

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





Microsoft
Direct Access

Microsoft
Exchange



BitLocker Drive Encryption

IIS

Lync 2013



APACHE
HTTP SERVER

Microsoft
Network Access Protection (NAP)

CISCO **JABBER**



VoIP

Microsoft
System Center

Mobile Device Management

Microsoft
Rights Management



...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

Feld	Wert
Seriennummer	45 cd 79 7f 86 42 cb 8d
Signaturalgorithmus	sha1RSA
Signaturhashalgorithmus	sha1
Aussteller	Shared Business CA 3, T-Syst...
Gültig ab	Donnerstag, 14. November 20...
Gültig bis	Dienstag, 15. November 2016 ...
Antragsteller	www.bechtle.de, IT, IT, becht...
Öffentlicher Schlüssel	RSA (2048 Bits)

CN = www.bechtle.de

OU = IT
OU = bechtle.com
O = Bechtle AG
C = DE

Feld	Wert
Gültig bis	Dienstag, 15. November 2016 ...
Antragsteller	www.bechtle.de, IT, IT, becht...
Öffentlicher Schlüssel	RSA (2048 Bits)
Stellenschlüsselkennung	Schlüssel-ID=92 01 43 40 b5 d...
Schlüsselkennung des Antra...	a6 18 87 63 1b d0 2d 18 d3 b9...
Erweiterte Schlüsselverwen...	Serverauthentifizierung (1.3.6...
Zertifikatrichtlinien	[1]Zertifikatrichtlinie:Richtlinie...
Basiseinschränkungen	Typ des Antragstellers=Endei...

Serverauthentifizierung (1.3.6.1.5.5.7.3.1)

• S/MIME Zertifikate

Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Schützt E-Mail-Nachrichten
- 1.3.6.1.4.1.6449.1.2.1.1.1

* Weitere Infos finden Sie in den Angaben der Zertifizierungsstelle.

Ausgestellt clemens.guttenberger@bechtle.com

Ausgestellt von: COMODO Client Authentication and Secure Email CA

Gültig ab 10. 01. 2014 **bis** 11. 01. 2015

 Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

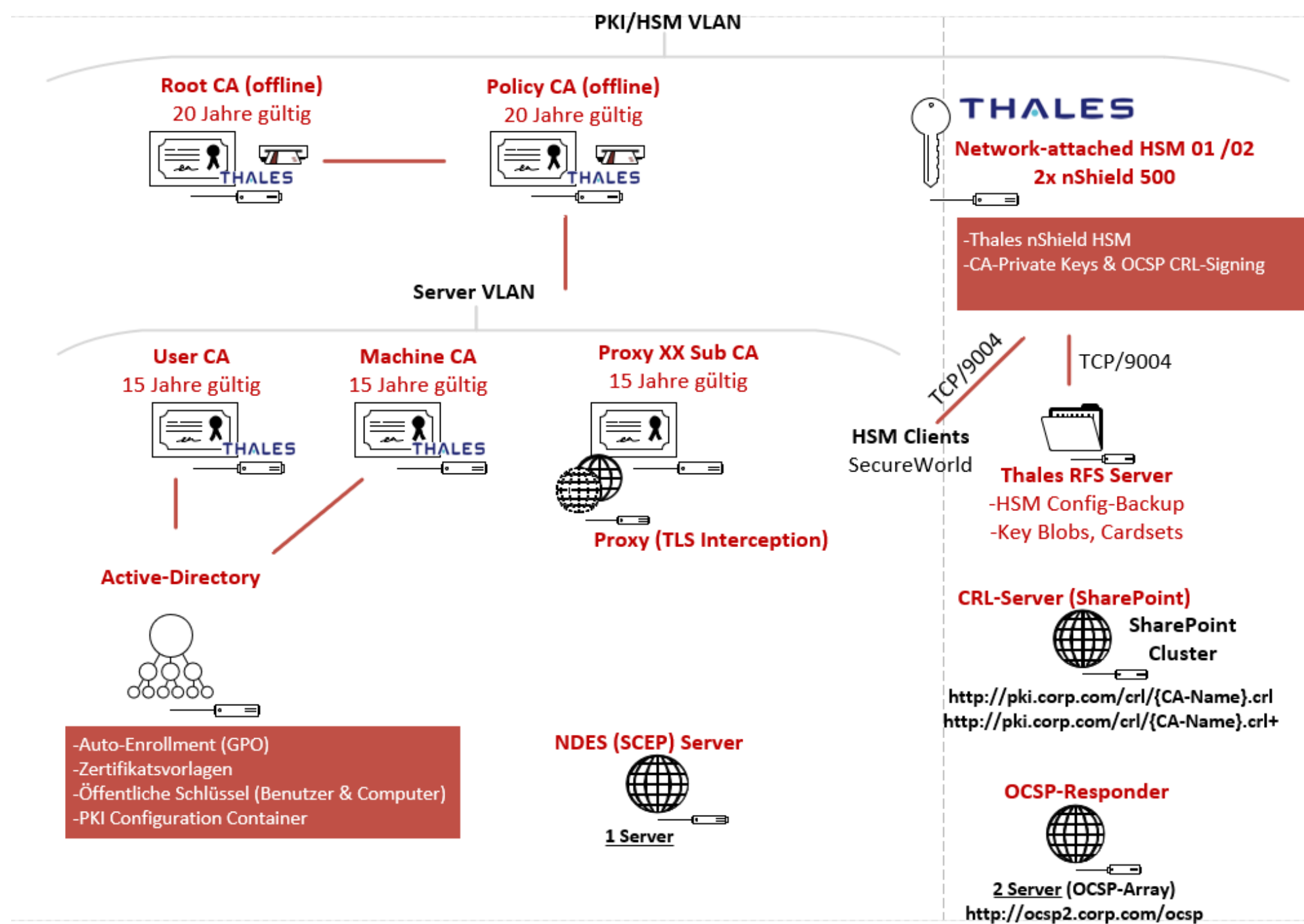
Feld	Wert
Stellenschlüsselkennung	Schlüssel-ID=7a 13 4e 00 74 5...
Schlüsselkennung des Antra...	b5 d6 36 d4 e0 44 83 02 7d 91...
Erweiterte Schlüsselverwen...	Sichere E-Mail (1.3.6.1.5.5.7...
Netscape-Zertifikattyp	SMIME (20)
Zertifikatrichtlinien	[1]Zertifikatrichtlinie:Richtlinie...
Sperrlisten-Verteilungspunkte	[1]Sperrlisten-Verteilungspunk...
Zugriff auf Stelleninformatio...	[1]Stelleninformationszugriff: ...
Alternativer Antragstellerna...	RFC822-Name=gerald.fehring

