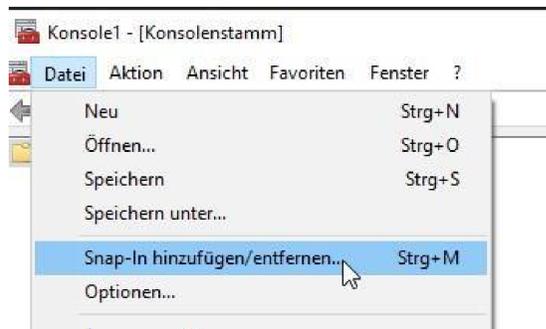
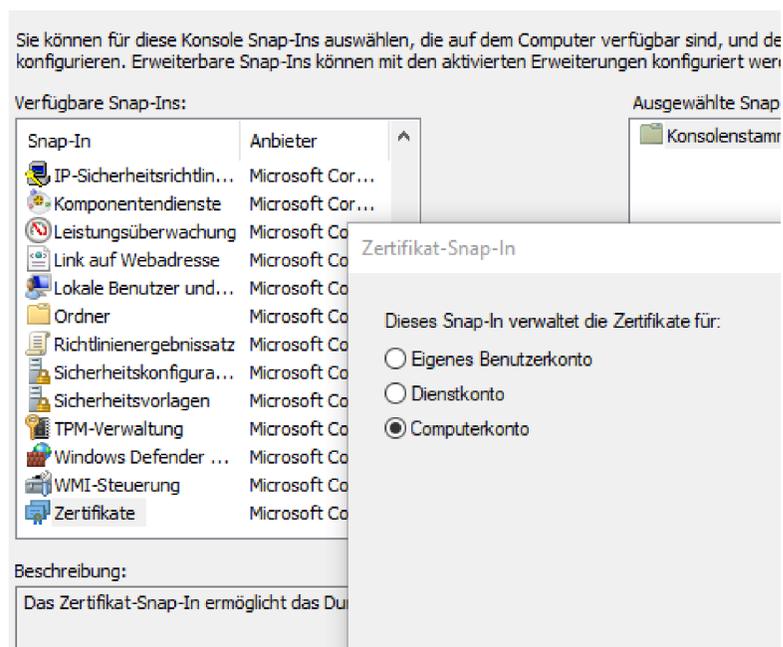


Am ATMS CORE NET Server die mmc starten

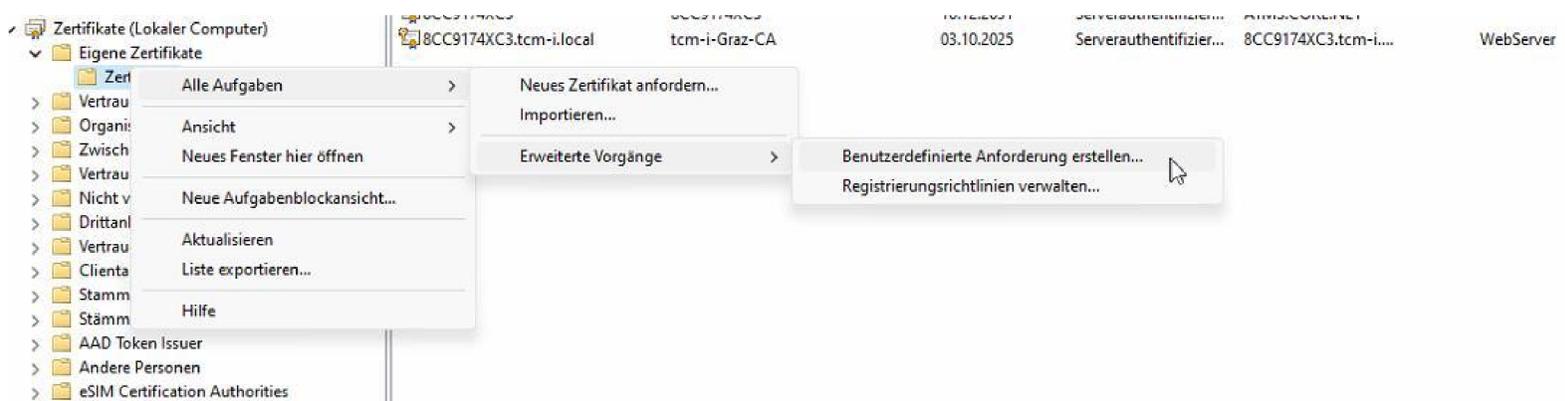
Das Snap-in Zertifikate (Lokaler Computer) hinzufügen.



