



Root Zertifikate Offline aktualisieren

Normalerweise werden die Root-Zertifikate (Stammzertifikate), im Rahmen eines Automatismus wöchentlich aktualisiert.

Microsoft verwaltet im Rahmen des „Microsoft Trusted Root Certificate Program“ eine Repository. Aus dieser Repository laden wir die Zertifikate herunter und verpacken diese in eine sst (Serialized Certificate Store File) Datei.

Mithilfe der Commandline und dem Befehl certutil erstellen wir nun diese Offline sst Datei.

certutil.exe -generateSSTFromWU roots.sst

```
Administrator: Eingabeaufforderung
C:\temp>certutil.exe -generateSSTFromWU roots.sst
Die SST-Datei wurde aktualisiert.
CertUtil: -generateSSTFromWU-Befehl wurde erfolgreich ausgeführt.
C:\temp>
```

Importieren von Zertifikaten anhand einer vorhandenen sst Datei:

Die sst (Serialized Certificate Store File) Datei kann nun auf jeden beliebigen Computer ohne Internetzugang verteilt und importiert werden.

\$sst = (Get-ChildItem -Path C:\Temp\roots.sst)
\$sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root

```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Import SST.ps1* X
1 $sst = ( Get-ChildItem -Path C:\Temp\roots.sst )
2 $sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root

PS C:\WINDOWS\system32> $sst = ( Get-ChildItem -Path C:\Temp\roots.sst )
$sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint Subject
-----
00EA522C8A9C06AA3ECCE0B4FA6CDC21D92E8099 CN=SecureSign RootCA2, O="Japan Certification Services, Inc.", C=JP
010C0695A6981914FFB5FC6808695EA29E912A6 CN=Hellenic Academic and Research Institutions RootCA 2015, O=Hellenic Academ...
0119E81BE9A14CD8E22F40AC118C687ECBA3F4D8 CN=Microsoft Time Stamp Root Certificate Authority 2014, O=Microsoft Corporat...
016897E1A0B8F2C3B134665C20A727B7A158E28F E=info@netlock.hu, CN=NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykia...
027268293E5F5D17AAA4B3C3E6361E1F92575EAA CN=KISA RootCA 1, OU=Korea Certification Authority Central, O=KISA, C=KR
02FAF3E291435468607857694DF5E45B68851868 CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB...
039EEDB80BE7A03C6953893B20D2D9323A4C2AFD CN=GeoTrust Primary Certification Authority - G3, OU=(c) 2008 GeoTrust Inc. -...
```



Root Zertifikate Offline aktualisieren

Optional:

```
Get-Childitem cert:\LocalMachine\root | format-list
Get-Childitem cert:\LocalMachine\root | Where {$_.NotAfter -lt (Get-Date).AddDays(90)}
```

Alternative mittels einer stl Datei. Diese wird alle 2 Monate von MS aktualisiert.

Download:

<http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab>

Import per CMD:

```
certutil -addstore -f root authroot.stl
```

Import per Powershell:

```
$sst = (Get-Childitem -Path C:\Temp\roots.sst )
$sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
```

Alternative mittels einem Direktdownload der Zertifikatsdateien

Download:

```
certutil -syncWithWU -f \\DC10\roots
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>certutil -syncWithWU -f \\DC10\roots
416 Dateien wurden hinzugefügt. 0 Dateien wurden aktualisiert.
CertUtil: -syncWithWU-Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>
```

