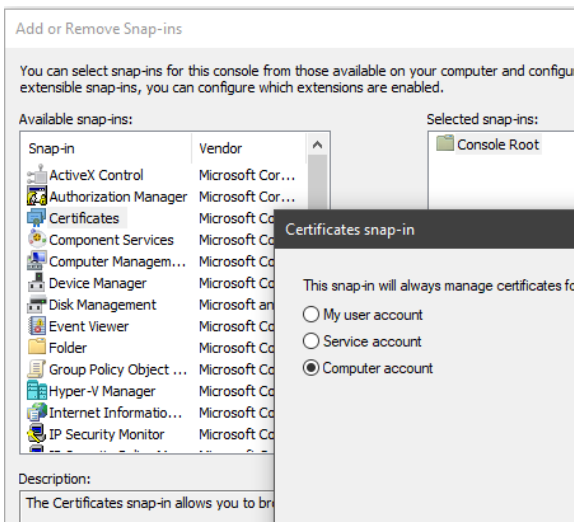
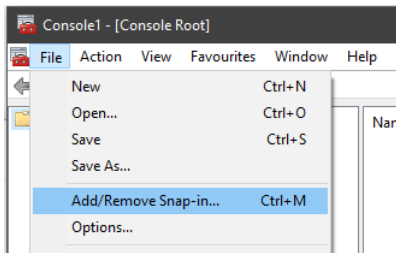
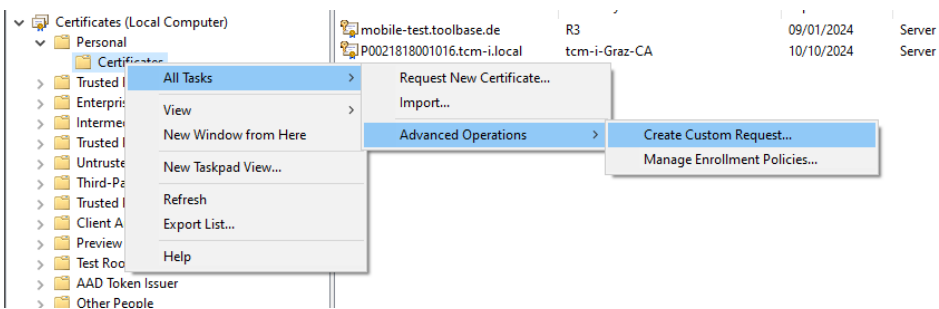


Open the Microsoft management console on the ATMS CORE NET Server


Add a Snap-in Certificate (Local Computer).



All Tasks – Advanced Operations – Create Custom Request



Continue without enrollment policy

 Certificate Enrollment

### Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator
Active Directory Enrollment Policy <span>▼</span>

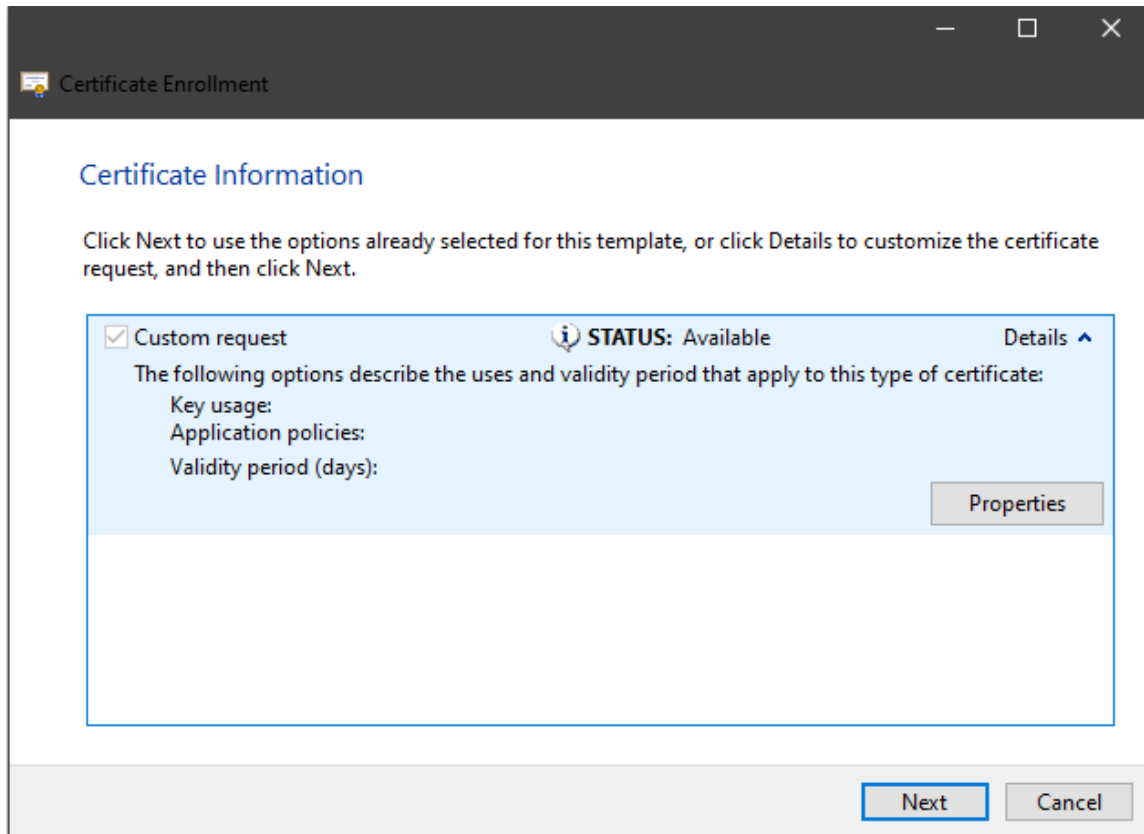
**Configured by you** Add New

**Custom Request**

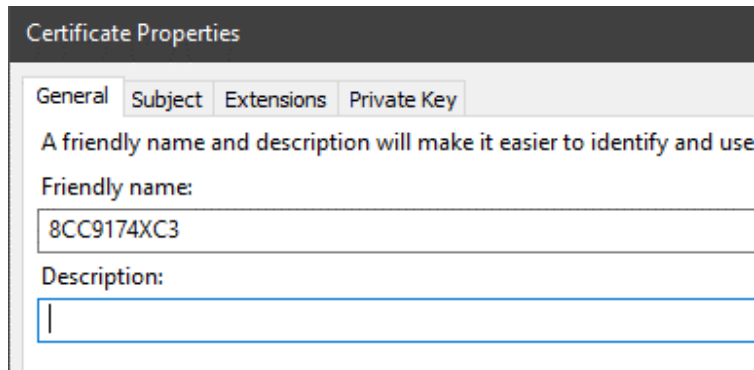
Proceed without enrollment policy
-----------------------------------