Sichere E-Mail (1.3.6.1.5.5.7.3.4)
Unbekannte Schlüsselverwendung (1.3.6.1.4.1.6449.1.3.5.2)

Feld	Wert
Erweiterte Schlüsselverwen...	Sichere E-Mail (1.3.6.1.5.5.7...
Netscape-Zertifikattyp	SMIME (20)
Zertifikatrichtlinien	[1]Zertifikatrichtlinie:Richtlinie...
Sperrlisten-Verteilungspunkte	[1]Sperrlisten-Verteilungspunk...
Zugriff auf Stelleninformatio...	[1]Stelleninformationszugriff: ...
Alternativer Antragstellerna...	RFC822-Name clemens.gut
Schlüsselverwendung	Digitale Signatur, Schlüsselver...
Basiseinschränkungen	Typ des Antragstellers=Endei

clemens.guttenberger@bechtle.com

Vollständige E-Mail Adresse

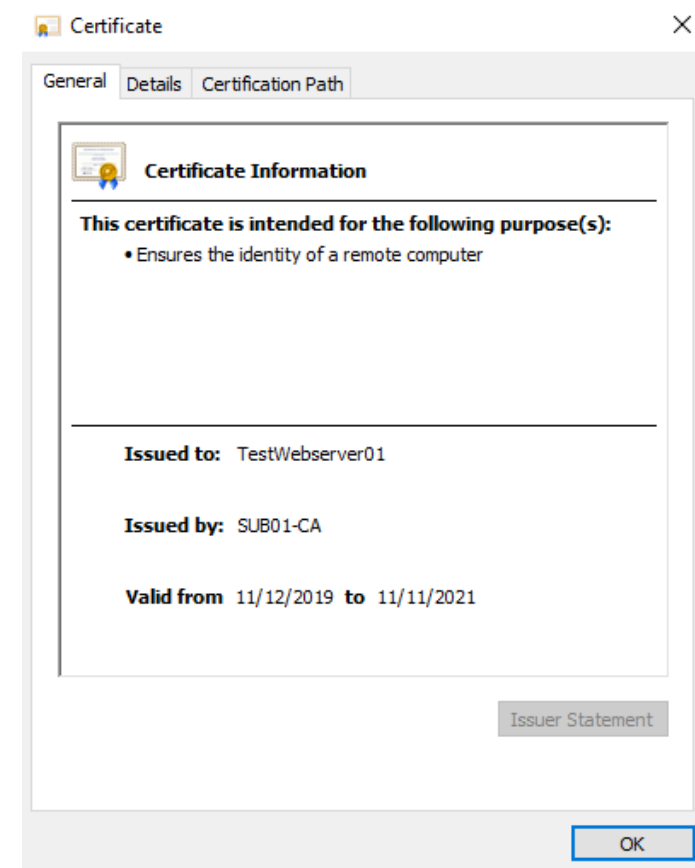


Was sind Zertifikate ?

