TeleTrusT-EBCA "PKI-Workshop" 2021

Berlin, 30.09.2021

Bedeutung und Zweck der PKI

Clemens Guttenberger
Information Security Consultant

Professional Service Bechtle Hamburg
CISSP | CISM | CISA

Mythos Public Key Infrastructure


WLAN
Microsoft
DirectAccess
Microsoft
Exchange
BitLocker Drive Encryption
IIS
Lync 2013
APACHE
HTTP SERVER
Microsoft
Network Access Protection (NAP)
CISCO JABBER
Secure https://
Windows Server
Active Directory
Microsoft
System Center
SSL VPN
VoIP
Mobile Device Management
Microsoft
Rights Management
PDF
...nur ein Auszug !!!!

• SSL/TLS Zertifikate

Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

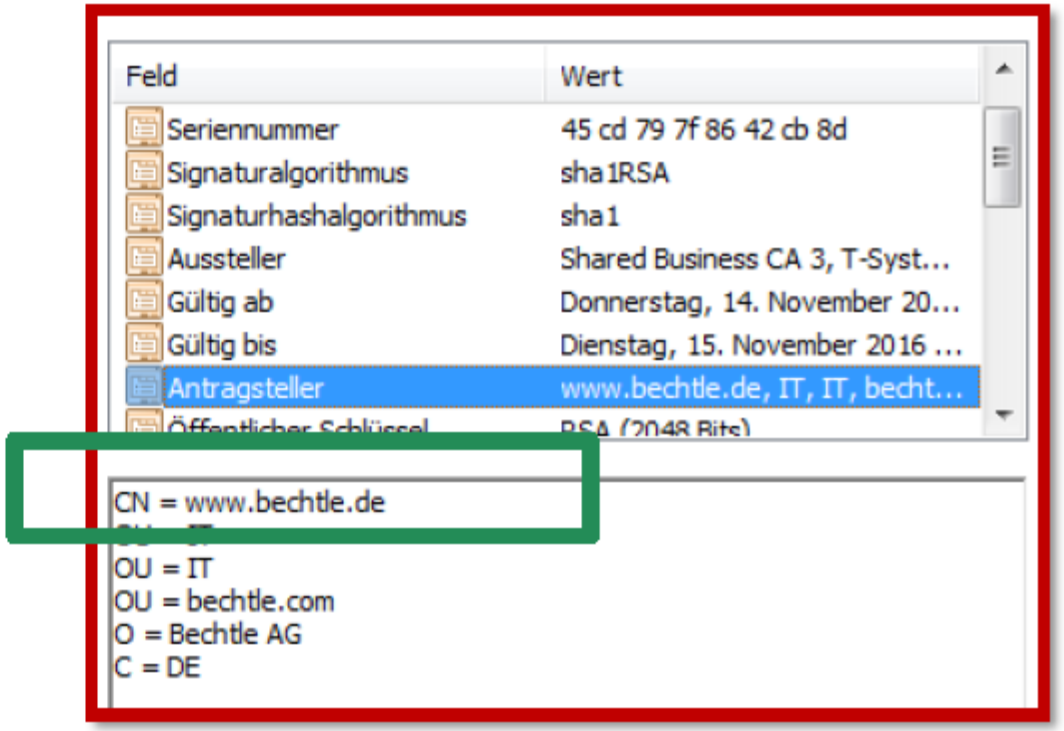
- Garantiert die Identität eines Remotecomputers
- 1.3.6.1.4.1.7879.13.25
- 2.23.140.1.2.2

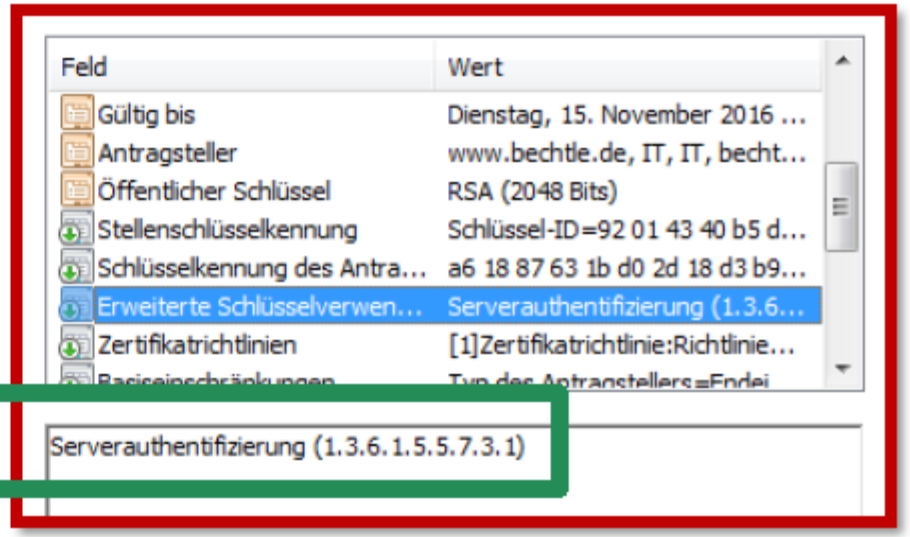
* Weitere Infos finden Sie in den Angaben der Zertifizierungsstelle.