Next Cancel

Properties



Enter the PC name



Certificate Properties

General Subject Extensions Private Key

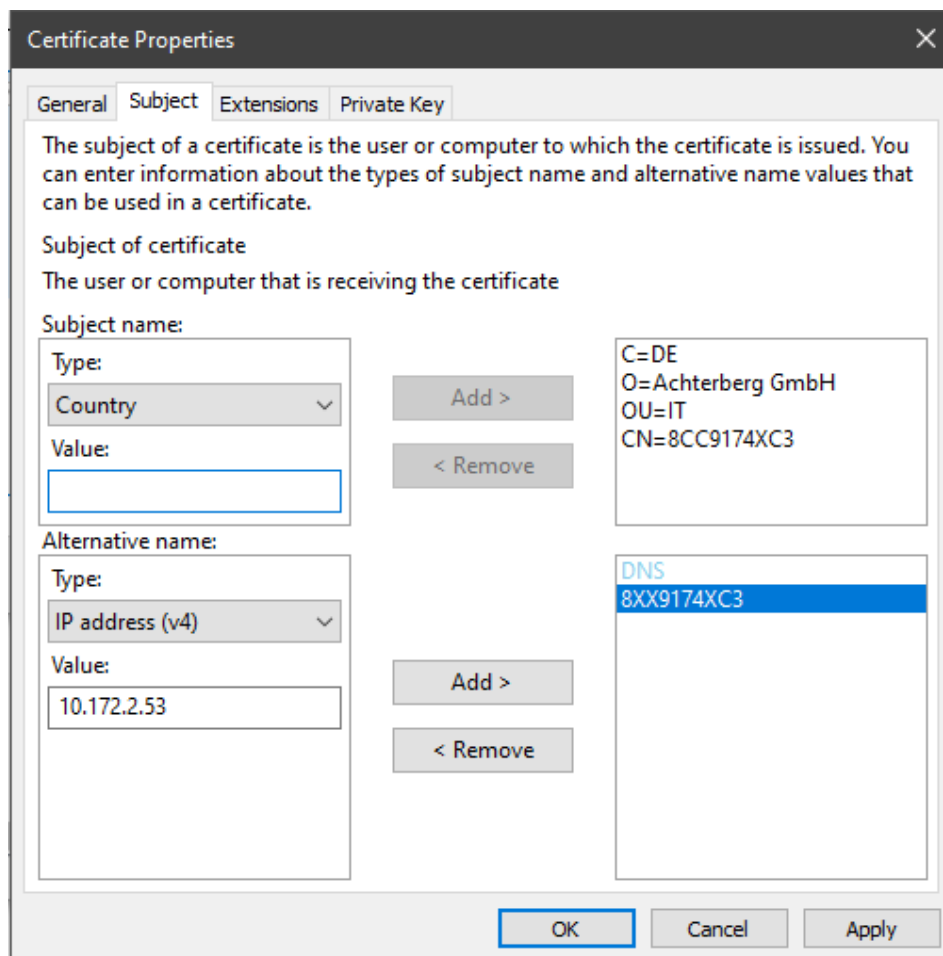
A friendly name and description will make it easier to identify and use

Friendly name:  
8CC9174XC3

Description:  
|

Enter Subject Information.

**Especially important: Alternative name!** In this case enter, Host (DNS Value) and IPv4 (IP Value).



Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate  
The user or computer that is receiving the certificate

Subject name:

Type: Country  
Value:

Add >  
< Remove

C=DE  
O=Achterberg GmbH  
OU=IT  
CN=8CC9174XC3

Alternative name:

Type: IP address (v4)  
Value: 10.172.2.53

Add >  
< Remove

DNS  
8XX9174XC3

OK Cancel Apply

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate  
The user or computer that is receiving the certificate

Subject name:

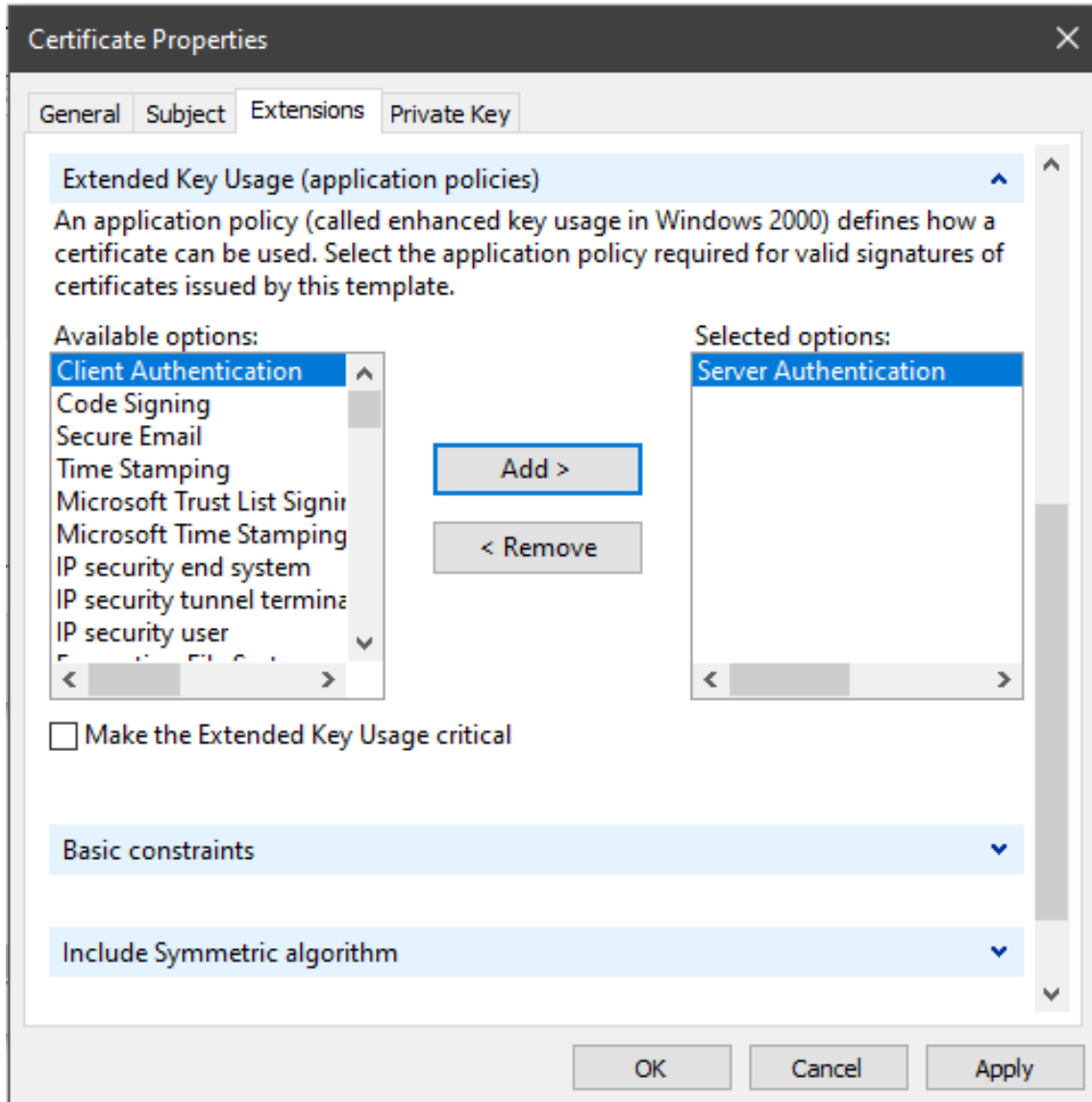
Type: Country	Add >	C=DE O=Achterberg GmbH OU=IT CN=8CC9174XC3
Value: <input type="text"/>	< Remove	

Alternative name:

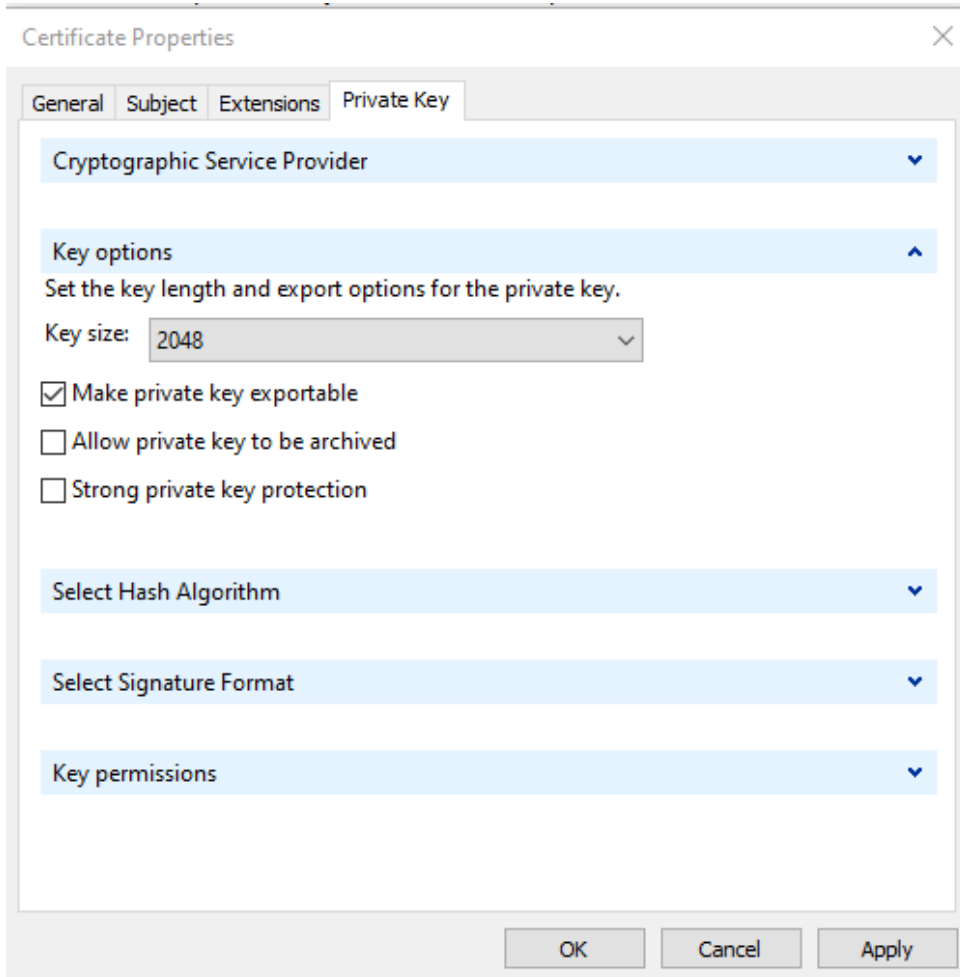
Type: IP address (v4)	Add >	DNS 8XX9174XC3 IP address (v4) 10.172.2.53
Value: <input type="text"/>	< Remove	

OK Cancel Apply

Extensions – Extended Key Usage – Server Authentication



Private Key – make exportable (allows the transfer of the key) Key size at least 2048.



The image shows a screenshot of the 'Certificate Properties' dialog box, specifically the 'Private Key' tab. The dialog has a title bar with 'Certificate Properties' and a close button. Below the title bar are four tabs: 'General', 'Subject', 'Extensions', and 'Private Key'. The 'Private Key' tab is selected and contains the following elements:

- 'Cryptographic Service Provider' dropdown menu.
- 'Key options' section with a sub-header 'Set the key length and export options for the private key.' and a 'Key size' dropdown menu set to '2048'.
- Three checkboxes: 'Make private key exportable' (checked), 'Allow private key to be archived' (unchecked), and 'Strong private key protection' (unchecked).
- 'Select Hash Algorithm' dropdown menu.
- 'Select Signature Format' dropdown menu.
- 'Key permissions' dropdown menu.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Save the properties.