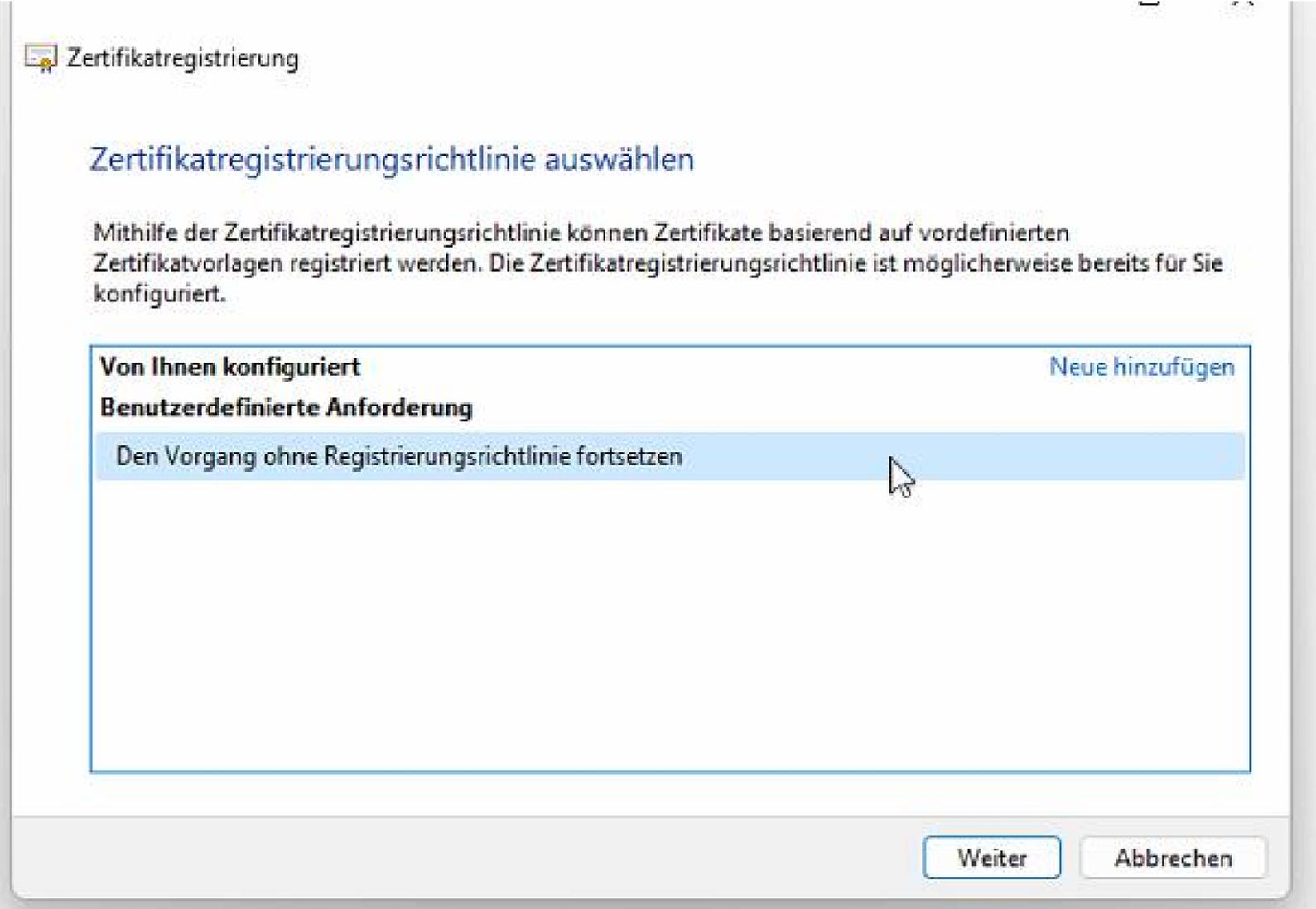
Snap-Ins hinzufügen bzw. entfernen



Alle Aufgaben – Erweiterte Vorgänge – Benutzerdefinierte Anforderung erstellen



Den Vorgang ohne Registrierungsrichtlinie fortsetzen



Zertifikatregistrierung

Zertifikatregistrierungsrichtlinie auswählen

Mithilfe der Zertifikatregistrierungsrichtlinie können Zertifikate basierend auf vordefinierten Zertifikatvorlagen registriert werden. Die Zertifikatregistrierungsrichtlinie ist möglicherweise bereits für Sie konfiguriert.

| Von Ihnen konfiguriert | Neue hinzufügen |
|--|-----------------|
| Benutzerdefinierte Anforderung | |
| Den Vorgang ohne Registrierungsrichtlinie fortsetzen | |

Weiter Abbrechen

Eigenschaften

 Zertifikatregistrierung

Zertifikatsinformationen

Klicken Sie auf "Weiter", um die bereits für diese Vorlage ausgewählten Optionen auszuwählen, oder klicken Sie auf "Details", um die Zertifikatanforderung anzupassen, und klicken Sie anschließend auf "Weiter".

Benutzerdefinierte Anforderung STATUS: Verfügbar Details ^

Die folgenden Optionen beschreiben die Verwendung und den Gültigkeitszeitraum, die auf diesen Zertifikattyp zutreffen:

- Schlüsselverwendung:
- Anwendungsrichtlinien:
- Gültigkeitszeitraum (Tage):

[Eigenschaften](#)

Weiter

Abbrechen

Computernamen eintragen

Zertifikateigenschaften

Allgemein Antragsteller Erweiterungen Privater Schlüssel

Anzeigename und Beschreibung vereinfachen die Identifizierung und Verwaltung des Zertifikats.

Anzeigename:
8CC9174XC3

Beschreibung:
|

Antragsteller Daten ausfüllen.

Besonders wichtig: Alternativer Name. Hier Host (DNS Wert) und IP v4 (IP Wert) eintragen.

Zertifikateigenschaften

Allgemein Antragsteller Erweiterungen Privater Schlüssel

Der Antragsteller eines Zertifikats ist der Benutzer oder Computer, für den das Zertifikat ausgestellt ist. Geben Sie Informationen über die zulässigen Antragstellernamen und alternative Namenswerte ein, die in einem Zertifikat verwendet werden dürfen.

Zertifikatsantragsteller
Der das Zertifikat empfangende Benutzer oder Computer

Antragstellername:

Typ:
Land/Region

Wert:

Hinzufügen >

< Entfernen

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

Alternativer Name:

Typ:
IP-Adresse (v4)