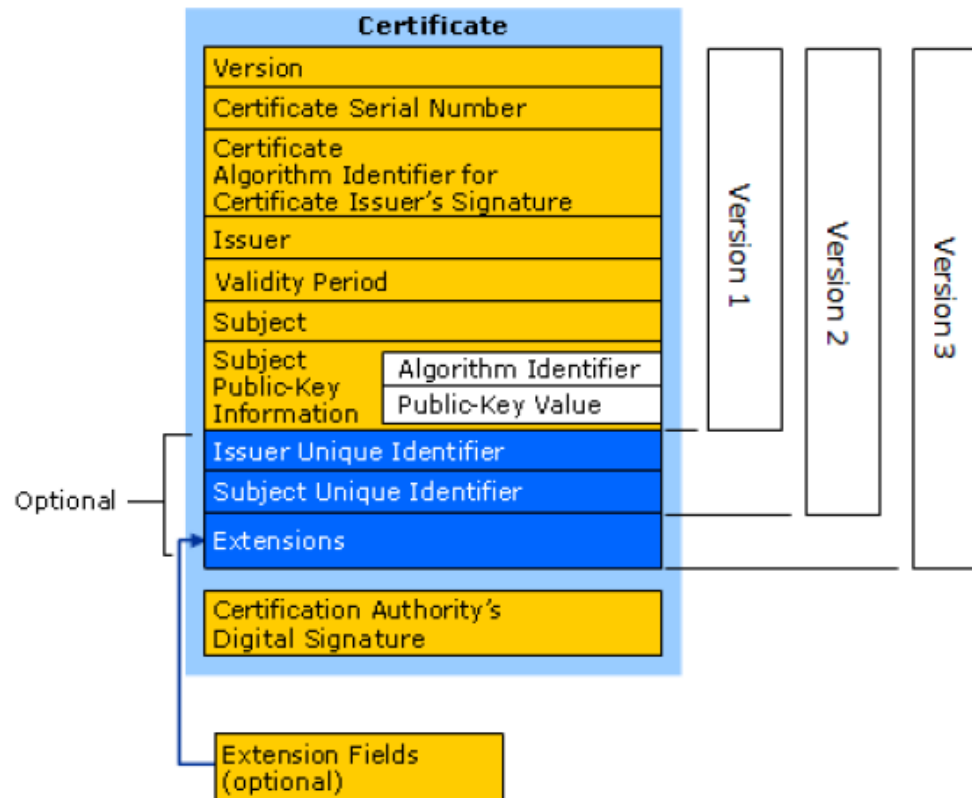
- Zertifikate bestehen aus einem öffentlichen Schlüssel und Identitätsinformationen, die durch einen Dritten mithilfe einer Signatur unterschrieben wurden
- Jeder öffentliche Schlüssel hat einen privaten Schlüssel
- Zertifikate dürfen und müssen mit einer breiten Öffentlichkeit geteilt werden, wohingegen 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

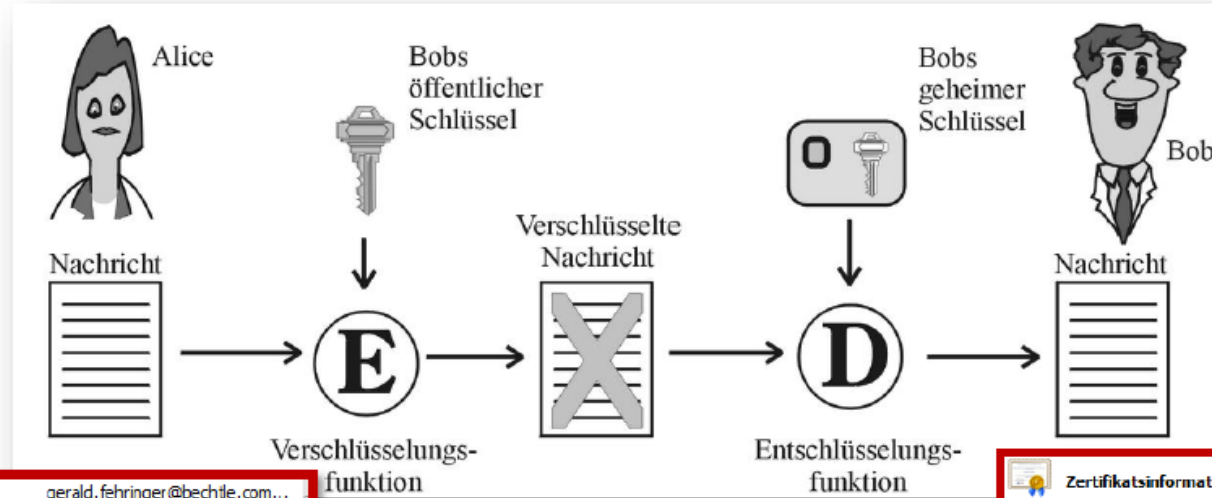
- Active-Directory Anmeldung
- MFA Token für Admins
- AD-AutoEnrollment für Computer- Zertifikate
- Smartcards
- Zertifikate für Benutzer und Code Signing
- Microsoft EFS
- Benutzerzertifikat
- TLS-/SSL- basierte Applikationen
- 802.1X (WLAN)
- Benutzer- bzw. Computerzertifikate
- Mac-OS und mobile Endgeräte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