Certificate Enrollment

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:  
C:\AdminOnly\8CC9174XC3 Browse...

File format:  
 Base 64  
 Binary

Finish Cancel





Open the file with notepad and copy the text.

```
1 -----BEGIN NEW CERTIFICATE REQUEST-----
2 MIID4TCCAskCAQAwSTETMBEGA1UEAwwKOENDOTE3NFhDMzELMAkGA1UECwwCSVQx
3 GDAWBgNVBAoMD0FjaHRlcmJlcmcgR2liSDELMakGA1UEBhMCREUwggEiMA0GCSqG
4 SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCi+TJ+JojC+aF3uX4yYw8UqRmj3LbNGe+1
5 93Dk8OPIXSOSCLnOUjC6+ApPRu4NM6xMB3jnqj7zBleKPwXov003mza0PIGWF/hH
6 760qwFr02eaHnoU8/Fuu+zCtvFq2XSnhN4vh6AjduNuALvrHa3g4eTNT/GwQKW7Q
7 5OV6pkUJV9eMsNOTxx211JQ/dj4qMh4UsthgwwRwhurI//lcN04DJ0SmgiAmn95C
8 JCVa28ajqmbzjrZwr8uVvbo7qM+Z+ijIUny8PlAS7XD/qdWuQohB5i2fRqtAiI7h
9 5P+xZ3SkgwKNHLeFAGRmyNqJ5uF8u5TpRbUh3lhhgy10tn+vRjQtAgMBAAQgggFR
10 MBwGCisGAQQBgjcNAgMxMhYMTAuMC4xOTA0NS4yMEoGCSsGAQQBgjcVFDE9MDSG
11 AQUMG1AwMDIxODE4MDAxMDE2LnRjbSlpLmxvY2FsDBFUQ00tSVxrc29tbWVyZmVs
12 ZAwHTU1DLkVYRTBmBgorBgEEAYI3DQICMVGwVgIBAB5OAE0AaQBjAHIAbwBzAG8A
13 ZgB0ACAAUwBvAGYAdAB3AGEAcgBlACAASwBlAHkAIABTAHQAbwByAGEAZwBlACAA
14 UABYAG8AdgBpAGQAZQByAwEAMHOGCSqGSIb3DQEJJDjFwMG4wGwYDVR0RBQwEoIK
15 OFhYOTE3NFhDM4cECqCNTATBgNVHSUEDDAKBggrBgEFBQCcDATAAbGkrBgEEAYI3
16 FQoEDjAMMAoGCCsGAQUFBwMBMB0GA1UdDgQWBSE1T9tQihsRj+o6MgsCx37ux4p
17 5DANBgkqhkiG9w0BAQsFAAOCAQEAEEDPaARLdQunliijR2SlmTAGzEcMxpvcEie6+
18 3eQMeEdg0dpgjvF5jkiVFkd1xUHWslclHhZiTPOinj6PXkC5K0e2HMCW9Zu5WNSI
19 blczlMXPONputOLOorsVlojxwSomB9P12yladWRoqgkdkmjO3f9EnQmZ7UfTv3BE
20 LNfzAsBwQ4NcNvwIbo89qjUqneiGnlPH6VHKcDwoE7Q/Z688copsA5DIJeAzapKc
21 Q/4XpL2w5RfLURRCnOpdqBazb2WjNpSJtj5mmB4GpdZa+wByyt/88VQ0PBI7SzT+
22 qA6DQAXHamKfF/MVudolwG8RZTs3/oqdyuR7B0Jkdmv68GW2CA==
23 -----END NEW CERTIFICATE REQUEST-----
24
```



Open the web application with a browser on the certification authority server.

A screenshot of a web browser window. The address bar shows "localhost/certsrv/". The page title is "Microsoft Active Directory-Zertifikatdienste - tcm-i-Graz-CA". The main content area has a heading "Willkommen" followed by introductory text about certificates. Below this, there is a section titled "Wählen Sie eine Aufgabe:" with three links: "Ein Zertifikat anfordern" (highlighted with a red box and a red arrow), "Status ausstehender Zertifikate anzeigen", and "Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste".

← localhost/certsrv/

Microsoft Active Directory-Zertifikatdienste – tcm-i-Graz-CA

### Willkommen

Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Programme anfordern. Mit einem Zertifikat können Sie das Web kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sicherheitsaufgaben, abhängig von den Einstellungen Ihres Computers, ausführen.

Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatsspeicherung anzeigen.

Weitere Informationen zu Active Directory-Zertifikatdiensten erhalten Sie unter [Active Directory-Zertifikatdienstedokumentation](#).

**Wählen Sie eine Aufgabe:**

- [Ein Zertifikat anfordern](#)
- [Status ausstehender Zertifikate anzeigen](#)
- [Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste](#)

Paste text from clipboard into the saved request field.

Chose „Web Server“

localhost/certsrv/certrqxt.asp

**Microsoft Active Directory-Zertifikatdienste – tcm-i-Graz-CA**

### Zertifikat- oder Erneuerungsanforderung einreichen

Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanforderung c Feld "Gespeicherte Anforderung" ein, um eine gespeicherte Anforderung bei de

**Gespeicherte Anforderung:**

Base-64-codierte Zertifikatanforderung (CMC oder PKCS #10 oder PKCS #7):

```

91BHc9HP2xyqfIpi6bgjdXsVT8vzVzf/vSyAyN8r
T7oYerI2bWVZO/kdMNv7AFJAtLcgTIqyX6li6wXIc
h9B8AtVvNmuRvCxz2L3kAJKMa0Ji0qqV77JhpV5Ug
6MBwUcqssZ7Zr/gmwNKQwawhzWg=
-----END NEW CERTIFICATE REQUEST-----

```

**Zertifikatvorlage:**

Webserver

**Zusätzliche Attribute:**

Attribute:

Einsenden >

Send in.