Wert:
10.172.2.53

Hinzufügen >

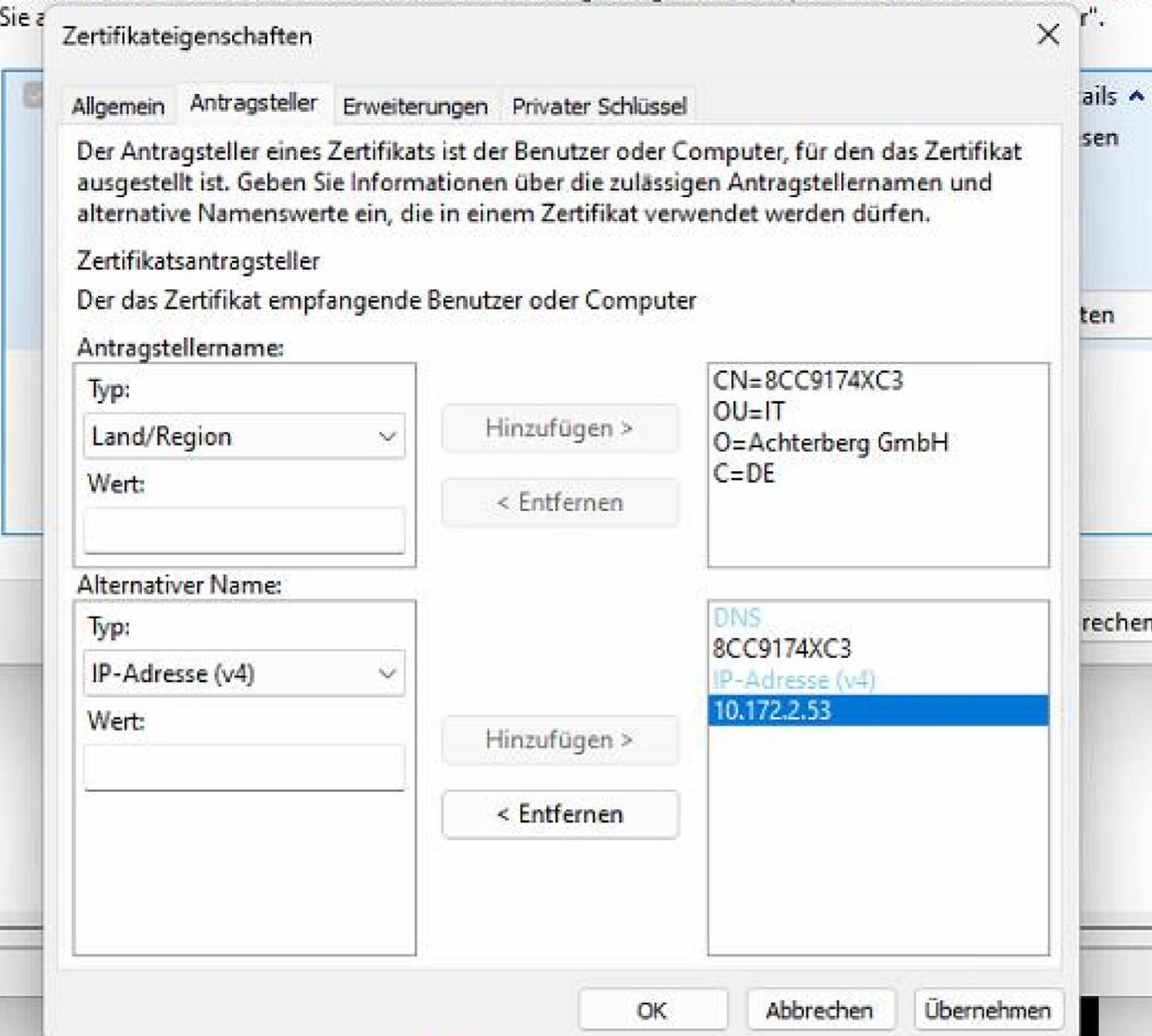
< Entfernen

DNS
8CC9174XC3

OK Abbrechen Übernehmen

Zertifikatsinformationen

Klicken Sie auf "Weiter", um die bereits für diese Vorlage ausgewählten Optionen auszuwählen, oder klicken Sie auf "Zurück", um die vorherigen Schritte zu wiederholen.



Zertifikateigenschaften

Allgemein Antragsteller Erweiterungen Privater Schlüssel

Der Antragsteller eines Zertifikats ist der Benutzer oder Computer, für den das Zertifikat ausgestellt ist. Geben Sie Informationen über die zulässigen Antragstellernamen und alternative Namenswerte ein, die in einem Zertifikat verwendet werden dürfen.

Zertifikatsantragsteller
Der das Zertifikat empfangende Benutzer oder Computer

Antragstellername:

Typ:
Land/Region

Wert:

Hinzufügen >

< Entfernen

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

Alternativer Name:

Typ:
IP-Adresse (v4)

Wert:

Hinzufügen >

< Entfernen

DNS
8CC9174XC3
IP-Adresse (v4)
10.172.2.53

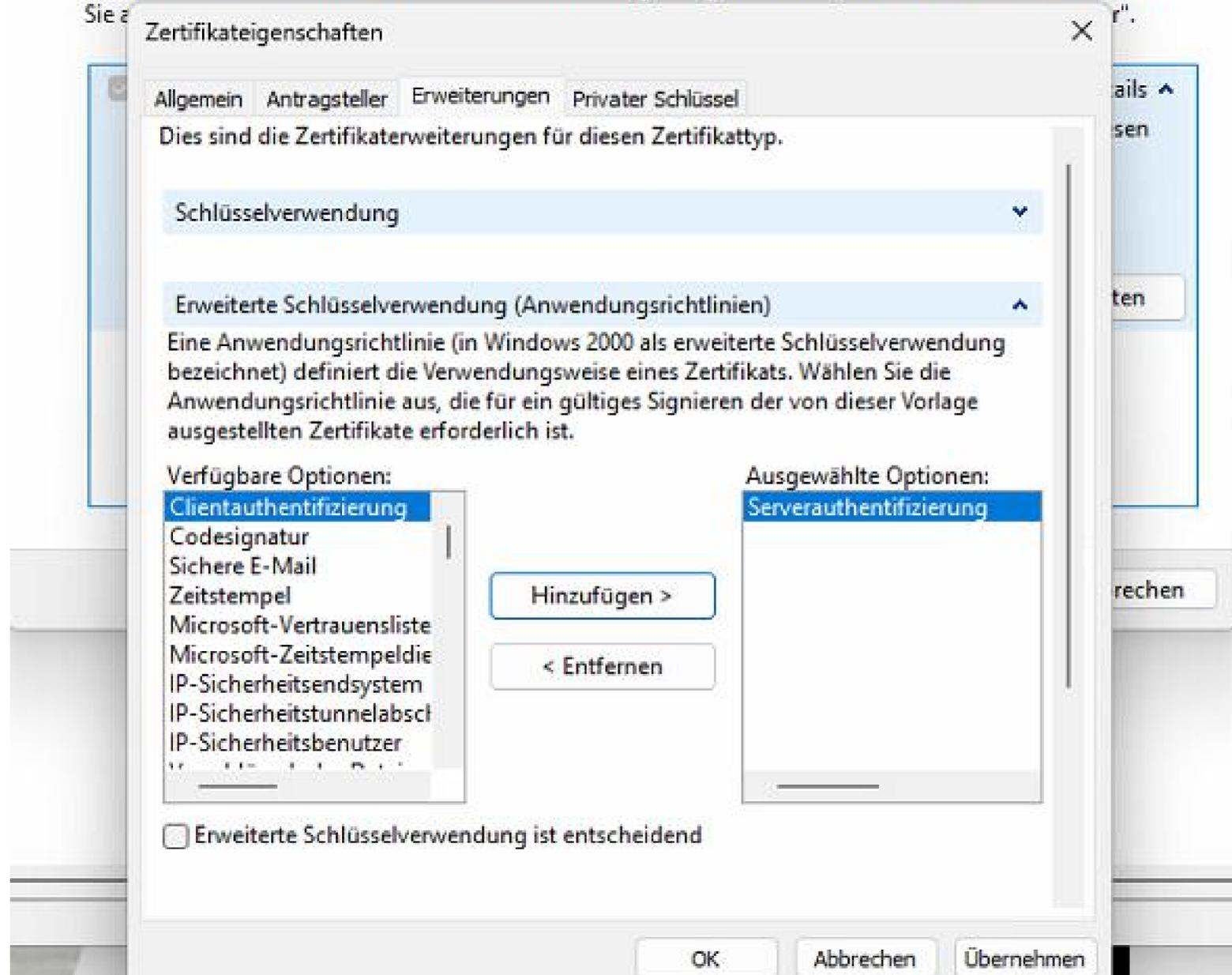
OK Abbrechen Übernehmen

Erweiterungen – Erweiterte Schlüsselverwendung - Serverauthentifizierung

 Zertifikatregistrierung

Zertifikatsinformationen

Klicken Sie auf "Weiter", um die bereits für diese Vorlage ausgewählten Optionen auszuwählen, oder klicken Sie auf "Zurück", um die bereits für diese Vorlage ausgewählten Optionen auszuwählen, oder klicken Sie auf "Abbrechen", um die Registrierung abzubrechen.