- Zertifikate sind aktuell im X.509 V3 Standard kodiert



Public-Key Verfahren (Bsp. X509v3 Zertifikate)



Antragsteller	gerald.fehringer@bechtle.com...
Öffentlicher Schlüssel	RSA (1024 Bits)
Schlüsselverwendung	Digitale Signatur, Schlüsselver...
SMIME-Funktionen	[1]SMIME-Funktion: Objekt-ID...
Anwendungsrichtlinien	[1]Anwendungszertifikatrichtli...
Erweiterte Schlüsselverwen...	Smartcard-Anmeldung (1.3.6...
Zertifikatvorlageninformati...	Vorlage=Smartcard1.nonn (Id...

30	81	89	02	81	81	00	b7	e2	bb	20	41	72	a9
4c	a5	32	99	f12	56	89	8a	d6	07	c9	f4	fe	4c
42	ee	db	e5	3d	c2	ee	19	08	76	a4	03	35	3e
13	ac	2c	92	da	ad	e1	9d	d7	db	81	6c	0f	ae
7a	fb	b8	b4	01	48	8d	ab	9c	6a	e4	38	26	76
69	20	d0	82	9d	b7	fa	fe	ef	8c	cd	f9	71	a4
41	af	7f	21	a4	d9	c5	d4	62	26	7a	e4	9c	a1
5c	e5	32	67	86	8b	ad	8a	ee	22	a1	1c	c6	2e
0b	81	50	b2	58	f9	78	e7	36	55	7b	07	f5	ed

 **Zertifikatsinformationen**

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Garantiert dem Remotecomputer Ihre Identität
- Servercard-Anmeldung

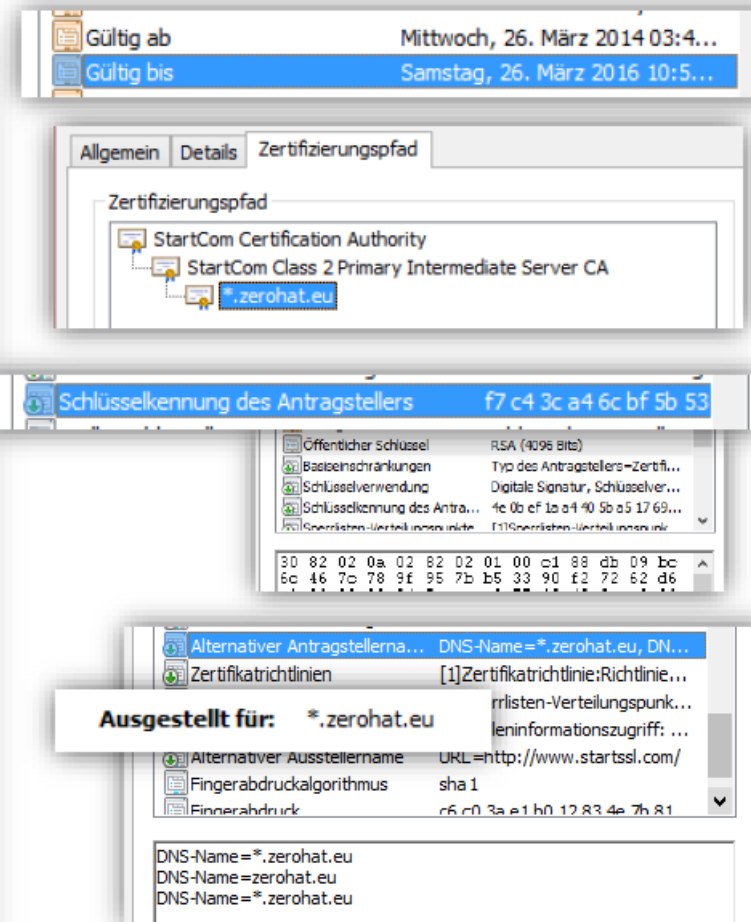
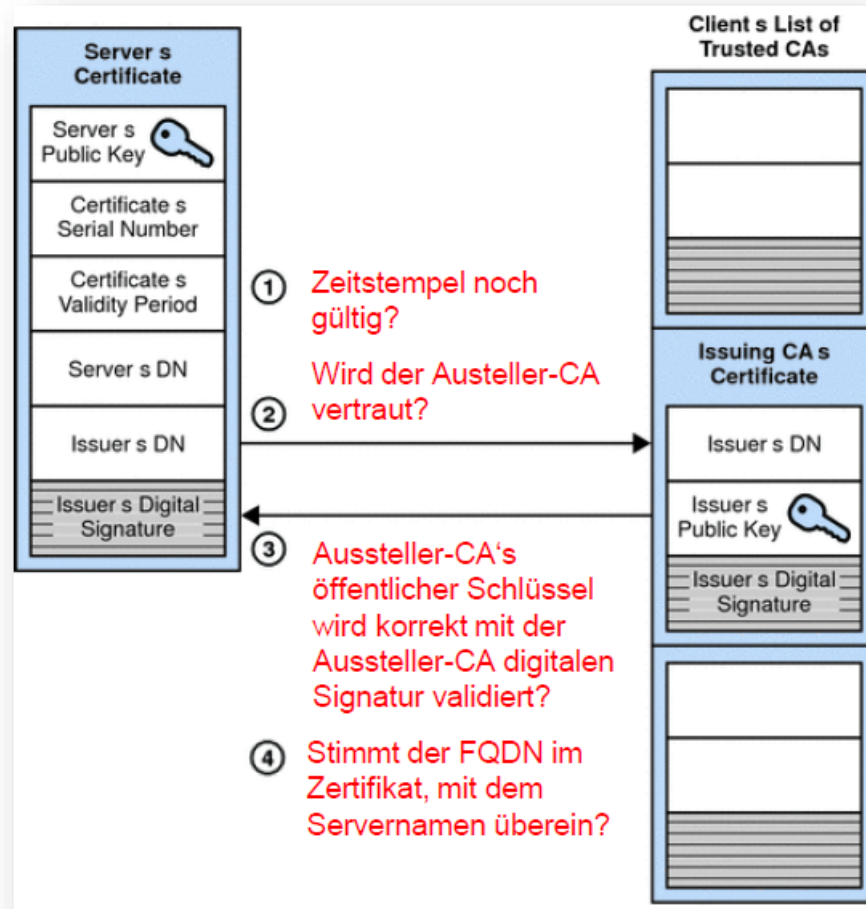
Ausgestellt für: Fehringer, Gerald