Ausgestellt für: www.bechtle.de

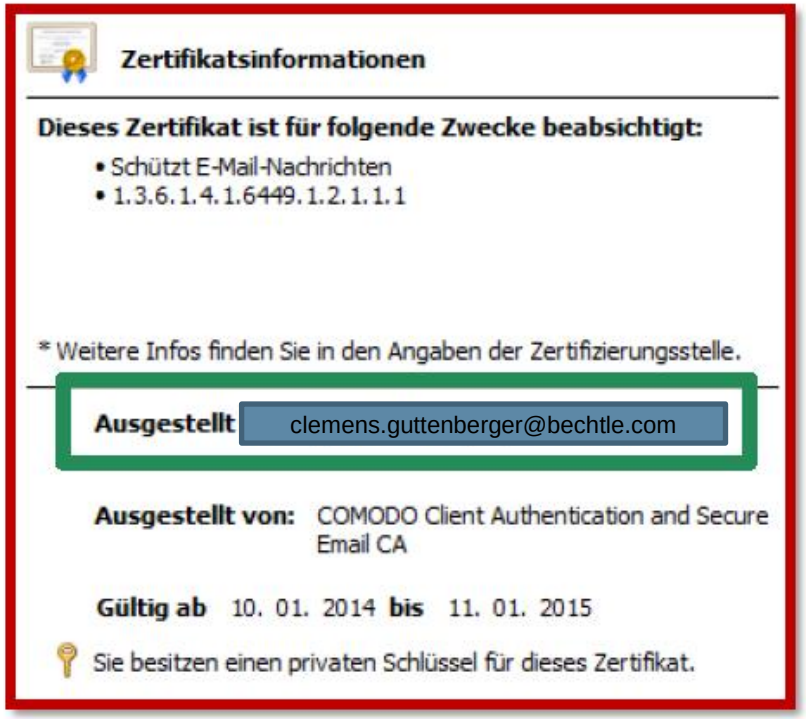
Ausgestellt von: Shared Business CA 3

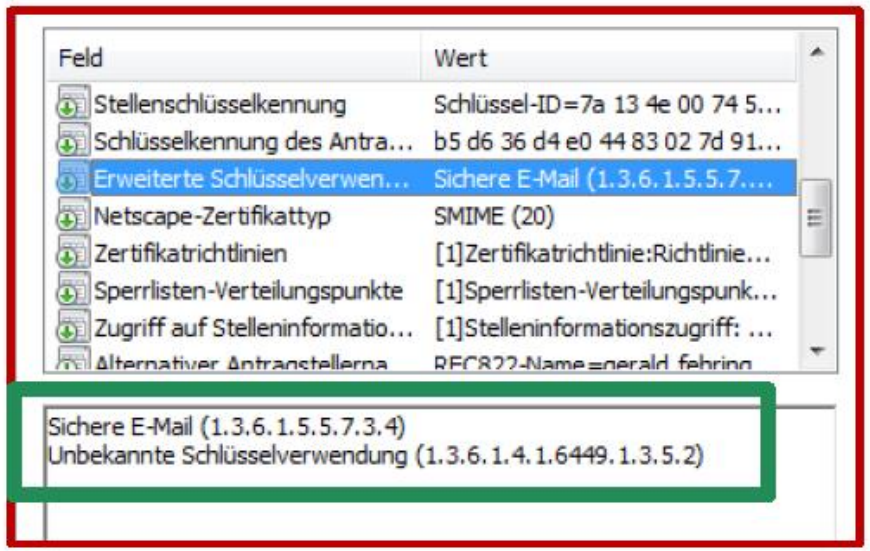
Gültig ab 14. 11. 2013 **bis** 15. 11. 2016