Zertifikateigenschaften

Allgemein Antragsteller Erweiterungen Privater Schlüssel

Dies sind die Zertifikaterweiterungen für diesen Zertifikattyp.

Schlüsselverwendung

Erweiterte Schlüsselverwendung (Anwendungsrichtlinien)

Eine Anwendungsrichtlinie (in Windows 2000 als erweiterte Schlüsselverwendung bezeichnet) definiert die Verwendungsweise eines Zertifikats. Wählen Sie die Anwendungsrichtlinie aus, die für ein gültiges Signieren der von dieser Vorlage ausgestellten Zertifikate erforderlich ist.

Verfügbare Optionen:

- Clientauthentifizierung
- Codesignatur
- Sichere E-Mail
- Zeitstempel
- Microsoft-Vertrauensliste
- Microsoft-Zeitstempeldie
- IP-Sicherheitsendsystem
- IP-Sicherheitstunnelabschl
- IP-Sicherheitsbenutzer

Hinzufügen >

< Entfernen

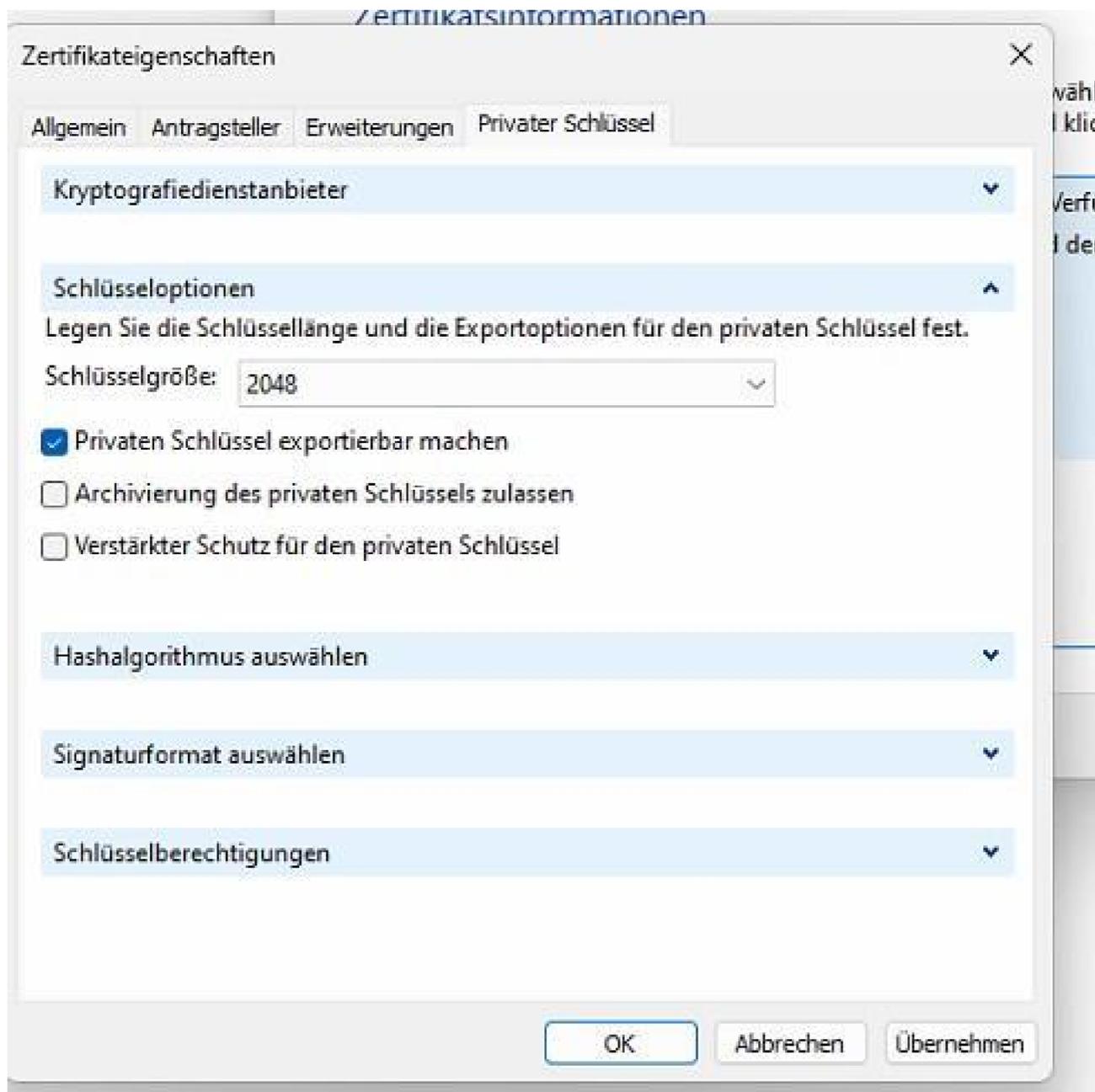
Ausgewählte Optionen:

- Serverauthentifizierung

Erweiterte Schlüsselverwendung ist entscheidend

OK Abbrechen Übernehmen

Privater Schlüssel – exportierbar machen (ermöglicht den Transfer des Schlüssels) Schlüsselgröße mind. 2048



Abspeichern der Anforderung.