Import per CMD:

```
certutil -addstore -f disallowed \\DC10\roots\disallowedcert.sst
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>certutil -addstore -f disallowed \\DC10\roots\disallowedcert.sst
disallowed "Nicht vertrauenswürdige Zertifikate"
Das Zertifikat "Microsoft Corporation" wurde zum Speicher hinzugefügt.
Das Zertifikat "Microsoft Corporation" wurde zum Speicher hinzugefügt.
Das Zertifikat "DigiNotar PKIoverheid CA Overheid" wurde zum Speicher hinzugefügt.
Das Zertifikat "DigiNotar PKIoverheid CA Overheid en Bedrijven" wurde zum Speicher hinzugefügt.
Das Zertifikat "DigiNotar PKIoverheid CA Organisatie - G2" wurde zum Speicher hinzugefügt.
Das Zertifikat "DigiNotar Root CA" wurde zum Speicher hinzugefügt.
Verwandte Zertifikate:

Element 0:
Seriennummer: 469c2caf
Aussteller: CN=Entrust.net Secure Server Certification Authority, OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS
in corp. by ref. (limits liab.), O=Entrust.net, C=US
Nicht vor: 26.07.2007 17:57
Nicht nach: 26.08.2013 18:27
Antragsteller: E=info@diginotar.nl, CN=DigiNotar Root CA, O=DigiNotar, C=NL
Kein Stammzertifikat
Zertifikathash(sha1): 86e817c81a5ca672fe00f36f878c19518d6f844
Das Zertifikat "DigiNotar Root CA" wurde zum Speicher hinzugefügt.
```



Root Zertifikate Offline aktualisieren

Synchronisierungsquelle per GPO an offline Computer verteilen:

Die im Speicher vorhandenen Zertifikate können zuvor gesichert werden, falls man sich unsicher ist.

Konsole1 - [Konsolestamm/Zertifikate (Lokaler Computer)/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate]

Die Tabelle zeigt eine Liste von Zertifikaten mit den Spalten: Ausgestellt für, Ausgestellt von, Ablaufdatum, Beabsichtigte Zweck..., Anzeigename, Status, Zertifikatvorlage.

Die Aktion 'Exportieren...' ist ausgewählt.

Konsole1 - [Konsolestamm/Zertifikate (Lokaler Computer)/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate]

Die Dialogbox 'Zertifikatexport-Assistent' ist geöffnet. Es wird das Format für die exportierten Zertifikate ausgewählt.

Format der zu exportierenden Datei:
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- ☐ DER-codiert-binär X.509 (.CER)
- ☐ Base-64-codiert X.509 (.CER)
- ☐ Syntaxstandard kryptografischer Meldungen - PKCS #7-Zertifikate (.P7B)
 - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- ☐ Privater Informationsaustausch - PKCS #12 (.PFX)
 - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - ☐ Privaten Schlüssel nach erfolgreichem Export löschen
 - ☐ Alle erweiterten Eigenschaften exportieren
 - ☒ Zertifikatsschutz aktivieren
- ☒ Microsoft Genereller Zertifikatsspeicher (.SST)

Buttons: Weiter, Abbrechen



Root Zertifikate Offline aktualisieren

Erstellen ein neues Gruppenrichtlinienobjekt mit folgenden Einstellungen:

Aktion: Aktualisieren

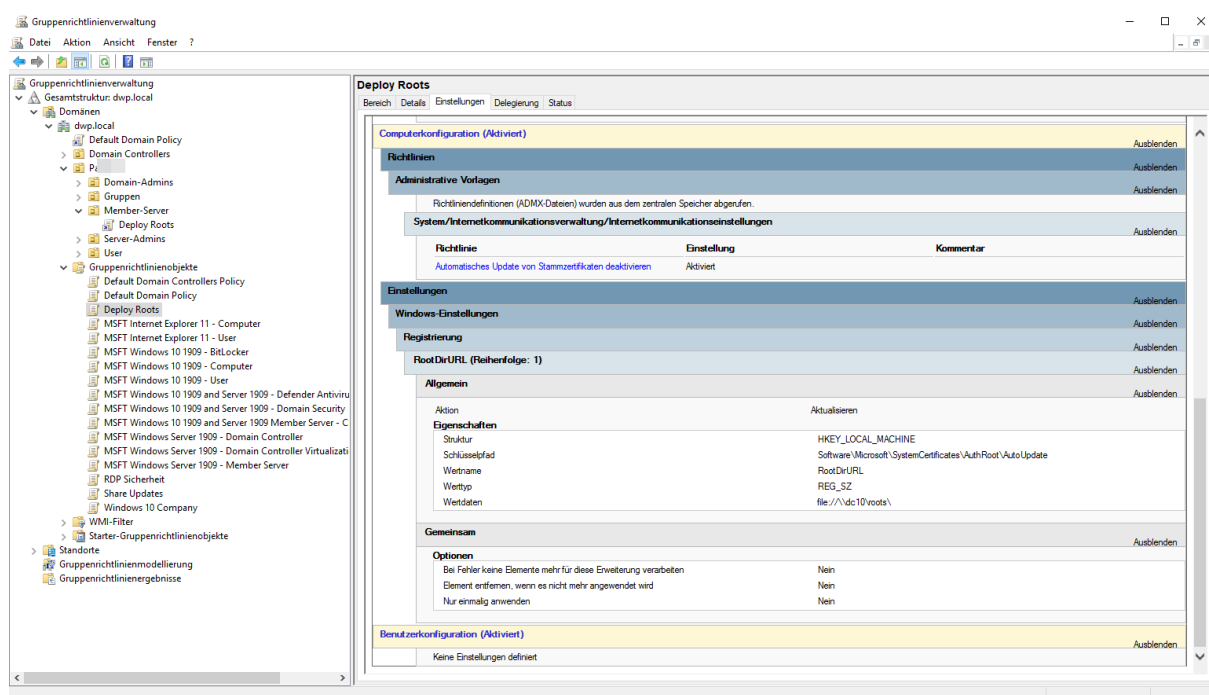
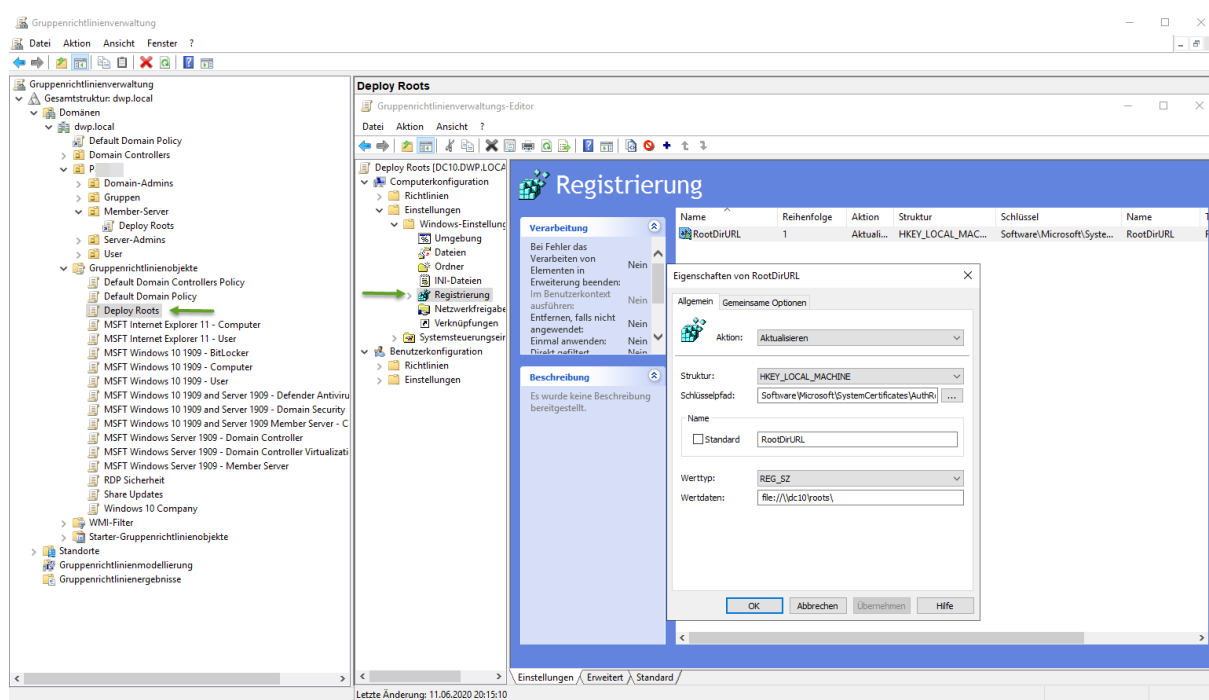
Schlüsselpfad: HKLM