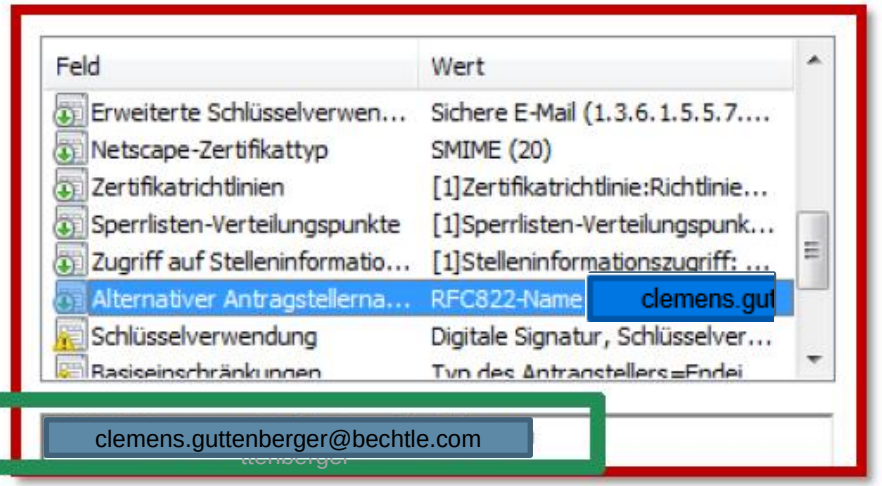




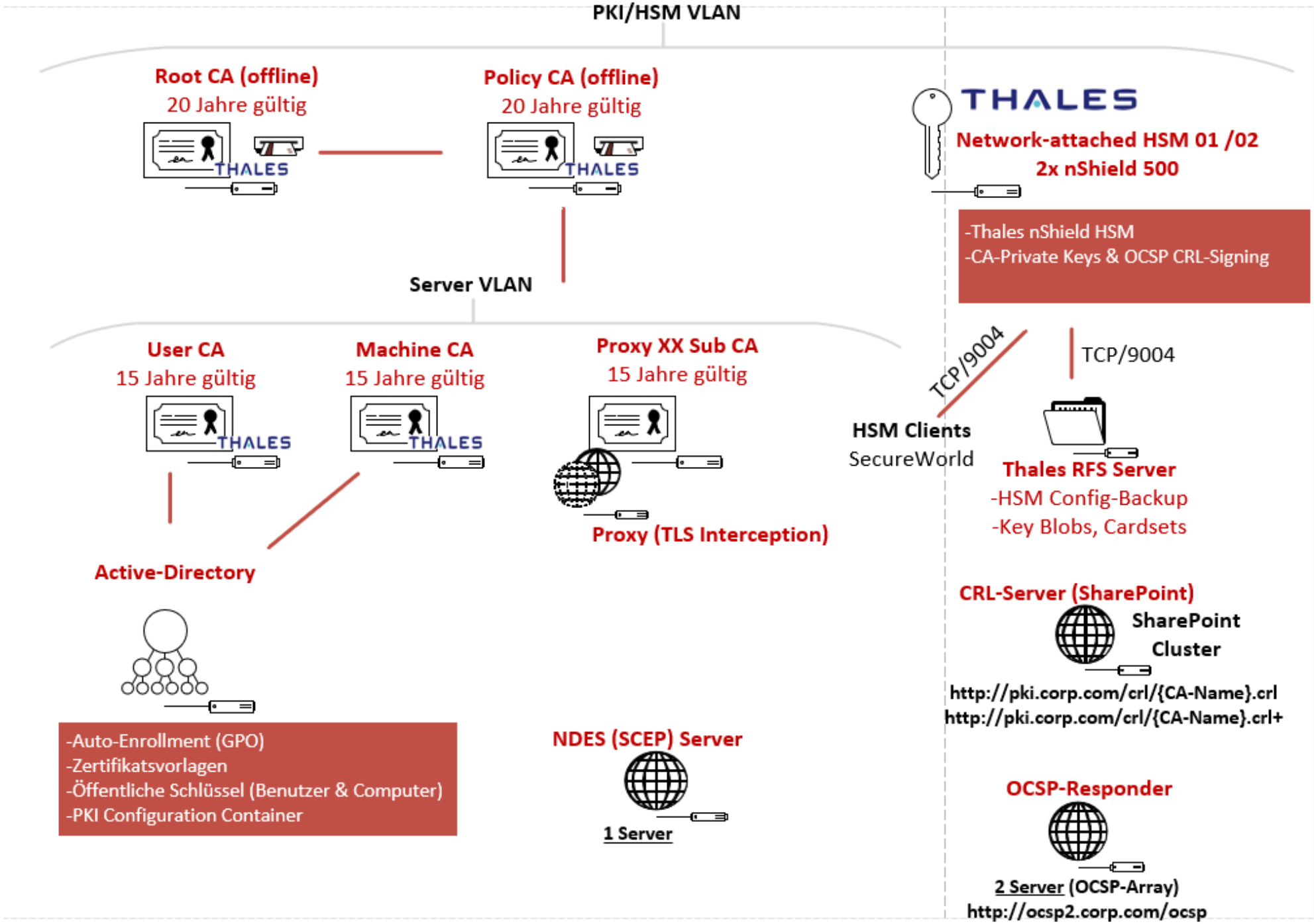
• S/MIME Zertifikate







Vollständige E-Mail Adresse


PKI/HSM VLAN
Root CA (offline)
20 Jahre gültig
Policy CA (offline)
20 Jahre gültig
THALES
Network-attached HSM 01 /02
2x nShield 500
-Thales nShield HSM
-CA-Private Keys & OCSP CRL-Signing
Server VLAN
User CA
15 Jahre gültig
Machine CA
15 Jahre gültig
Proxy XX Sub CA
15 Jahre gültig
TCP/9004
TCP/9004
HSM Clients
SecureWorld
Thales RFS Server
-HSM Config-Backup
-Key Blobs, Cardsets
Proxy (TLS Interception)
Active-Directory
CRL-Server (SharePoint)
SharePoint
Cluster
http://pki.corp.com/crl/{CA-Name}.crl
http://pki.corp.com/crl/{CA-Name}.crl+
-Auto-Enrollment (GPO)
-Zertifikatsvorlagen
-Öffentliche Schlüssel (Benutzer & Computer)
-PKI Configuration Container
NDES (SCEP) Server
1 Server
OCSP-Responder
2 Server (OCSP-Array)
http://ocsp2.corp.com/ocsp

Was sind Zertifikate ?

- Zertifikate bestehen aus einem öffentlichen Schlüssel und Identitäts-informationen, die durch einen Dritten mithilfe einer Signatur unter-schrieben wurden

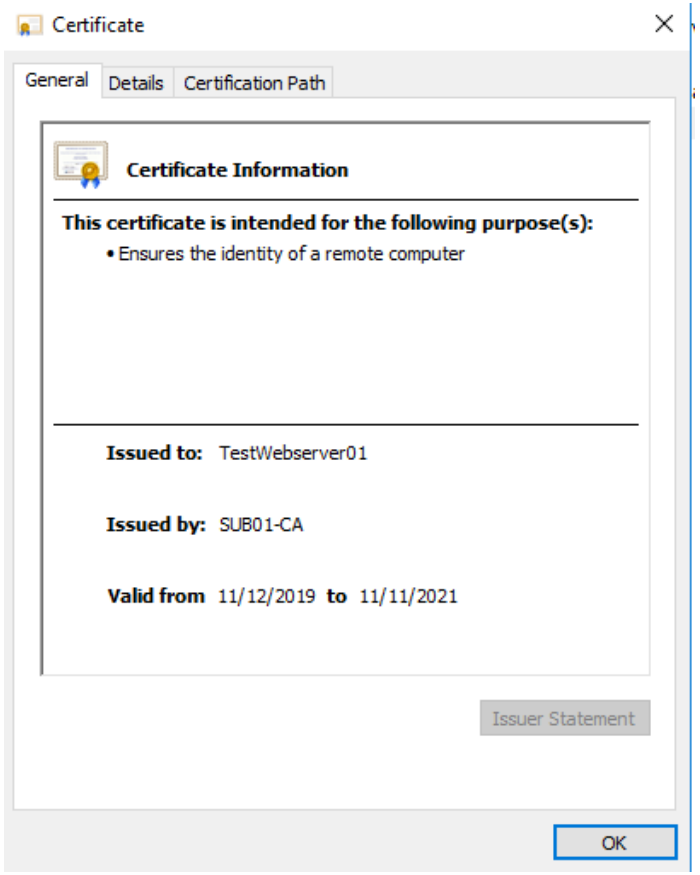
- Jeder öffentliche Schlüssel hat einen privaten Schlüssel