Ausgestellt von: Bedtke-CA02

Gültig ab 25. 02. 2013 **bis** 25. 02. 2015

 Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

• Zertifikatsüberprüfung Reihenfolge



Wer kennt diese Fehlermeldung nicht....



Es besteht ein Problem mit dem Sicherheitszertifikat der Website.

Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.

Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch, Daten die Sie an den Server gesendet haben abzufangen.

Es wird empfohlen, dass Sie die Webseite schließen und nicht wechseln.

- ✓ Klicken Sie hier, um diese Webseite zu schließen.
- ✗ Laden dieser Website fortsetzen (nicht empfohlen).
- 🔍 Weitere Informationen



Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!

Sie haben versucht, auf vpn.austdcl.org zuzugreifen. Der Server hat sich jedoch mit einem Zertifikat ausgewiesen, das von einem Aussteller herausgegeben wurde, dem das Betriebssystem des Computers nicht vertraut. Dies bedeutet möglicherweise, dass der Server seine eigenen Sicherheitsinformationen erzeugt hat, auf die Chrome als Identitätsangabe nicht vertrauen kann, oder dass ein Hacker versucht, Ihre Kommunikation abzufangen.

Fahren Sie nicht fort, insbesondere wenn diese Warnung für diese Website vorher noch nie erschienen ist.