Schlüsselpfad: Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate

Wertname: RootDirURL

WertTyp: REG_SZ

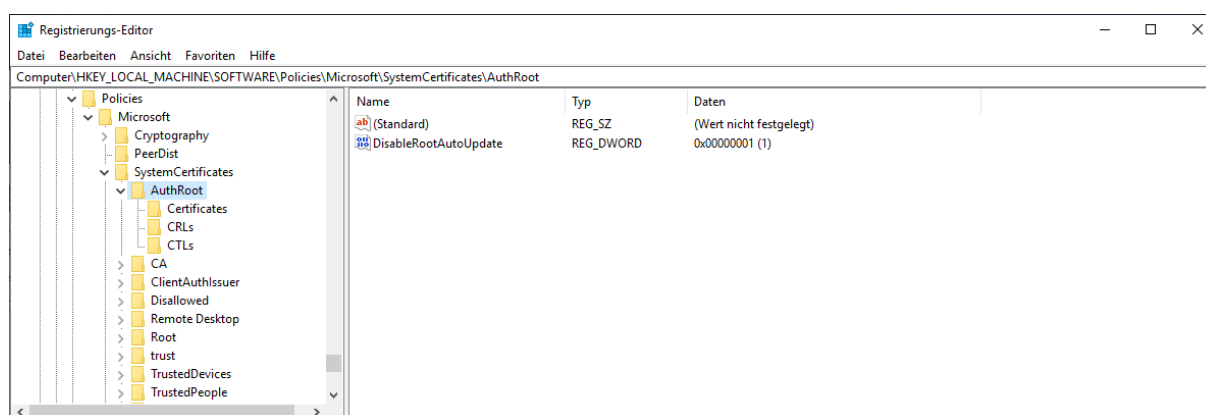
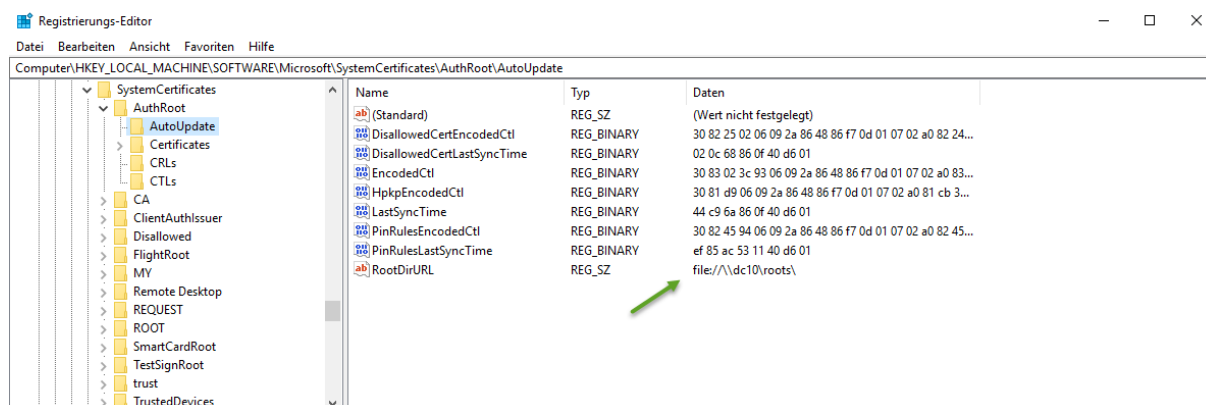
Wertdaten: file://\\DC10\roots\