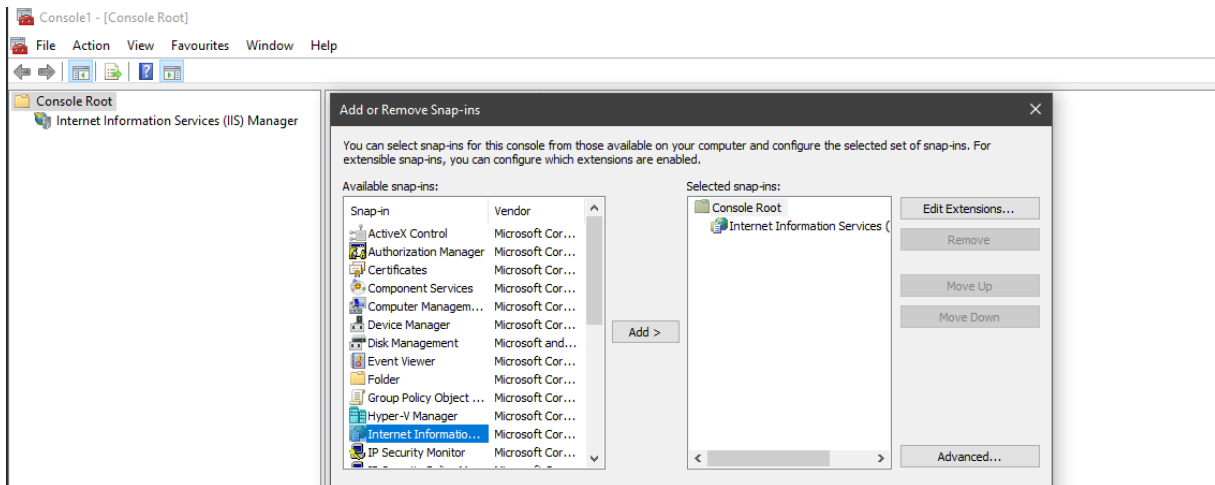
Download the certificate. Recommended as Base 64 coded.

Transfer the .cer file to the ATMS CORE NET Server.

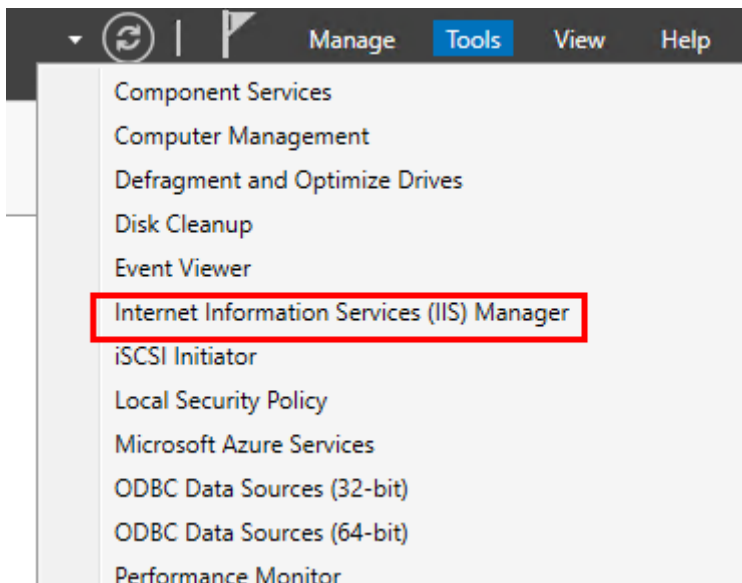
Name	Änderungsdatum	Typ	Größe
8CC9174XC3.cer	04.10.2023 13:04	Sicherheitszertifikat	2 KB
8CC9174XC3.req	04.10.2023 13:02	REQ-Datei	2 KB
root-ca.cer	19.01.2023 15:06	Sicherheitszertifikat	2 KB

Client Operating System:

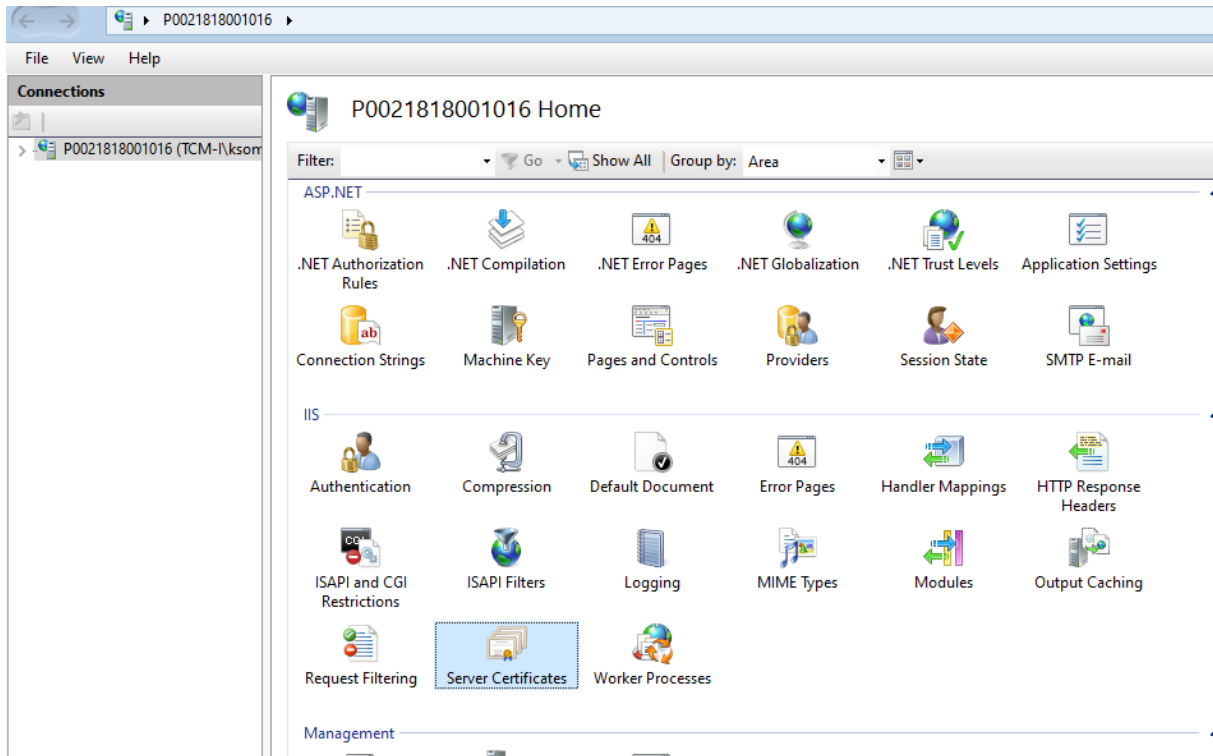
Add IIS administration snap-in to mmc.



