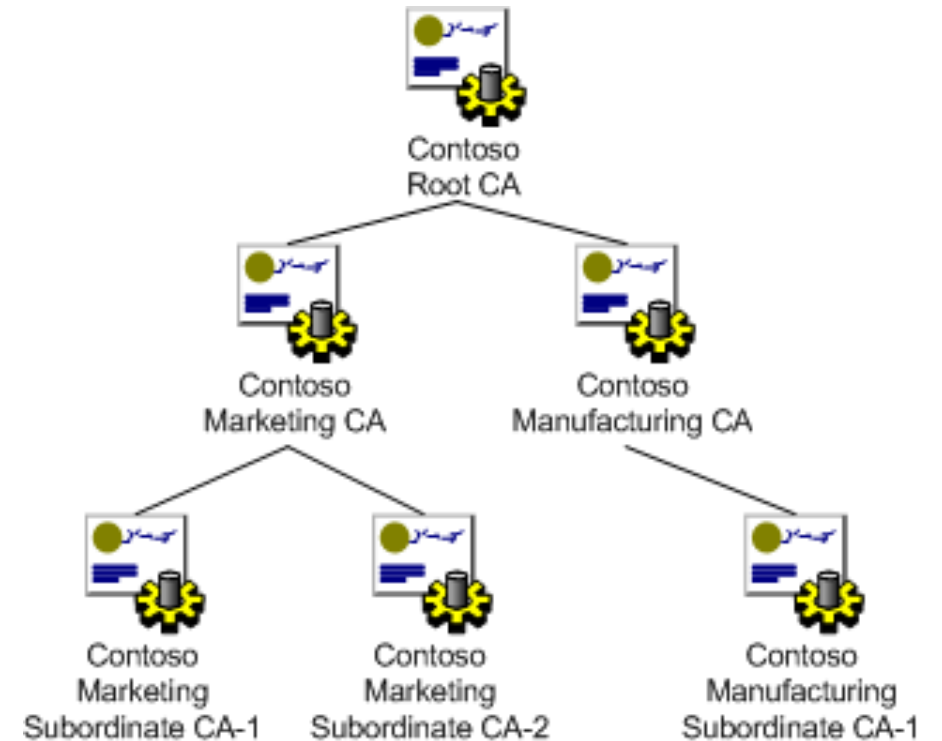
# Aufbau und Gültigkeit einer PKI 2- oder 3-stufig

- Gültigkeit der CA's richtet sich nach Gültigkeit der ausgestellten Zertifikate für die
- Eine PKI kann ein- oder mehrstufig sein
- „Sichere“ PKI sollte aber zumindest immer 2-stufig sein
- Root CA immer offline – nur für CRLs und CA Zertifikate
- Dreistufige CA nur wenn CA Policies (Policy CA) notwendig sind
  - Constraints
  - Issuing,...



# Aufbau und Gültigkeit

- Public key certificates („digital certificates“) sind elektronische Identitätsdokumente
- Rollen
  - **Certification Authorities (CA)** speichert, stellt aus und signiert Zertifikate
  - **Registration Authorities (RA)** Überprüft die Identität der CA's
- Technologien
  - **Zentrales Verzeichnis** bietet sicheren Ort wo Schlüssel gespeichert und indiziert sind
  - **Certificate management system**
    - Erstellt, sperrt und liefert neu auszustellende Zertifikat
    - Sucht, ruft ab und greift auf gespeicherte Zertifikate zu
- **Zertifikatsrichtlinie** legt fest, die es außenstehenden ermöglicht, der Vertrauenswürdigkeit der PKI zu analysieren



# Einsatzgebiete einer PKI

- Ist ein System zum Erstellen, Speichern, Verteilen, Validieren, Widerrufen und verwalten digitaler Zertifikate, mit dem die Identität des Eigentümers eines im Zertifikat öffentlichen Schlüssel überprüft wird
- Eine PKI kann ein- oder mehrstufig sein
- „Sichere“ PKI sollte aber zumindest immer 2-stufig sein
- Root CA immer offline – nur für CRLs und CA Zertifikate
- Dreistufige CA nur wenn CA Policies (Policy CA) notwendig sind
  - Constraints
  - Issuing,...