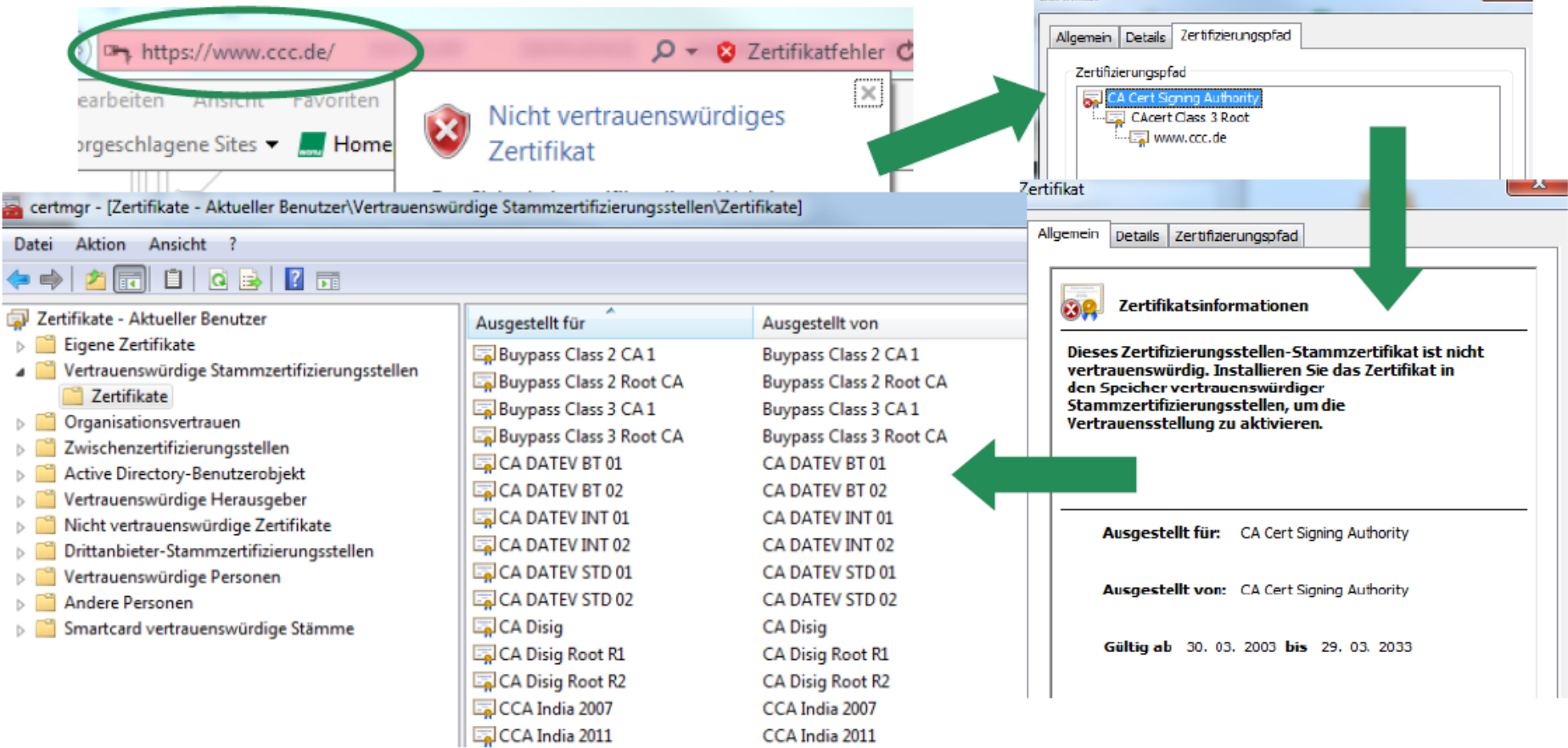
[Trotzdem fortfahren](#) [Zurück zu sicherer Website](#)

[Mehr Infos dazu](#)

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



https://www.ccc.de/

Nicht vertrauenswürdiges Zertifikat

certmgr - [Zertifikate - Aktueller Benutzer\Vertrauenswürdige Stammzertifizierungsstellen\Zertifikate]

Ausgestellt für	Ausgestellt von
Buypass Class 2 CA 1	Buypass Class 2 CA 1
Buypass Class 2 Root CA	Buypass Class 2 Root CA
Buypass Class 3 CA 1	Buypass Class 3 CA 1
Buypass Class 3 Root CA	Buypass Class 3 Root CA
CA DATEV BT 01	CA DATEV BT 01
CA DATEV BT 02	CA DATEV BT 02
CA DATEV INT 01	CA DATEV INT 01
CA DATEV INT 02	CA DATEV INT 02
CA DATEV STD 01	CA DATEV STD 01
CA DATEV STD 02	CA DATEV STD 02
CA Disig	CA Disig
CA Disig Root R1	CA Disig Root R1
CA Disig Root R2	CA Disig Root R2
CCA India 2007	CCA India 2007
CCA India 2011	CCA India 2011

Zertifikat

Algemein Details Zertifizierungspfad

Zertifizierungspfad

CA Cert Signing Authority

CAcert Class 3 Root

www.ccc.de

Zertifikatsinformationen

Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.