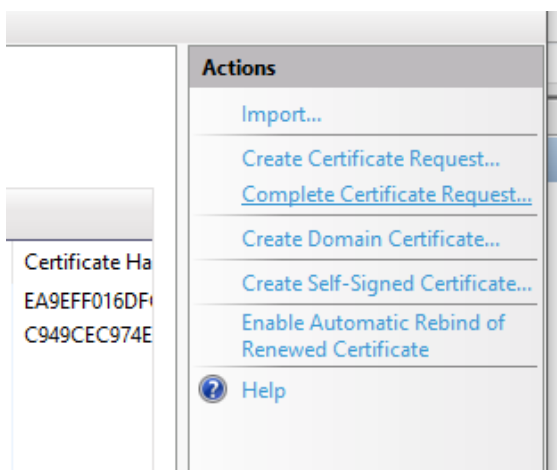
Server Operating System: Open this entry in the server manager.




## Open Server certificates



## Complete Certificate Request...



Complete Certificate Request

 **Specify Certificate Authority Response**

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

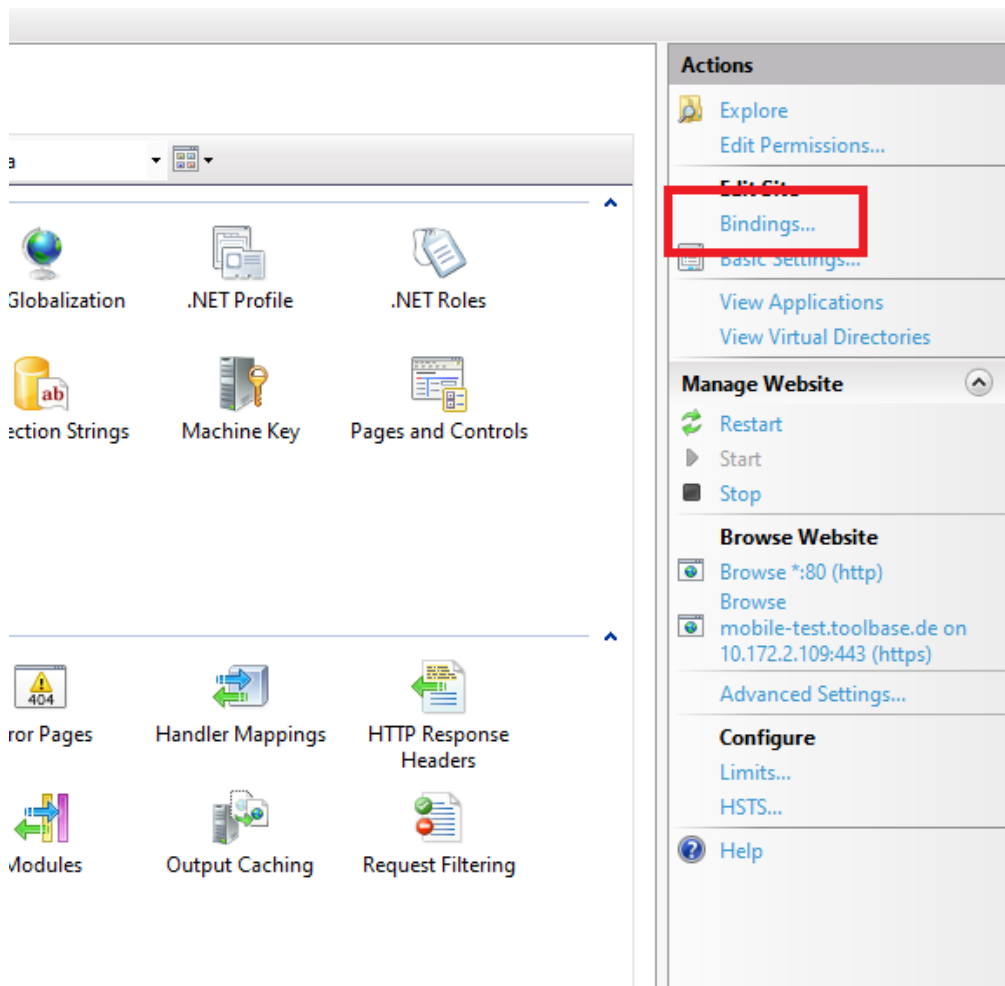
...

Friendly name:

Select a certificate store for the new certificate:

▾

OK Cancel



The screenshot shows the IIS Manager console. The main area displays various configuration options for the selected website, including Globalization, .NET Profile, .NET Roles, Action Strings, Machine Key, Pages and Controls, Error Pages, Handler Mappings, HTTP Response Headers, Modules, Output Caching, and Request Filtering. On the right side, the Actions pane is visible, containing options like Explore, Edit Permissions..., Edit Site, Bindings..., Basic Settings..., View Applications, and View Virtual Directories. The Bindings... option is highlighted with a red rectangle. Below the Actions pane, the Manage Website section includes Restart, Start, and Stop buttons. The Browse Website section shows links to Browse \*:80 (http) and Browse mobile-test.toolbase.de on 10.172.2.109:443 (https). The Configure section includes Limits... and HSTS... options, and a Help link is at the bottom.