## ◆ PKI-Einsatzgebiete

Die Haupteinsatzgebiete der PKI sind u.a.:

Sicherheitsdienste	Sicherheitsmechanismen
• <b>Authentifizierung</b> – Message origin authentication (Echtheit)	Digital Signature
• <b>Integrität</b> – Message integrity (Veränderung)	Digital Signature
• <b>Nichtzurückweisung</b> – Nonrepudiation of origin	Digital Signature
• <b>Vertraulichkeit</b> – Message confidentiality (Verschlüsselung)	Encryption
• <b>Schlüssel-Management</b> – Key Management	PKI-Management

Die Anwendungen der PKI in einer Windows-Welt sind u. a.:

- **SSL/TLS** → Secure Channel-Authentifizierung
- **S/MIME** → Email
- **Smart Card** → Zweifaktor-Authentifizierung
- **Software-Authentication Code** → Signierung von Software
- **Encrypted File System (EFS)** → Datei-Verschlüsselung
- **BitLocker** → Volumen-Verschlüsselung
- **IPSec** → Datenpaket-Verschlüsselung und Authentifizierung
- **Port Authentication** → Schützen von Switch Ports durch Zertifikat



# Grundlagen zur Verschlüsselung

- RSA (Rivest-Shamir-Adleman) asymmetrisches Verfahren
  - Schlüssellängen von min. 3k sind vertretbar bis 2031
- AES (Advanced Encryption Standard) symmetrisches Verfahren
- ECC (Elliptic Curve cryptography) asymmetrisches Kryptosystem
- SHA (Secure Hash Algorithms) kollisionsresistente Einwegfunktion
  - SHA-256 als Mindeststandard

## Algorithm Strength „RSA“ und „EC“ Key Type

### Comparable Algorithm Strengths

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>

Strength	Symmetric	RSA	ECDSA	Hash	Not in NIST, but comparable anyway
80 bit	2TDEA	RSA 1024	ESDSA 160	SHA-1	<b>Key Type „RSA“</b>
112 bit	3TDEA	RSA 2048	ECDSA 224	SHA-224	
128 bit	AES-128	RSA 3072	ECDSA 256	SHA-256	
192 bit	AES-192	RSA 7680	ECDSA 384	SHA-384	
256 bit	AES-256	RSA 15360	ECDSA 512	SHA-512	

Security Strength	Through 2030	2031 and Beyond
< 112	Applying	Disallowed
	Processing	Legacy-use
112	Applying	Disallowed
	Processing	Acceptable
128	Applying/Processing	Acceptable
192	Applying/Processing	Acceptable
256	Applying/Processing	Acceptable

### Key Type „EC“

128 Bit Strength (RSA)	128 Bit Strength (Suite-B)	Zweck
RSA 4096	ECDSA_P256	Digital Signature
AES-128 oder höher	AES-128 oder höher	Symmetric Encryption
SHA-256	SHA-256	Hash

CNG (Cryptography Next Generation – Windows PKI 2018) supports the following key types:

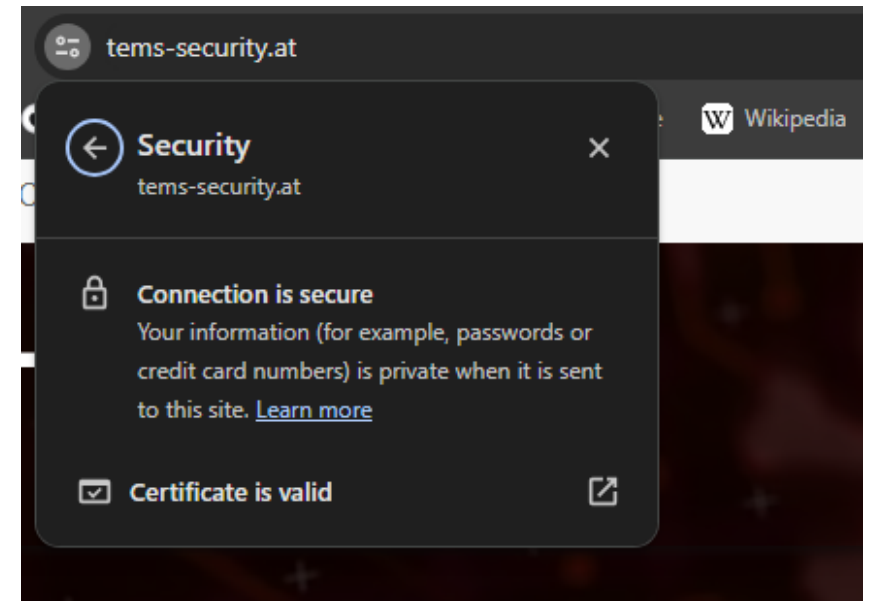
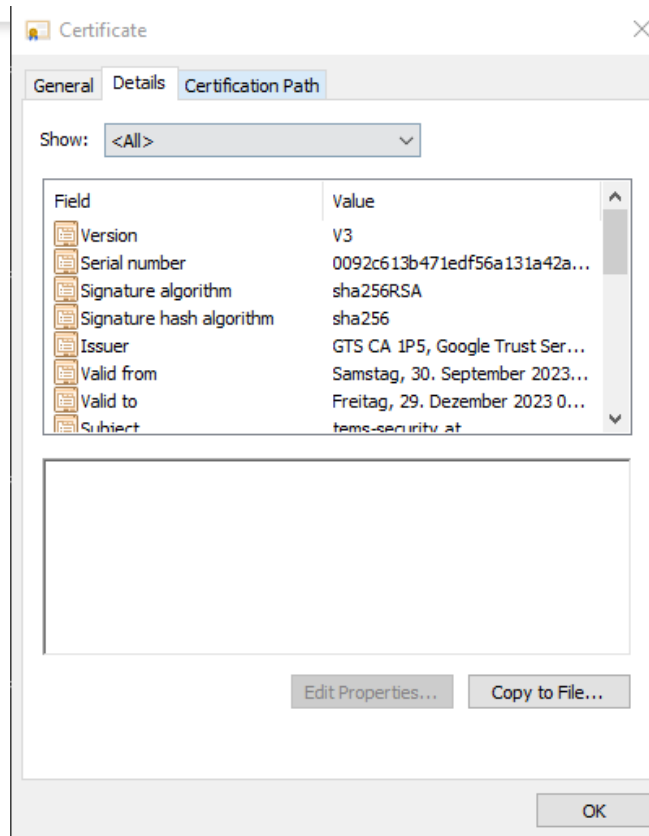
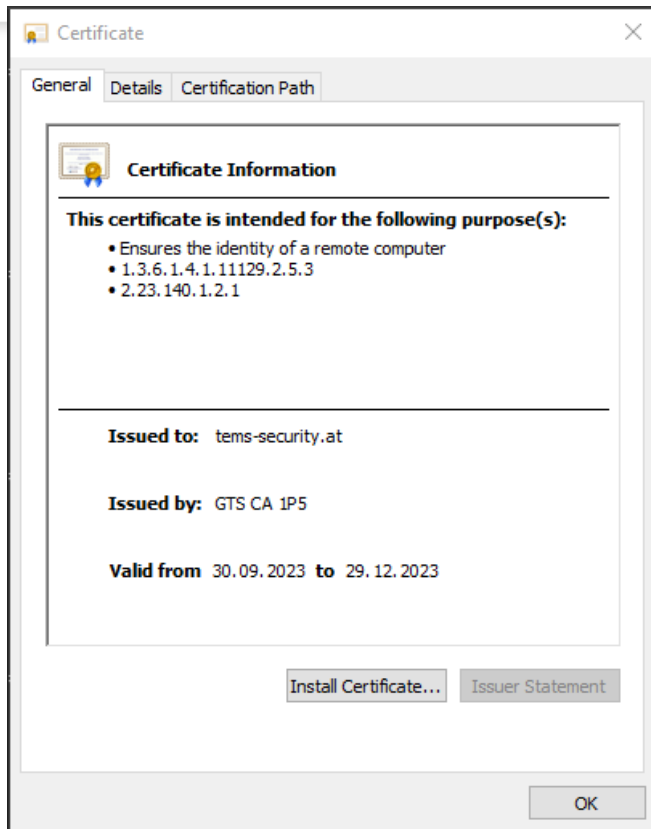
- DH: Diffie-Hellman Public & Private keys.
- DSA: Digital Signature Algorithm (DSA, FIPS 186-2) Public & Private keys.
- **RSA**: PKCS #1 Public & Private keys.
- Legacy CryptoAPI: Public & Private keys.
- **EC**: Elliptic Curve Cryptography Public & Private keys.