- Zertifikate dürfen und müssen mit einer breiten Öffentlichkeit geteilt werden, wohingegen der private Schlüssel sicher verwahrt werden muss

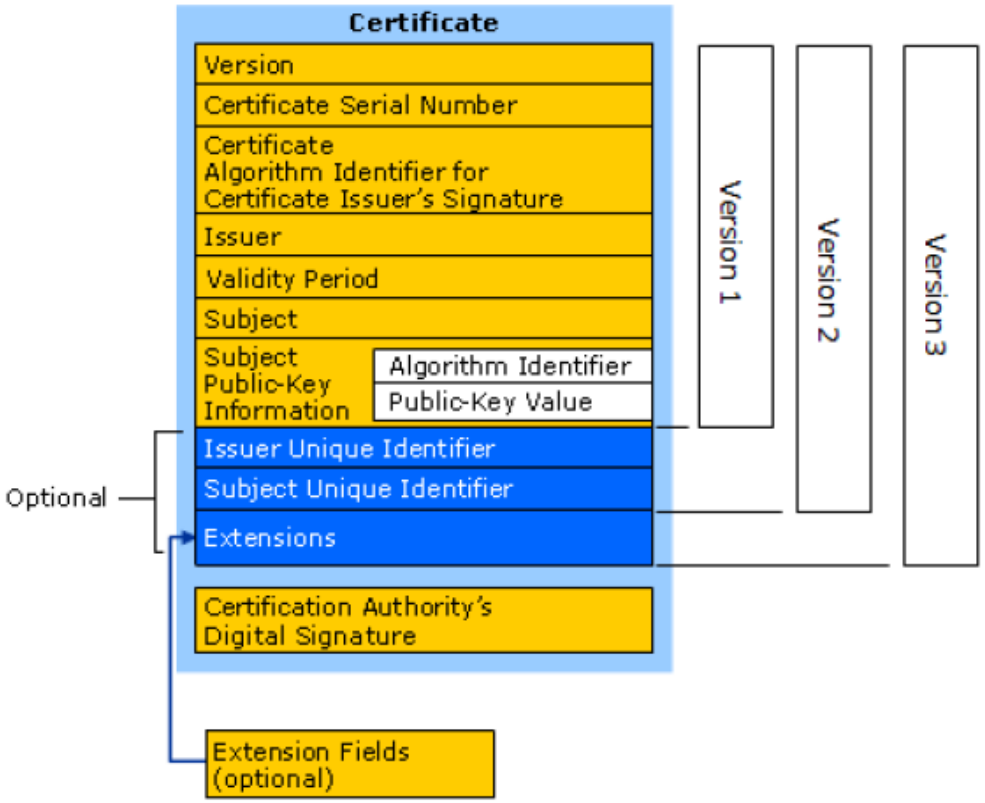
- Dem Aussteller eines Zertifikats muss Vertrauen entgegen gebracht werden (Bsp.: Deutsche Telekom, Verisign oder Thawte Trustcenter

Typische Anwendungsfälle für Zertifikate

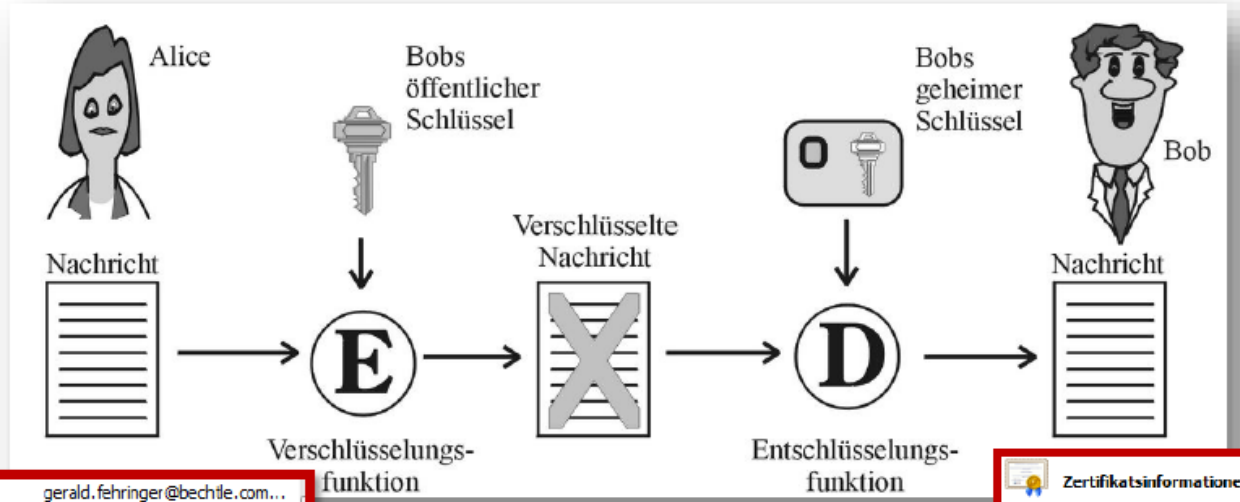
- Active-Directory Anmeldung
- MFA Token für Admins
- AD-AutoEnrollment für Computer- Zertifikate
- Smartcards
- Zertifikate für Benutzer und Code Signing
- Microsoft EFS
- Benutzerzertifikat
- TLS-/SSL- basierte Applikationen
- 802.1X (WLAN)
- Benutzer- bzw. Computerzertifikate
- Mac-OS und mobile Endgeräte
- Microsoft Rights Management Services (RMS)
- Email Signatur / Verschlüsselung