**Add Site Binding**

Type: **https** IP address: **10.172.2.53** Port: **443**

Host name:

Require Server Name Indication

Disable TLS 1.3 over TCP       Disable QUIC

Disable Legacy TLS       Disable HTTP/2

Disable OCSP Stapling

SSL certificate:  
**ATMS.CORE.NET TCM CA**



## Export Root CA:

At the certification authority server with web application

Microsoft-Active Directory-Zertifikatdienste — tcm-i-Graz-CA

---

**Willkommen**

Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Programme anfordern. Mit einem Zertifikat können Sie Ihre das Web kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sicherheitsaufgaben, abhängig vom angeforderten

Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatssperrliste verwenden, od anzeigen.

Weitere Informationen zu Active Directory-Zertifikatdienste erhalten Sie unter [Active Directory-Zertifikatdienstedokumentation](#).

**Wählen Sie eine Aufgabe:**

- [Ein Zertifikat anfordern](#)
- [Status ausstehender Zertifikate anzeigen](#)
- [Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste](#)

Microsoft-Active Directory-Zertifikatdienste — tcm-i-Graz-CA

---

**Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatssperrliste**

[installieren Sie dieses Zertifizierungsstellenzertifikat](#), damit von dieser Zertifizierungsstelle ausgestellten Zertifikaten vertraut werden kann.

Wählen Sie das Zertifikat und die Codierungsmethode für den Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste aus.

**Zertifizierungsstellenzertifikat:**

Aktuelles [tcm-i-Graz-CA]

**Codierungsmethode:**

DER

Base 64

[Zertifizierungsstellenzertifikat installieren](#)

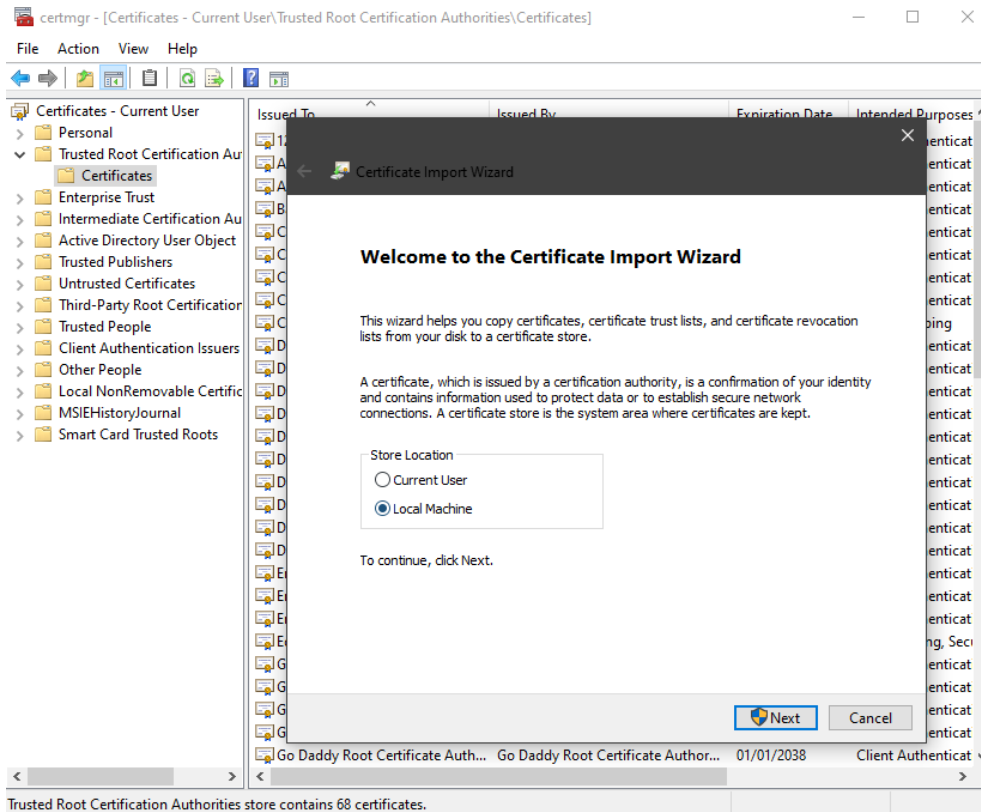
[Download des Zertifizierungsstellenzertifikats](#) ←

[Download der Zertifizierungsstellen-Zertifikatkette](#)

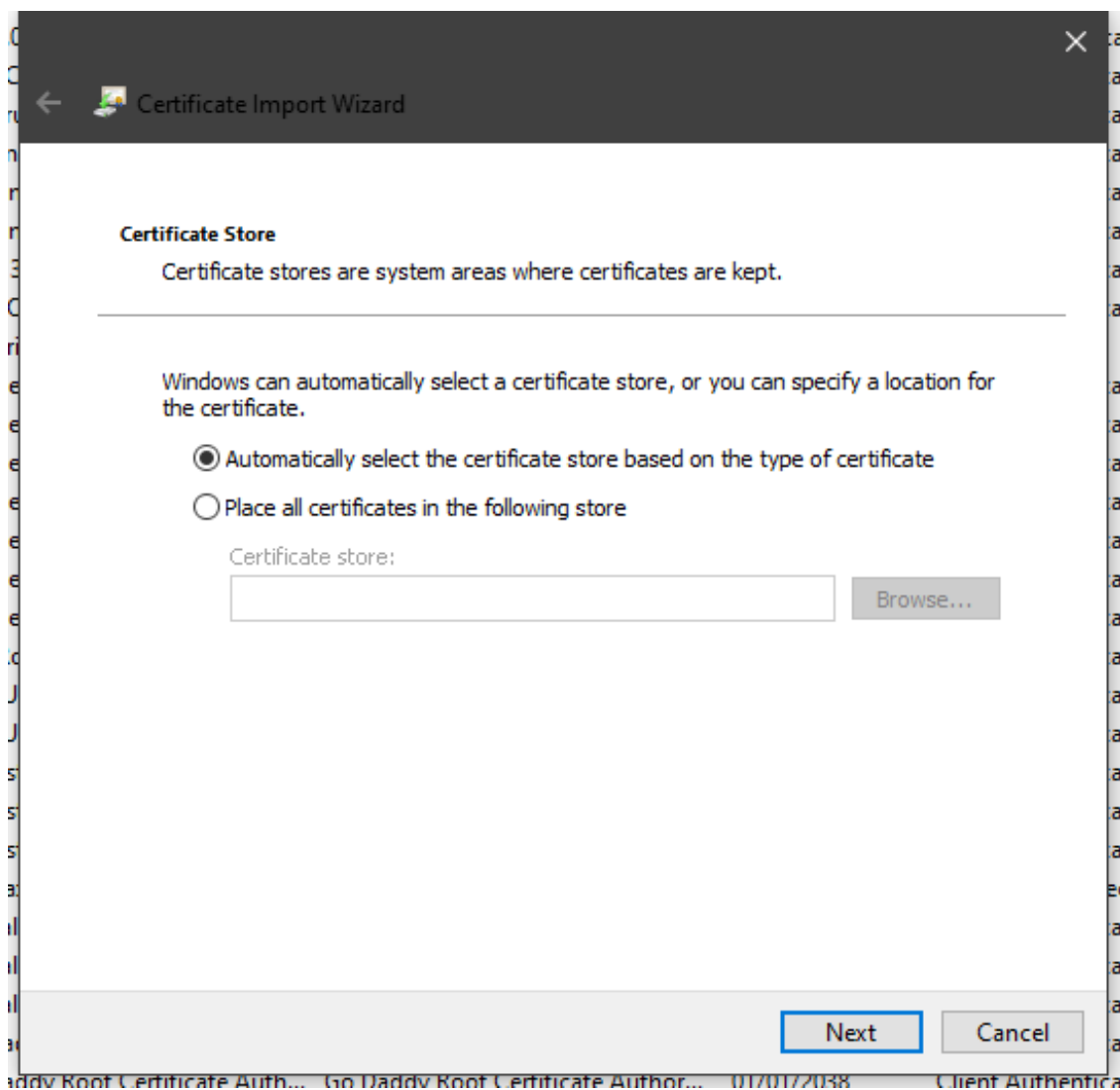
[Download der aktuellen Basisperrliste](#)