Windows Certificate Management console showing a list of certificates and a dialog box for saving an offline request.

| Ausgestellt für | Ausgestellt von | Ablaufdatum | Beabsichtigte Zwec... | Anzeigename | Sta |
|------------------------|-----------------|-------------|-------------------------|----------------------|-----|
| 8CC9174XC3 | 8CC9174XC3 | 16.12.2031 | Serverauthentifizier... | ATMS.CORE.NET | |
| 8CC9174XC3.tcm-i.local | tcm-i-Graz-CA | 03.10.2025 | Serverauthentifizier... | 8CC9174XC3.tcm-i-... | |
| ATMS CORE NET | tcm-i-Graz-CA | 03.10.2025 | Serverauthentifizier... | ATMS.CORE.NET.new | |

Zertifikatregistrierung

Wohin möchten Sie die Offlineanforderung speichern?

Möchten Sie eine Kopie der Zertifikatanforderung speichern, oder die Anfrage später verarbeiten, speichern Sie die Anfrage auf der Festplatte oder auf mobilen Speichermedien. Geben Sie Standort und Namen der Zertifikatanforderung ein, und klicken Sie anschließend auf "Fertig stellen".

Dateiname:
C:\AdminOnly\8CC9174XC3.req Durchsuchen...

Dateiformat:
 Base 64
 Binär

Fertig stellen Abbrechen



Datei mit Editor öffnen. Text kopieren.

```
8CC9174XC3.req
Datei Bearbeiten Ansicht
|-----BEGIN NEW CERTIFICATE REQUEST-----
MIID0DCCArgCAQAwSTELMAkGA1UEBhMCREUxGDAWBgNVBAoMD0FjaHRlcmJlcmcg
R21iSDELMakGA1UECwwCSVQxEzARBgNVBAMMCjhDQzKxNzRYQzMwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDT1dx3gCb106JOdyD8LwViLjBUdaiQpMGj
6Xx9dK3DkWzWFDVvI52nbUtKpJp+OuUWNxvsX0Uf1q8cNdPRz7F9S9q6/i932w/G
gfrZs68SPRdzJZfiIaLESv/7N03zMdk0938trsJoF0BSsjQhRjvzQvuJFpeYx5/z
eLWztW/wbtFvJxA2UtzFUyFYv6d8UCmhjKVNUxtP8cipF0ceLON17ff5GNSMbAuR
V6TstFrTRY2WR05mut3Q27p7z4meHXsdmmUGe3IpKI/y0JhyA8ULERbcUNcgibh1
3LXFNXtHvp4azHaj9Q1Ke8TzFa8HwePtZPIsaE34Gj80X1sdtmGpAgMBAAGgggFA
MBwGCisGAQQBgjcNAgMxDhYMMTAuMC4yMjYyMS4yMDkGCSSGAQQBgjcVFDESMDCoC
AQUMCjhDQzKxNzRYQzMMEDhDQzKxNzRYQzNcQWRtaW4MB01NQy5FWEUwZgYKKwYB
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMabwBmAHQAdwBh
AHIAZQAgaEAsAZQB5ACAuW0B0AG8AcgBhAGcAZQAgaFAAcgBvAHYAaQBkAGUAacgMB
ADB9BggqhkiG9w0BCQ4xcDBuMBsGA1UdEQQUUMBKCCjhDQzKxNzRYQzOHBAqsAjUw
EwYDVR01BAwwCgYIKwYBBQUHAWewGwYJKwYBBAGCNxUKBA4wDDAKBggrBgEFBQcD
ATAdBgNVHQ4EFgQU2Bsa9Jh5d0L+xGsR7k1CzbmPmnEwDQYJKoZIhvcNAQELBQAD
ggEBAC1WNk3E250eRirMDrvwxHb/Ir60xXdMjC1GGuATME0q9gJWrsKIvbx57Zcg
bv/x3ELCVaNVZxWtzQH9LDU8YzD99/Yp3J/XaQrwGDWAjRa/jYK03VD2LyMh7FG+
91BHc9HP2xyqfIpi6bgjdXsVT8vzVzf/vSyAyN8nD2q12VeE0PBW36KLH1U3ETC
T7oYerI2bWVZO/kdMNV7AFJAtLcgTIqyX61i6wXIo7uW0J4N6bmktq9950ofcCnR
h9B8AtVvNmuRvCz2L3kAJKMa0Ji0qqV77JhpV5Ug1p2c1UgvZ53mXQ8DP2rzQ4/
6MBwUcqssZ7Zr/gmwNKQwawhzWg=
-----END NEW CERTIFICATE REQUEST-----
```



Am Zertifizierungsstellen Server die Web Anwendung mit Browser öffnen

← 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 der Konfiguration, 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](#)

Text aus Zwischenablage in Feld gespeicherte Anforderung einfügen.

Auswahl Webserver

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):

```
91BHc9HP2xyqfIpif6bgjdXsVT8vzVzf/vSyAyN8r
T7oYerI2bWVZO/kdMNV7AFJAtLcgTIqyX6li6wXIc
h9B8AtVvNmuRvCxx2L3kAJKMa0Ji0qqV77JhpV5Ug
6MBwUcqssZ7Zr/gmwNKQwawhzWg=
-----END NEW CERTIFICATE REQUEST-----
```

Zertifikatvorlage:

Webserver

Zusätzliche Attribute:

Attribute:

Einsenden >

Einsenden.

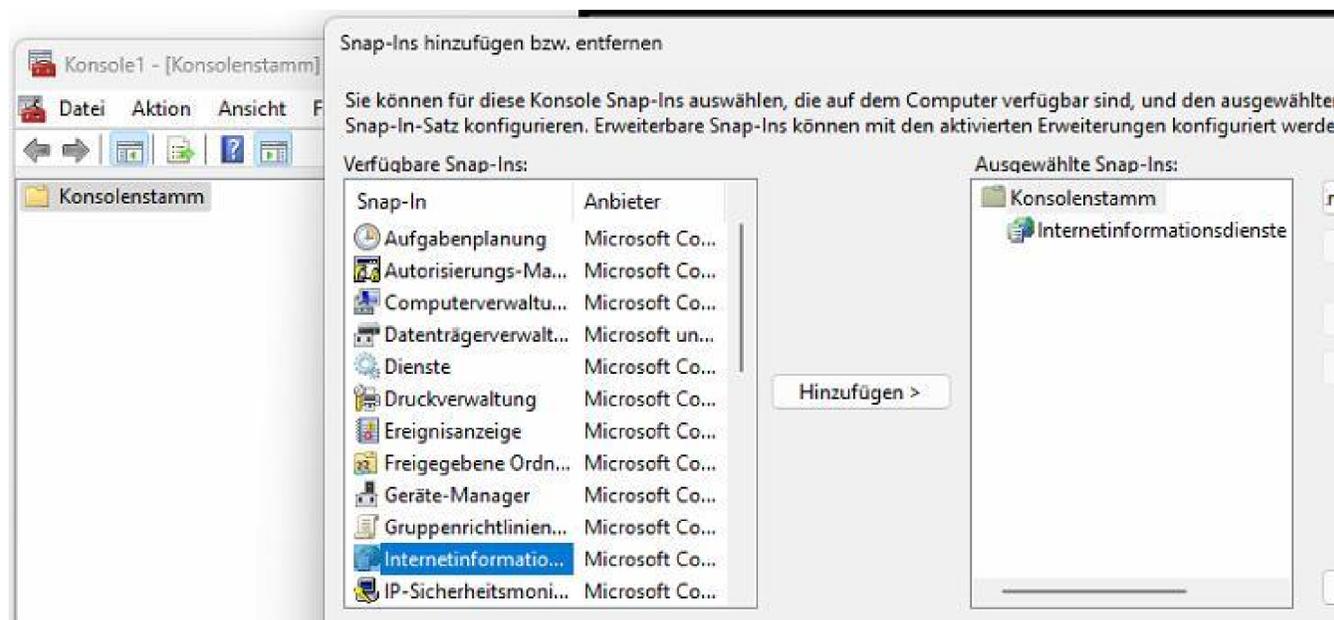
Download des Zertifikates. Empfehlung Base 64 codiert.