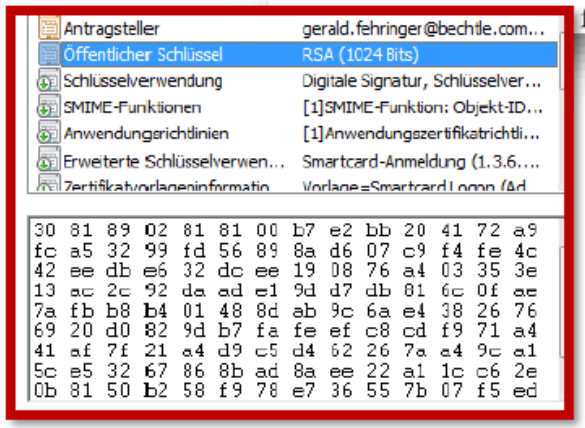


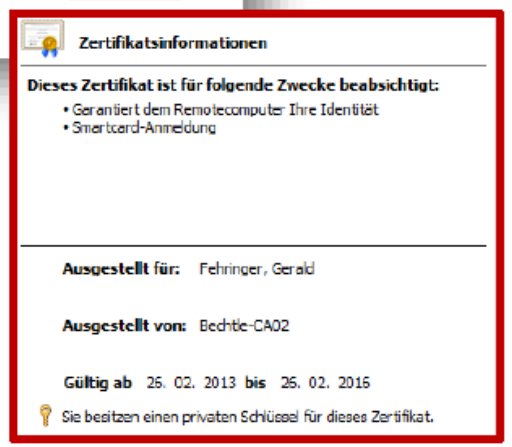
- Zertifikate sind aktuell im X.509 V3 Standard kodiert



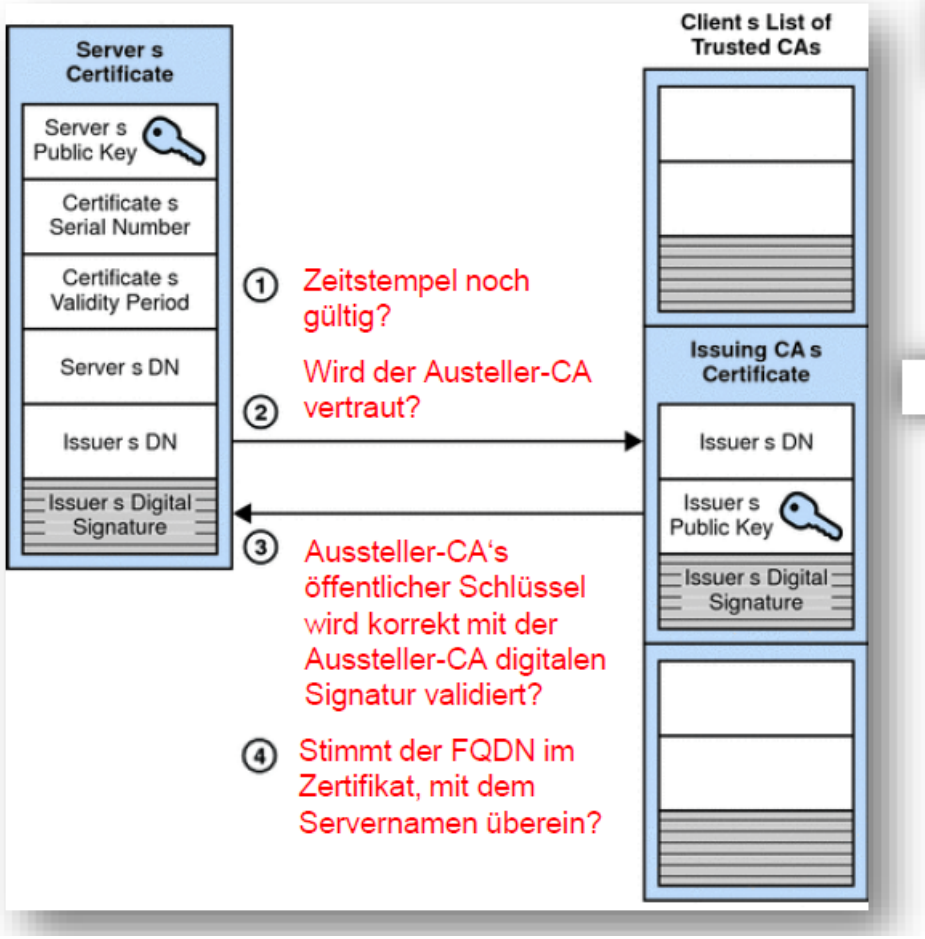
Public-Key Verfahren (Bsp. X509v3 Zertifikate)