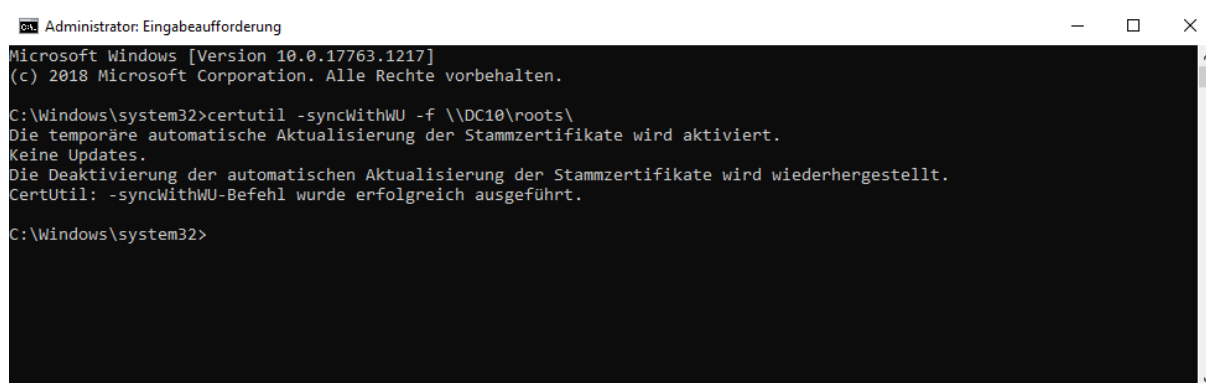


Root Zertifikate Offline aktualisieren

Nachdem die Richtlinie angewendet wurde, finden wir in der Registry den Remote-Pfad, um nach Root-Zertifikaten zu suchen sofern diese benötigt werden.



certutil -syncWithWU -f [\\DC10\roots\](#)



Registry keys	Value and Description
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate	A value of 1 disables the Windows AutoUpdate of the trusted CTL.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\EnableDisallowedCertAutoUpdate	A value of 1 enables the Windows AutoUpdate of the untrusted CTL.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\RootDirUrl	Configures the shared location (the HTTP or the FILE path).



Root Zertifikate Offline aktualisieren

Einsicht in eine sst Datei:

start explorer \\dc10\roots\roots.sst

The screenshot shows a Windows command prompt window with the command `start explorer \\dc10\roots\roots.sst` executed. Below it, the Certificate Manager (certmgr) window is open, displaying a list of certificates. The list includes columns for 'Ausgestellt für', 'Ausgestellt von', 'Ablaufdatum', 'Beabsichtigte Zweck...', and 'Anzeigenname'. The certificates are listed in a table format.