Transfer der cer Datei zum ATMS CORE NET Server.

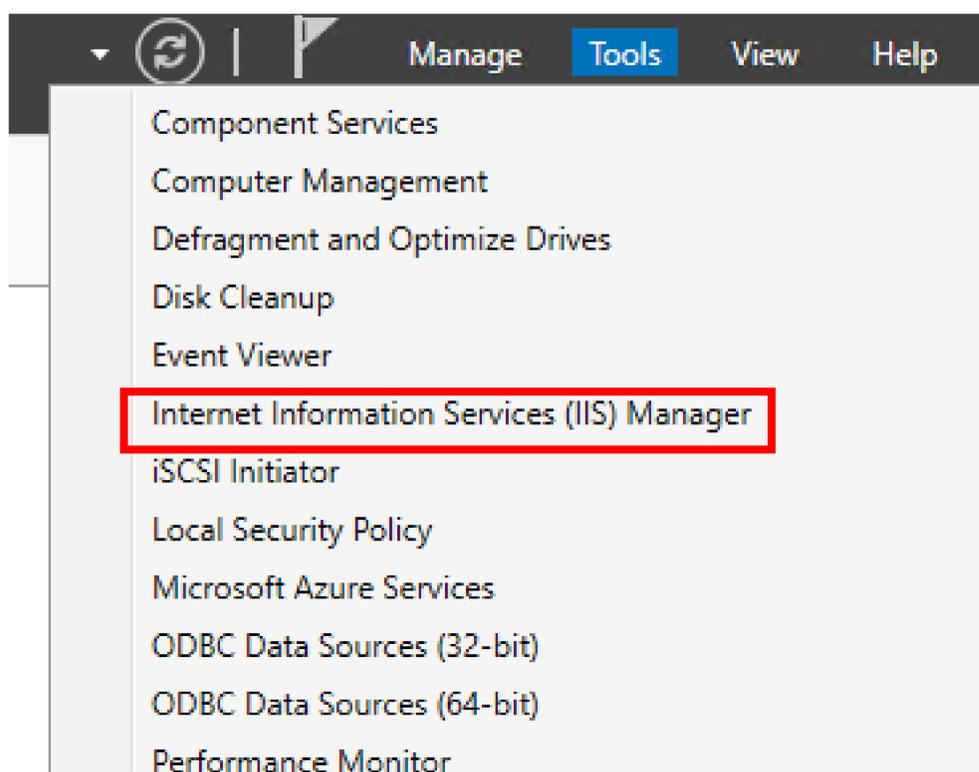
| Name | Änderungsdatum | Typ | Größe |
|----------------|------------------|-----------------------|-------|
| 8CC9174XC3.cer | 04.10.2023 13:04 | Sicherheitszertifikat | 2 KB |
| 8CC9174XC3.req | 04.10.2023 13:02 | REQ-Datei | 2 KB |
| root-ca.cer | 19.01.2023 15:06 | Sicherheitszertifikat | 2 KB |

Client Betriebssysteme:

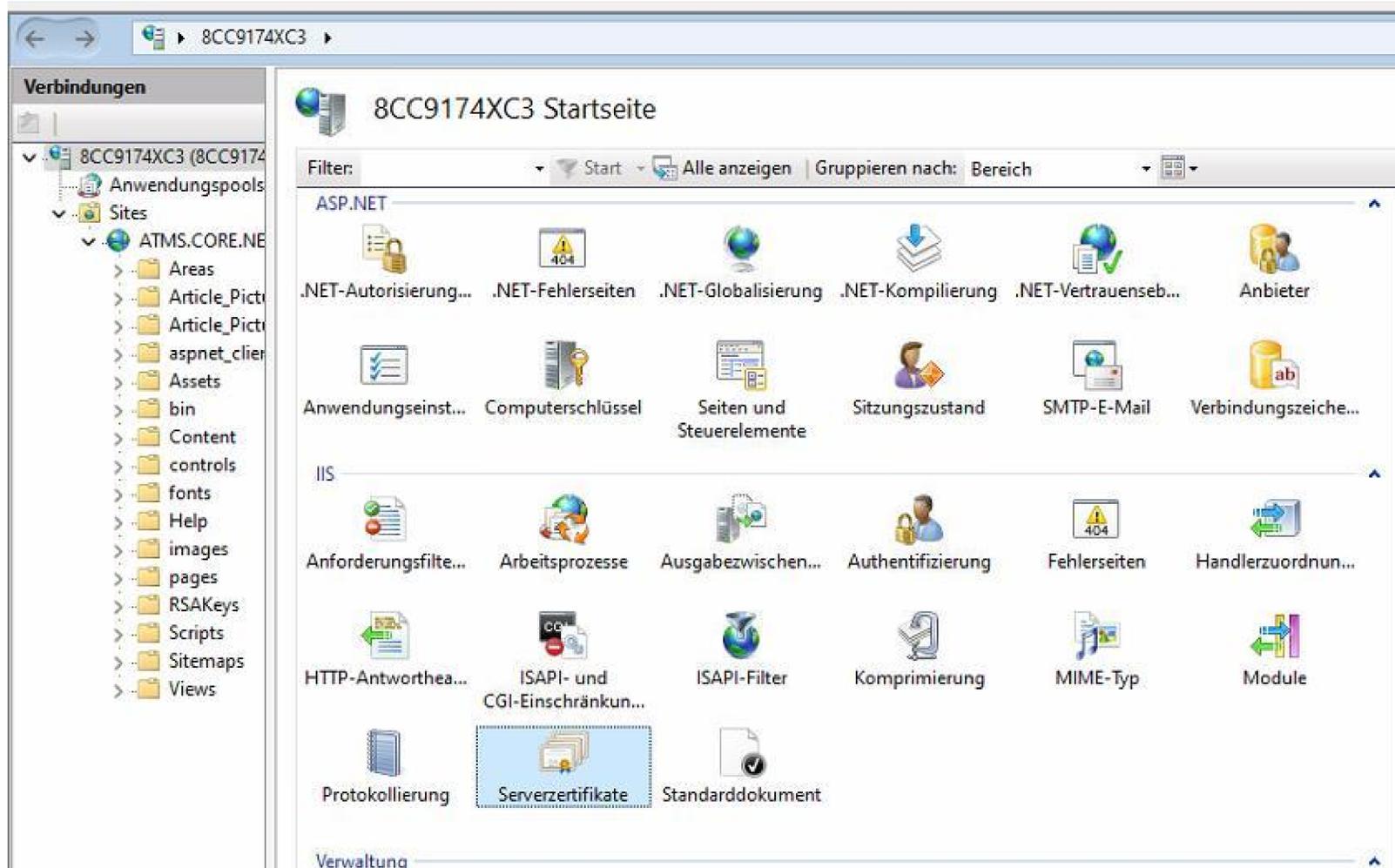
IIS Verwaltung Snap-in zu mmc hinzufügen.