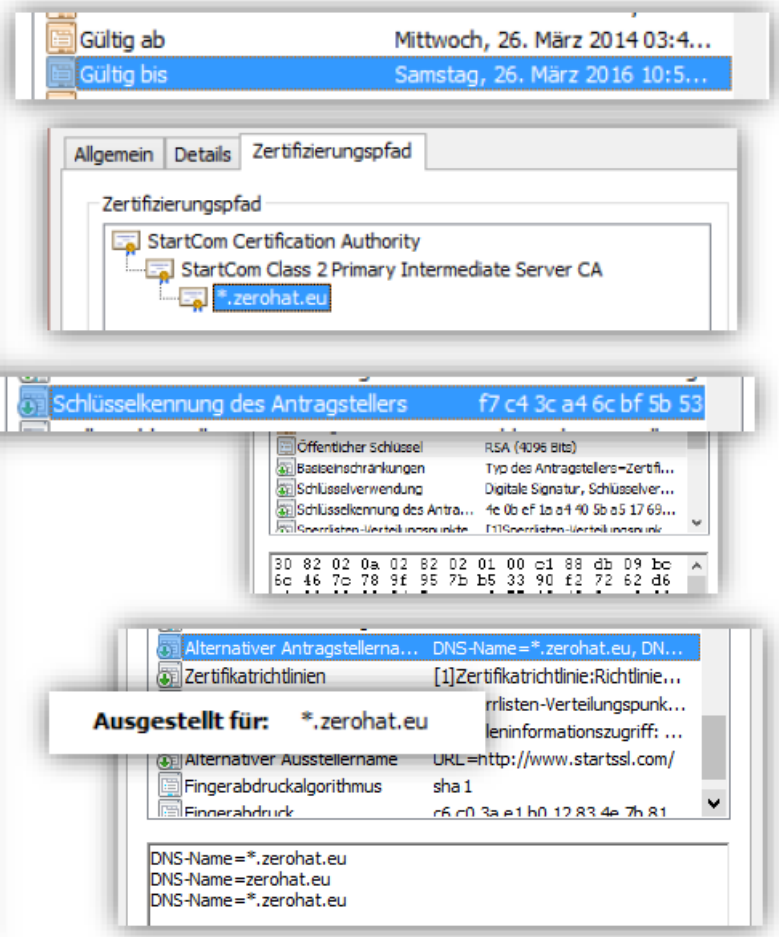




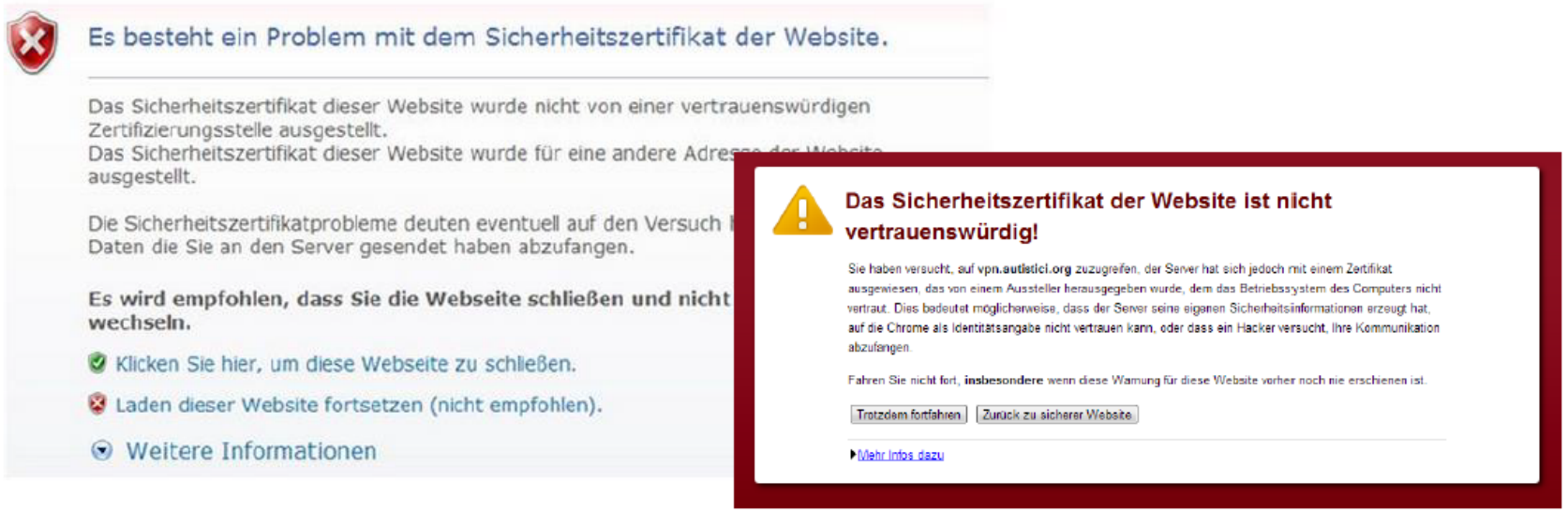


Zertifikatsüberprüfung Reihenfolge





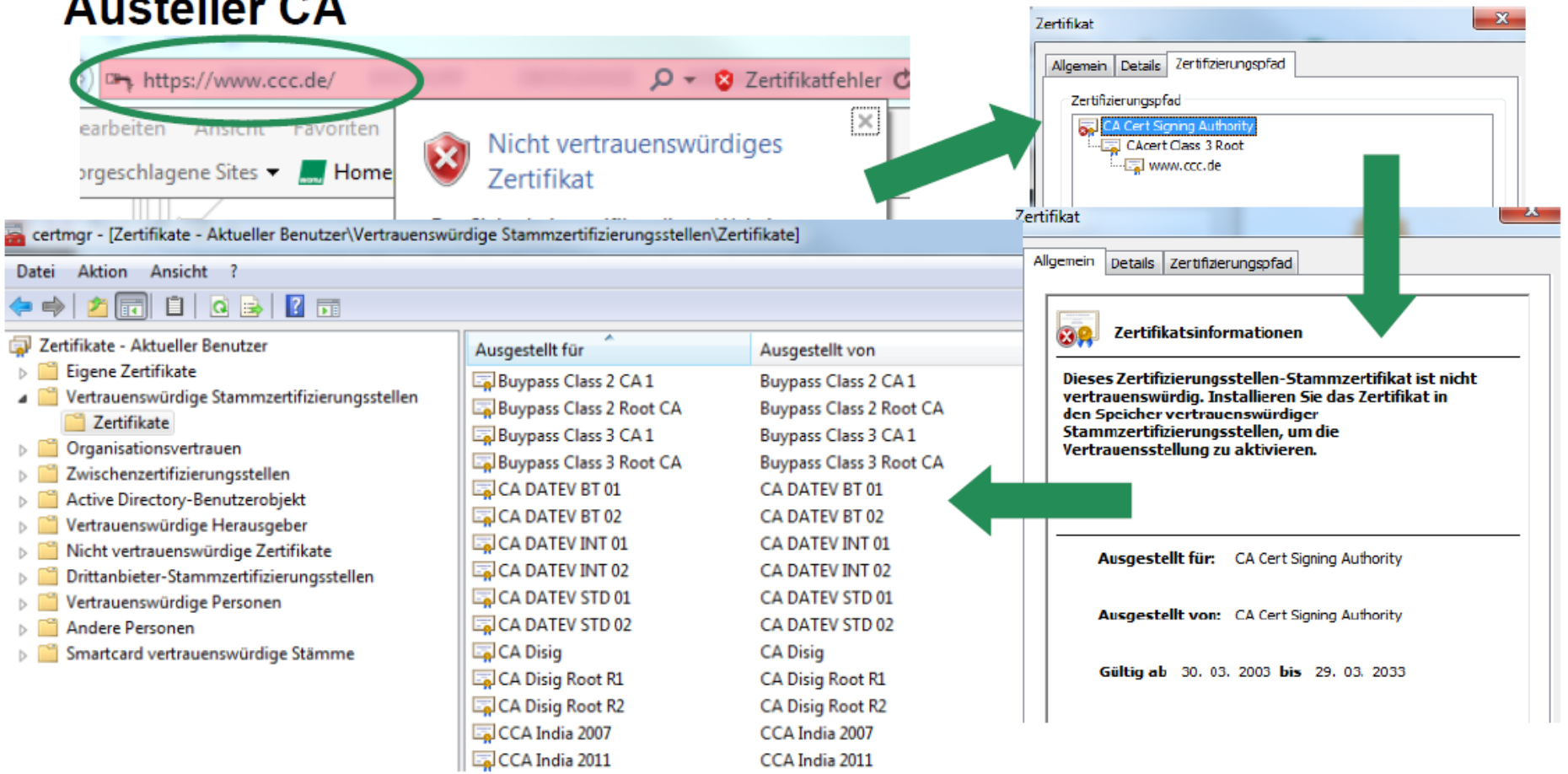
Wer kennt diese Fehlermeldung nicht….