# Certificate Revocatin List (CRL)

- CRL ist der Mechanismus, mit dem die Zertifizierungsstelle andere darüber informiert, dass ein Zertifikat aus irgendeinem Grund ungültig geworden ist
- Gründe warum ein Zertifikate zurück- bzw. eingezogen werden
  - Der private Schlüssel des Zertifikatsinhaber wurde kompromittiert
  - Zertifikat wurde an eine falsche Person ausgestellt
  - Zertifikat ist abgelaufen
  - Zertifikat ist ungültig geworden aus diversen anderen Gründen – CA Manager hat es für ungültig erklärt...
- Ungültige Zertifikate kommen auf der **certificate revocation list** (CRL)
  - Abfrage erfolgt per http – ist im Zertifikat (CDP) vermerkt wo diese zu finden ist
  - OCSP (Online Certificate Status Protocol) neuer Variante. Wesentlich schneller CRL Veröffentlichung



# Zertifikatsaufbau



# Lab - SCAMA

The image shows a Windows command prompt window displaying the output of the 'GROUP INFORMATION' command. The output is a table with columns for Group Name, Type, SID, and Attributes. The 'EMICH\Enterprise Admins' group is highlighted with a yellow circle. Below the command prompt, two Active Directory console windows are open. The 'Enterprise Admins Properties' window shows its members, with 'Administrator' and 'T0-EntAdmins' circled in yellow. The 'T0-EntAdmins Properties' window is also open, showing its members list.

```
GROUP INFORMATION
-----
Group Name                                     Type                SID                  Attributes
-----
Everyone                                       Well-known group    S-1-1-0              Mandatory
BUILTIN\Users                                 Alias                S-1-5-32-545         Mandatory
BUILTIN\Certificate Service DCOM Access      Alias                S-1-5-32-574         Mandatory
BUILTIN\Administrators                       Alias                S-1-5-32-544         Group users
BUILTIN\Remote Desktop Users                Alias                S-1-5-32-555         Mandatory
NT AUTHORITY\REMOTE INTERACTIVE LOGON        Well-known group    S-1-5-14             Mandatory
NT AUTHORITY\INTERACTIVE                     Well-known group    S-1-5-4              Mandatory
NT AUTHORITY\Authenticated Users             Well-known group    S-1-5-11             Mandatory
NT AUTHORITY\This Organization               Well-known group    S-1-5-15             Mandatory
LOCAL                                         Well-known group    S-1-2-0              Mandatory
EMICH\T0-EntAdmins                           Group                S-1-5-21-679215464-461140693-3863167668-1135 Mandatory
EMICH\Enterprise Admins                       Group                S-1-5-21-679215464-461140693-3863167668-519 Group users
EMICH\T1-Denied                               Group                S-1-5-21-679215464-461140693-3863167668-1138 Mandatory
EMICH\T0-Allowed                              Group                S-1-5-21-679215464-461140693-3863167668-1139 Mandatory
EMICH\T2-Denied                               Group                S-1-5-21-679215464-461140693-3863167668-1140 Mandatory
EMICH\PAW-Users                               Group                S-1-5-21-679215464-461140693-3863167668-1141 Mandatory
NT AUTHORITY\Claims Valid                     Well-known group    S-1-5-113            Mandatory
Authentication authority assertion           Well-known group    S-1-5-114            Mandatory
Fresh public key identity                    Well-known group    S-1-5-115            Mandatory
NT AUTHORITY\Compound Identity                Well-known group    S-1-5-116            Mandatory
EMICH\Denied RODC Password Replication       Well-known group    S-1-5-117            Mandatory
NT AUTHORITY\This Organization                Well-known group    S-1-5-15             Mandatory
Mandatory Label\Medium Mandatory Control     Well-known group    S-1-5-118            Mandatory

C:\Users\t-0entseadm>
```