[Download der aktuellen Deltasperrliste](#)

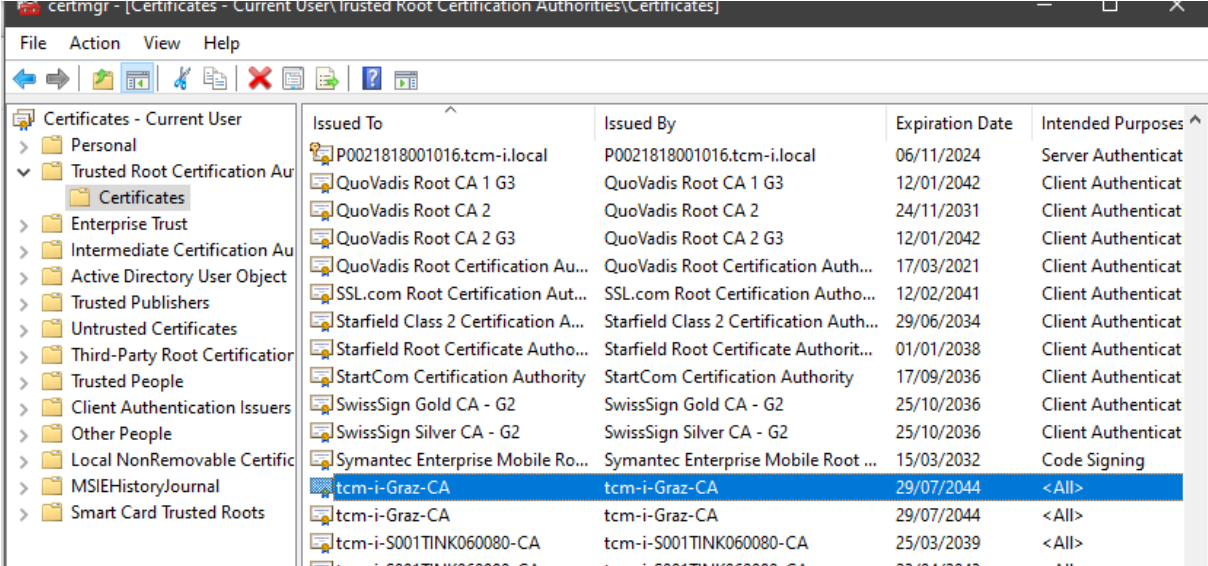
Import root CA on ATMS CORE NET Server:  
 mmc Certificates (Local Computer)



Name	Änderungsdatum	Typ	Größe
8CC9174XC3.cer	04.10.2023 13:04	Sicherheitszertifikat	2 KB
8CC9174XC3.req	04.10.2023 13:02	REQ-Datei	2 KB
root-ca.cer	19.01.2023 15:06	Sicherheitszertifikat	2 KB



Check if the import was successful.



Issued To	Issued By	Expiration Date	Intended Purposes
P0021818001016.tcm-i.local	P0021818001016.tcm-i.local	06/11/2024	Server Authenticat
QuoVadis Root CA 1 G3	QuoVadis Root CA 1 G3	12/01/2042	Client Authenticat
QuoVadis Root CA 2	QuoVadis Root CA 2	24/11/2031	Client Authenticat
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	12/01/2042	Client Authenticat
QuoVadis Root Certification Au...	QuoVadis Root Certification Auth...	17/03/2021	Client Authenticat
SSL.com Root Certification Aut...	SSL.com Root Certification Autho...	12/02/2041	Client Authenticat
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	29/06/2034	Client Authenticat
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	01/01/2038	Client Authenticat
StartCom Certification Authority	StartCom Certification Authority	17/09/2036	Client Authenticat
SwissSign Gold CA - G2	SwissSign Gold CA - G2	25/10/2036	Client Authenticat
SwissSign Silver CA - G2	SwissSign Silver CA - G2	25/10/2036	Client Authenticat
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15/03/2032	Code Signing
tcm-i-Graz-CA	tcm-i-Graz-CA	29/07/2044	<All>
tcm-i-Graz-CA	tcm-i-Graz-CA	29/07/2044	<All>
tcm-i-S001TINK060080-CA	tcm-i-S001TINK060080-CA	25/03/2039	<All>

Test the Website on the ATMS CORE NET Server:

There mustn't be a warning.