Wo liegt der Fehler?

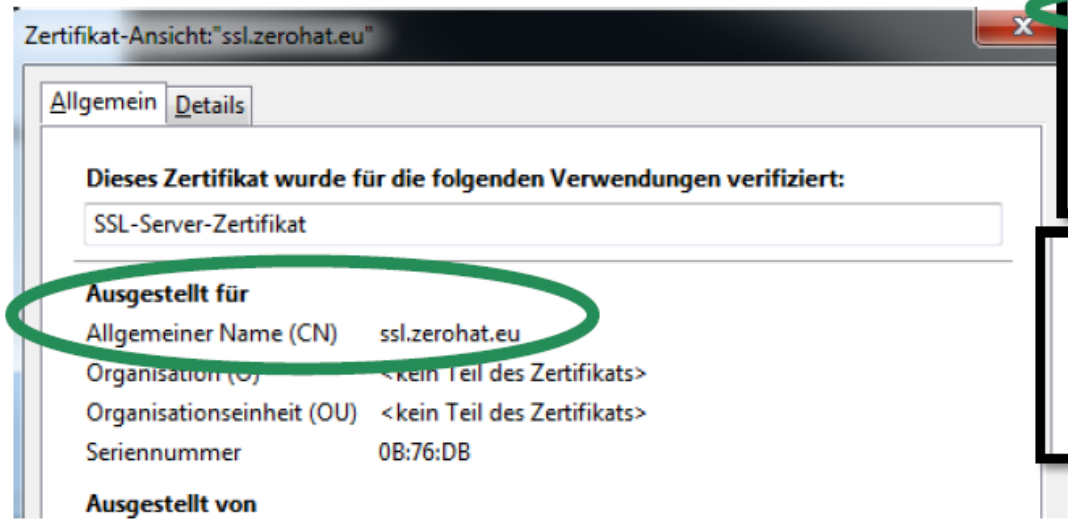
Fehlender **Trust Anchor**: dem Serverzertifikat bzw. dessen Rootzertifikat wird schlicht nicht vertraut, oder der Aufruf der Website stimmt nicht exakt mit dem **Common Name (CN)** oder einem der **SANs (Subject Alternative Names)** die im Zertifikat hinterlegt wurden überein.