Active Directory Users and Computers

Enterprise Admins Properties

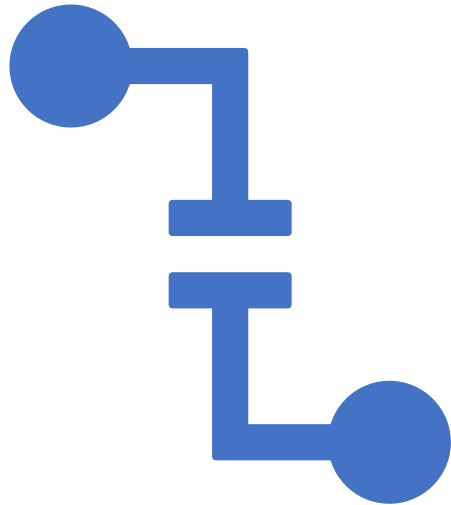
Name	Active Directory Domain Services Folder
Administrator	emich.local/Users
T0-EntAdmins	emich.local/ESAE/Tier 0/Groups

T0-EntAdmins Properties

Name	Active Directory Domain Services Folder
------	---

# Lab – certutil - Examples

---



- `certutil -url cert.cer -> CRL u. OCSP überprüfen`
- `certutil -dspublish RootCA.cert RootCa -> Enterprise Trust`
- `certutil -urlfetch -verify cert.cer -> Zertifikat auf Gültigkeit prüfen`
- `certutil -urlcache * delete -> OSCP u. CRL Cache am Client löschen`

# Dos and Don'ts (1)



- Einschränkung Verwendungszwecke der CA -> soll kein digital Signing machen können
- RootCA soll
  - Keinen Netzwerkzugang haben
  - Keine Windowsupdates (kaputte CA nach Update)
  - Einschalten für Sperrlisten Veröffentlichung und SubCA signing
- Im PKI Name kein Hinweis auf Server bzw. interne Domain Names
- Keine Verwendung der Standard Templates – nur Kopien mit entsprechenden Berechtigungen auf das Template
- Subjectname beim Ausstellen nicht anpassbar bzw. nur dann, wenn der CA Manager „händisch“ ausstellen muss

## Dos and Don'ts (2)



- GPO für Autoenrollment verwenden
- Enterprise Trust für die CA Veröffentlichung, keine GPO zum Zertifikatsverteilen
- EFS Zertifikatsausstellung in GPO deaktivieren
  - Wenn notwendig nur bei aktivem KRA
  - Verlorenes EFS Zertifikat = Datenverlust
  - Ebenso verlorenes S/MIME Zertifikat
- Im PKI Name kein Hinweis auf Server bzw. interne Domain Names
- Sicherung der CA über System State Backup
- Laufzeiten der Zertifikate beachten

# Poll

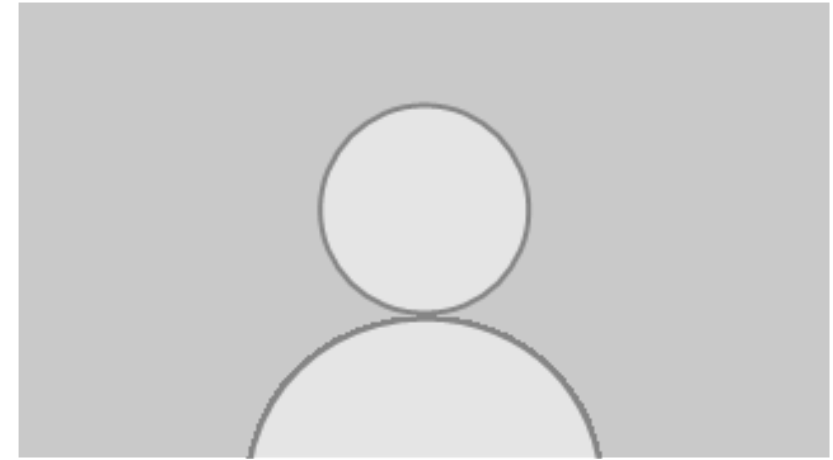
1. PKI im Einsatz?
2. CA Zertifikate eingeschränkt?
3. Template Security angepasst bzw. alle default Templates verwendet







# Next Webinar



December 20th 2023  
09:00am – 12:00pm



Incident Game  
(Max 12 person)

Q&A

tems  
security






Get in contact with us

*Book your expert*

Philip Berger  
Managing Director

 +43(664) 343 8644

 [Philip.berger@tems-security.at](mailto:Philip.berger@tems-security.at)

Michael Meixner, CISSP  
Managing Director

 +43(664) 1453328

 [Michael.meixner@tems-security.at](mailto:Michael.meixner@tems-security.at)