Ausgestellt für: CA Cert Signing Authority

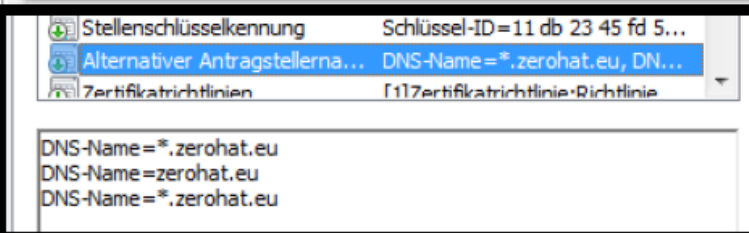
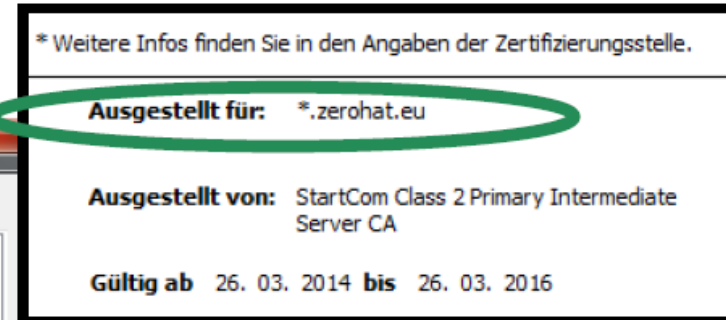
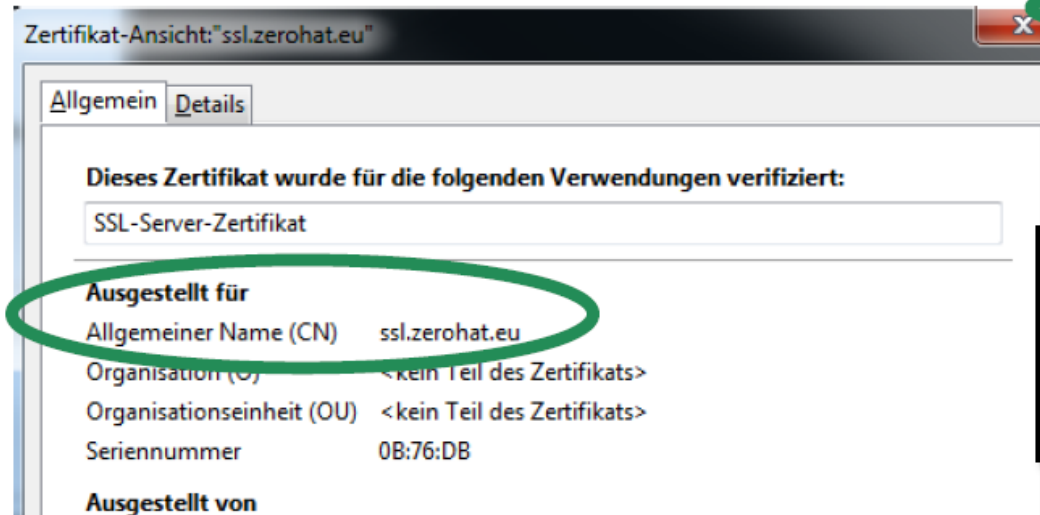
Ausgestellt von: CA Cert Signing Authority

Gültig ab: 30. 03. 2003 **bis:** 29. 03. 2033

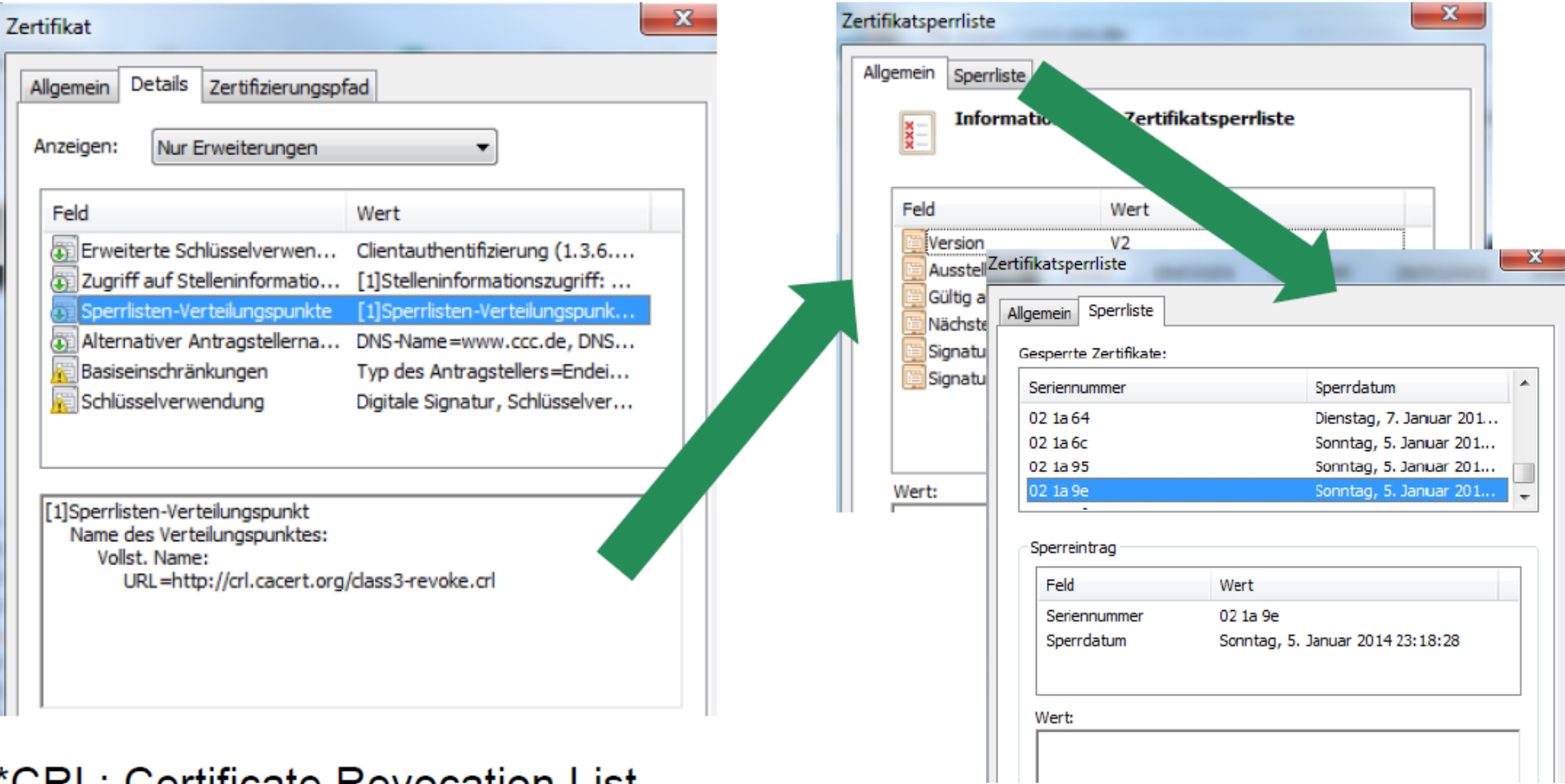
Wer kennt diese Fehlermeldung nicht....Beispiel: falscher CN