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zweck...	Anzeigenname
AAA Certificate Services	AAA Certificate Services	01.01.2029	Zeitstempel, Versch...	Sectigo (AAA)
AC Raíz Certicámara S.A.	AC Raíz Certicámara S.A.	24.05.2031	Clientauthentifizier...	AC Raíz Certicámar...
AC Raíz Certicámara S.A.	AC Raíz Certicámara S.A.	02.04.2030	Zeitstempel, Versch...	AC Raíz Certicámar...
AC RAIZ DNIE	AC RAIZ DNIE	09.02.2036	Serverauthentifizier...	DIRECCION GENER...
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01.01.2030	Serverauthentifizier...	AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01.01.2030	Serverauthentifizier...	AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM SERVIDOR...	AC RAIZ FNMT-RCM SERVIDORES...	20.12.2043	Serverauthentifizier...	AC RAIZ FNMT-RC...
AC1 RAIZ MTIN	AC1 RAIZ MTIN	03.11.2019	Serverauthentifizier...	AC1 RAIZ MTIN
ACA ROOT	ACA ROOT	27.05.2041	Serverauthentifizier...	ACA ROOT
ACCVRAIZ1	ACCVRAIZ1	31.12.2030	Serverauthentifizier...	ACCVRAIZ1
ACEDICOM Root	ACEDICOM Root	13.04.2028	Serverauthentifizier...	EDICOM
ACNLB	ACNLB	15.05.2023	Serverauthentifizier...	NLB Nova Ljubljans...
Actalis Authentication CA G1	Actalis Authentication CA G1	25.06.2022	Serverauthentifizier...	Actalis Authenticati...
Actalis Authentication Root CA	Actalis Authentication Root CA	22.09.2030	Serverauthentifizier...	Actalis Authenticati...
AddTrust External CA Root	AddTrust External CA Root	30.05.2020	Zeitstempel, Versch...	Sectigo (AddTrust)
AdminCA-CD-T01	AdminCA-CD-T01	25.01.2016	Serverauthentifizier...	BIT AdminCA-CD-...
Admin-Root-CA	Admin-Root-CA	10.11.2021	Serverauthentifizier...	BIT Admin-Root-CA
ADOCa02	ADOCa02	27.01.2019	Serverauthentifizier...	Australian Defence ...
AffirmTrust Commercial	AffirmTrust Commercial	31.12.2030	Zeitstempel, Versch...	AffirmTrust Comm...
AffirmTrust Networking	AffirmTrust Networking	31.12.2030	Zeitstempel, Versch...	AffirmTrust Networ...
AffirmTrust Premium	AffirmTrust Premium	31.12.2040	Zeitstempel, Versch...	AffirmTrust Premium

Welcher Container enthält welche Zertifikate?

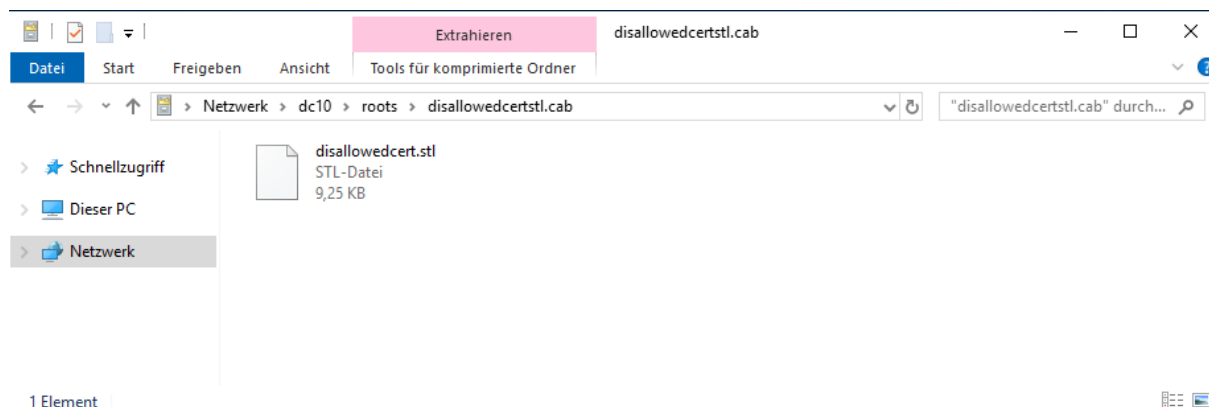
Die authrootstl.cab enthält Root-Zertifikate nur keine von Microsoft

The screenshot shows a Windows File Explorer window with the address bar set to `Netzwerk > dc10 > roots > authrootstl.cab`. The file `authrootstl.cab` is selected, and its details are shown: `authrootstl`, `STL-Datei`, `143 KB`. The left sidebar shows the 'Netzwerk' view.



Root Zertifikate Offline aktualisieren

Die disallowedcertstl.cab enthält eine CTL mit nicht vertrauenswürdigen Zertifikaten



Die disallowedcert.sst enthält nicht vertrauenswürdige Zertifikate