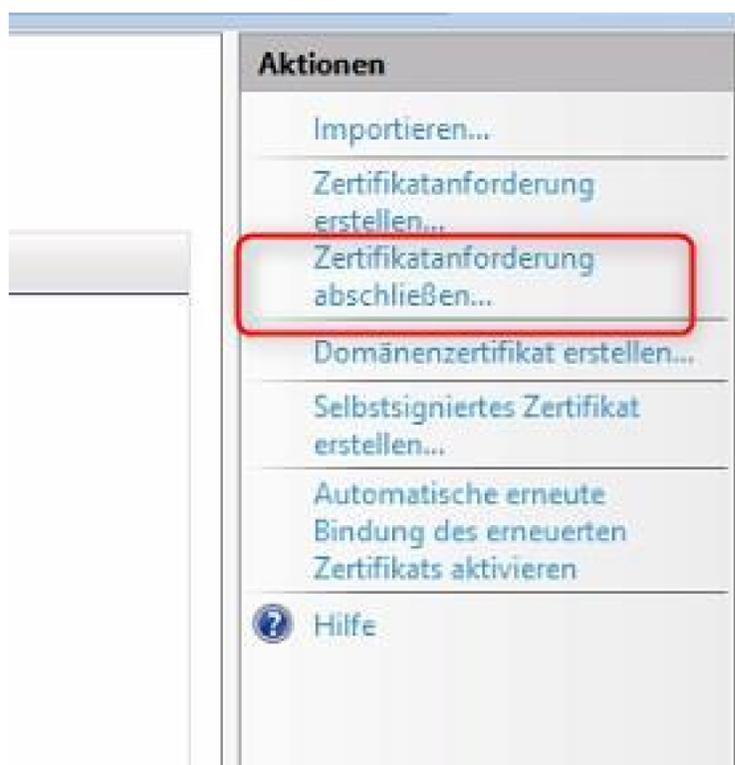
Server Betriebssysteme: Im Servermanager den Eintrag aufrufen.



Server Zertifikate öffnen



Zertifikatsanforderung abschließen...



Zertifikatanforderung abschließen ? X

 **Antwort der Zertifizierungsstelle angeben**

Bereits erstellte Zertifikatanforderung durch Abrufen der Datei mit der Antwort der Zertifizierungsstelle abschließen

Name der Datei mit der Antwort der Zertifizierungsstelle:

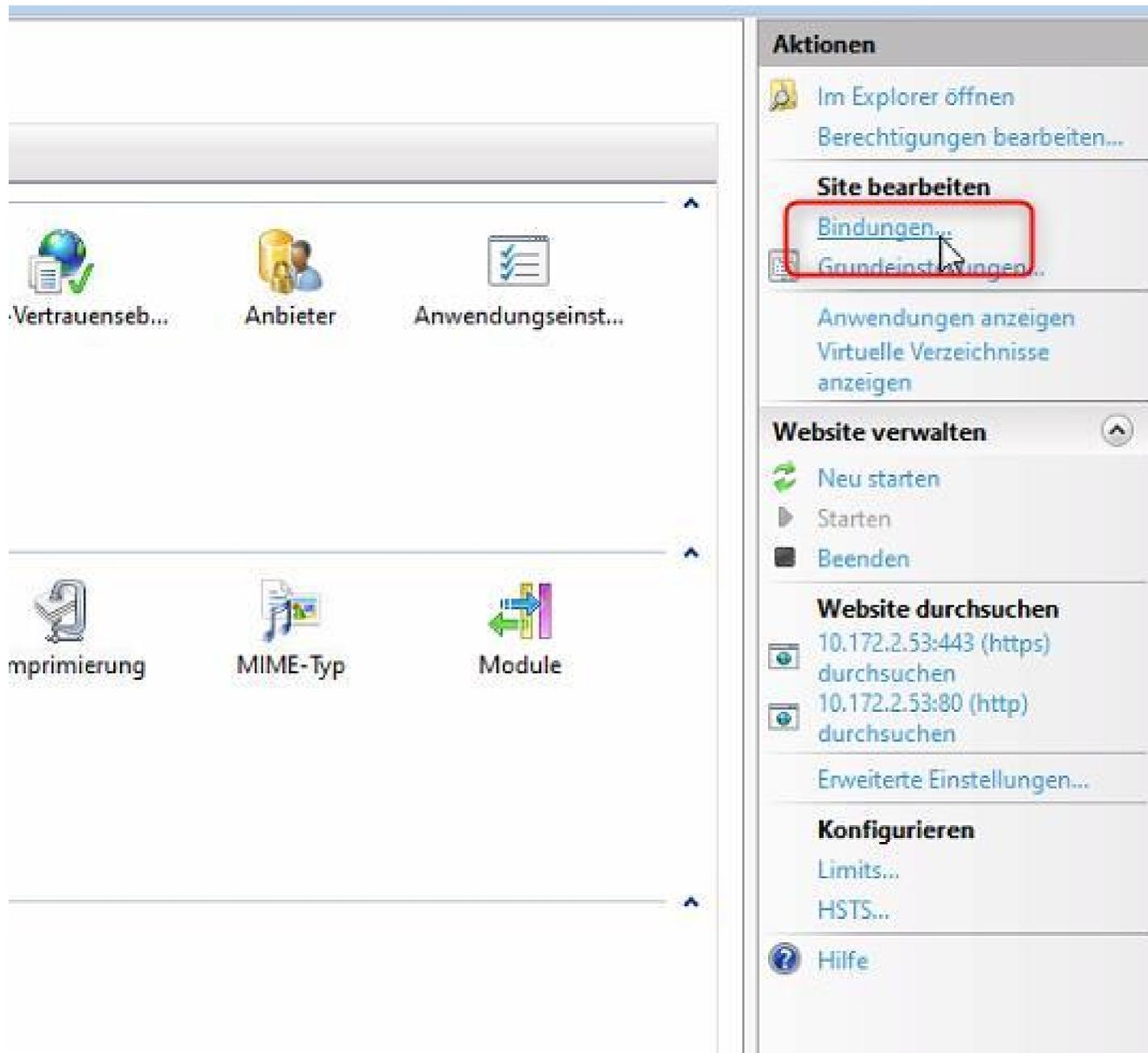
...