versus Wildcard Zertifikate...



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



Zertifikat

Algemein Details Zertifizierungspfad

Anzeigen: Nur Erweiterungen

Feld	Wert
Erweiterte Schlüsselverwen...	Clientauthentifizierung (1.3.6...
Zugriff auf Stelleninformatio...	[1]Stelleninformationszugriff: ...
Sperrlisten-Verteilungspunkte	[1]Sperrlisten-Verteilungspunk...
Alternativer Antragstellerna...	DNS-Name=www.ccc.de, DNS...
Basiseinschränkungen	Typ des Antragstellers=Endei...
Schlüsselverwendung	Digitale Signatur, Schlüsselver...

[1]Sperrlisten-Verteilungspunkt
Name des Verteilungspunktes:
Vollst. Name:
URL=http://crl.cacert.org/class3-revoke.crl

Zertifikatsperrliste

Algemein Sperrliste

Informationen zur Zertifikatsperrliste

Feld	Wert
Version	V2
Ausstellung	Zertifikatsperrliste
Gültig ab	
Nächstes	
Signatur	
Signatur	

Wert:

Zertifikatsperrliste

Algemein Sperrliste

Gesperrte Zertifikate:

Seriennummer	Sperrdatum
02 1a 64	Dienstag, 7. Januar 201...
02 1a 6c	Sonntag, 5. Januar 201...
02 1a 95	Sonntag, 5. Januar 201...
02 1a 9e	Sonntag, 5. Januar 201...

Sperreintrag

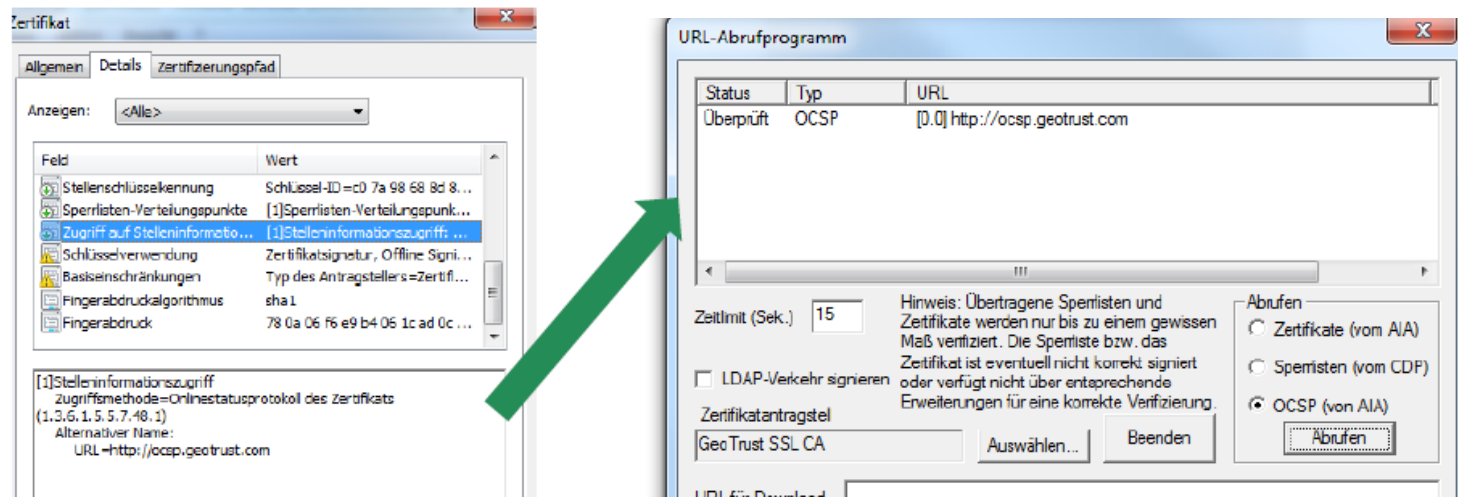
Feld	Wert
Seriennummer	02 1a 9e
Sperrdatum	Sonntag, 5. Januar 2014 23:18:28

Wert:

*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