Wer kennt diese Fehlermeldung nicht….Beispiel: fehlende Austeller CA

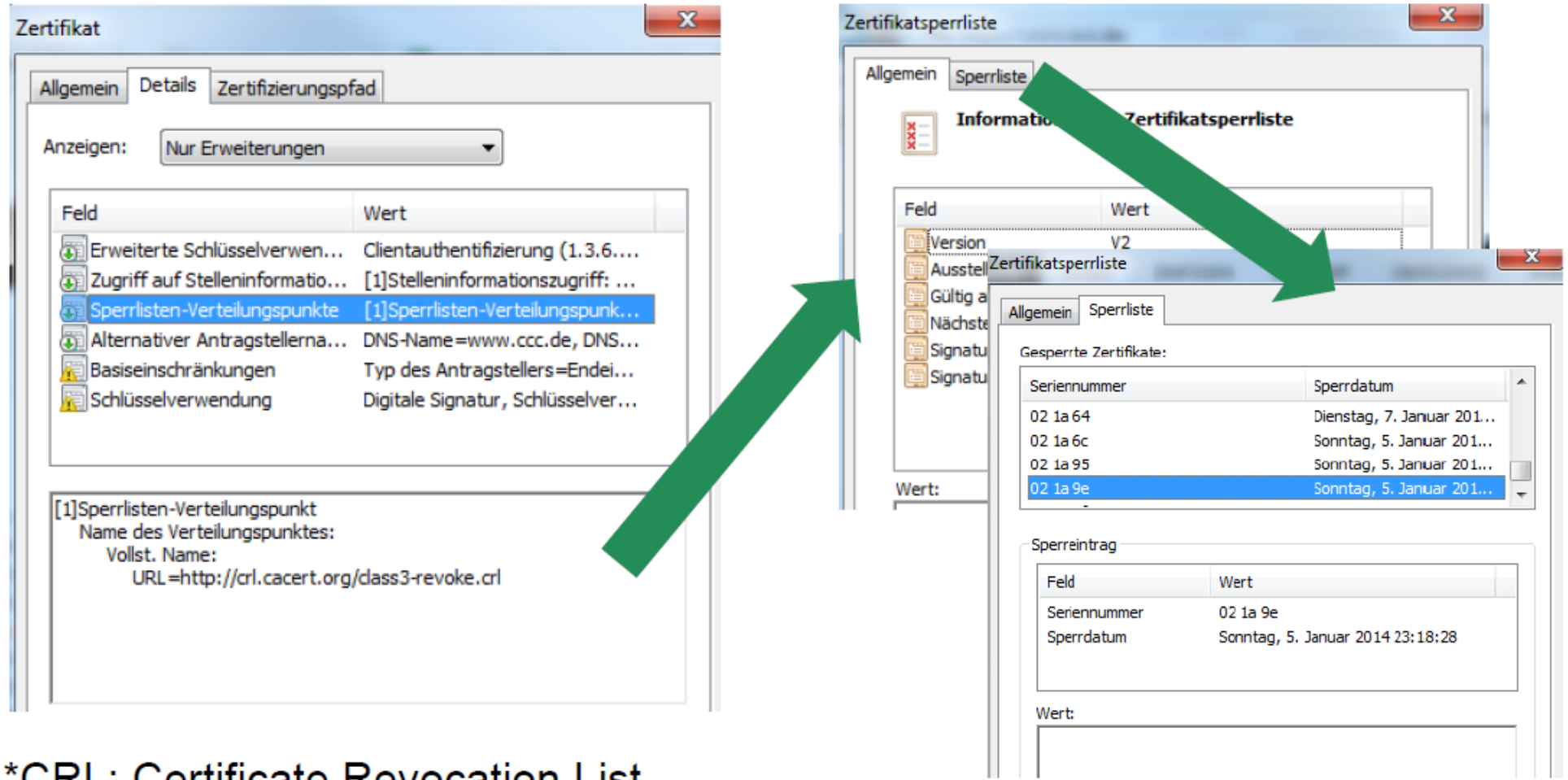


Wer kennt diese Fehlermeldung nicht….Beispiel: falscher CN

versus Wildcard Zertifikate…

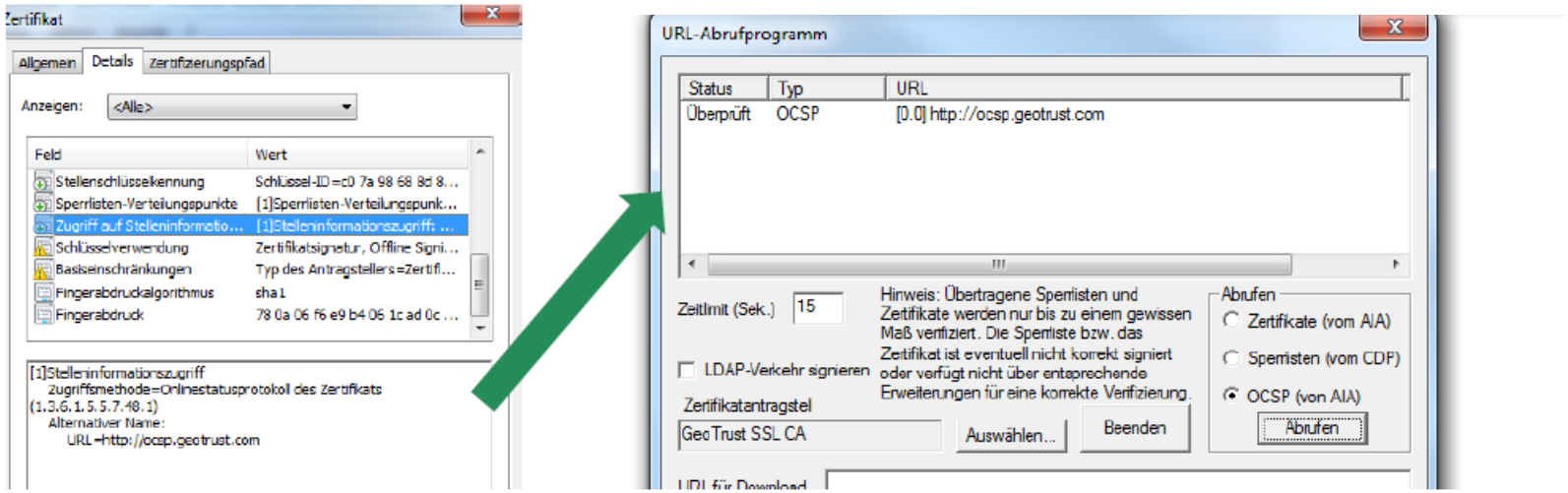


- **Widerrufslisten aka *CRL‘s – sperren von Zertifikaten**



*CRL: Certificate Revocation List

- **Widerrufslisten Problem:**
  - werden mit der Zeit relativ groß (Endgerät muss/sollte diese stets aktuell halten), bei großen CA‘s schon mal ~20MB+
  - Viele Endgeräte-Applikationen überprüfen erst gar nicht auf aktuelle Sperrlisten
  - Neuere Methode: OCSP (Online Certificate Status Protocol) CRL Echtzeitabfrage



Zeit für Ihre Fragen?

ZUVERLÄSSIGKEIT

BEGEISTERUNGSFÄHIGKEIT

BEHARRLICHKEIT

BODENHAFTUNG

Vielen Dank für die Aufmerksamkeit!

clemens.guttenberger@bechtle.com