Anzeigename:

Zertifikatspeicher für das neue Zertifikat auswählen:

▾

OK Abbrechen

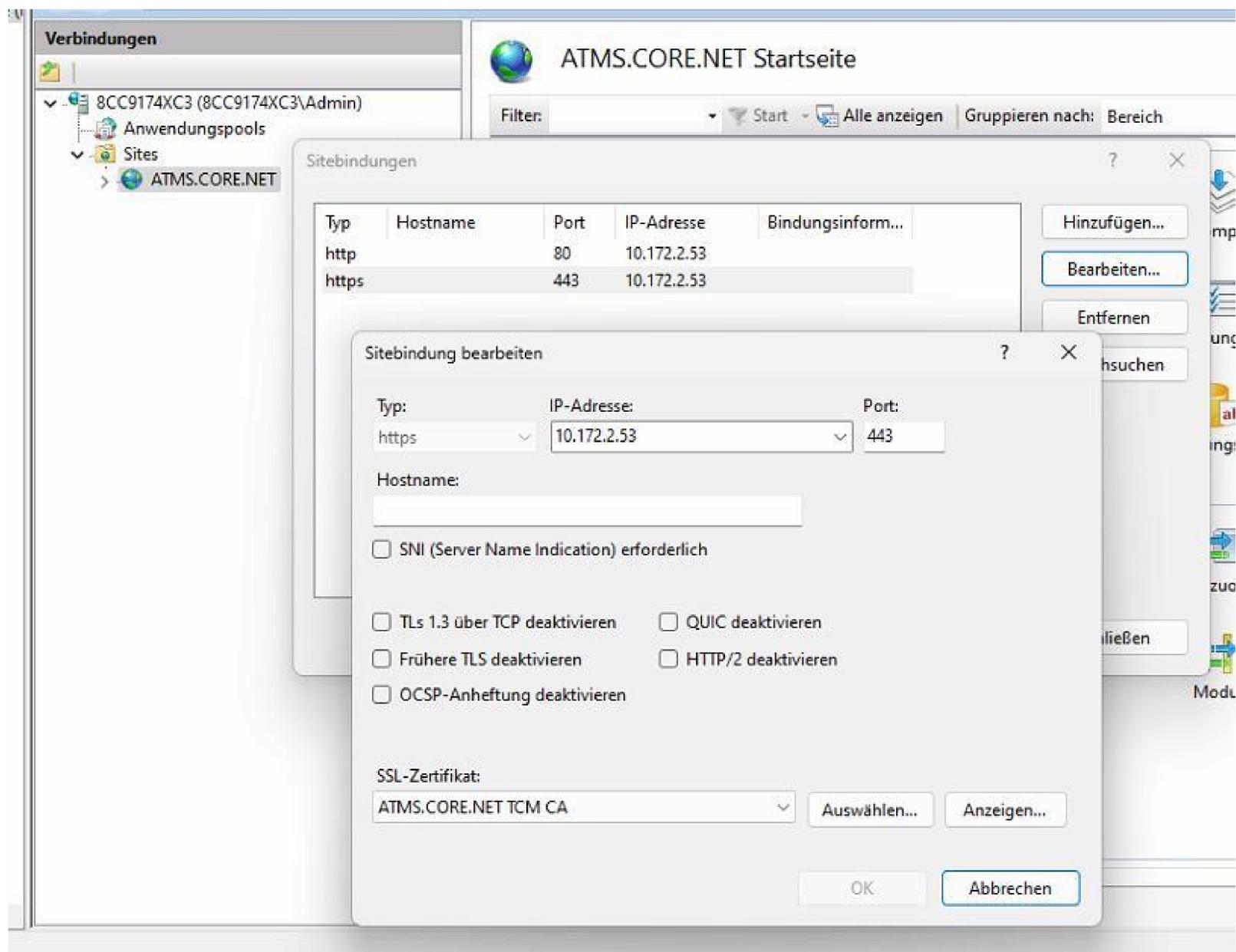


The screenshot displays the ATMScore management interface. The main area contains several configuration categories:

- Vertrauensbereich** (Trust area)
- Anbieter** (Providers)
- Anwendungseinstellungen** (Application settings)
- Comprimierung** (Compression)
- MIME-Typ** (MIME type)
- Module**

The right-hand sidebar, titled **Aktionen** (Actions), contains the following sections:

- Aktionen**
 - Im Explorer öffnen
 - Berechtigungen bearbeiten...
- Site bearbeiten**
 - Bindungen...** (highlighted with a red box)
 - Grundeinstellungen...
- Anwendungen anzeigen**
- Virtuelle Verzeichnisse anzeigen**
- Website verwalten**
 - Neu starten
 - Starten
 - Beenden
- Website durchsuchen**
 - 10.172.2.53:443 (https) durchsuchen
 - 10.172.2.53:80 (http) durchsuchen
- Erweiterte Einstellungen...
- Konfigurieren**
 - Limits...
 - HSTS...
- Hilfe



Root CA exportieren:

Am Zertifizierungsstellen Server mit Webanwendung

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](#) ←

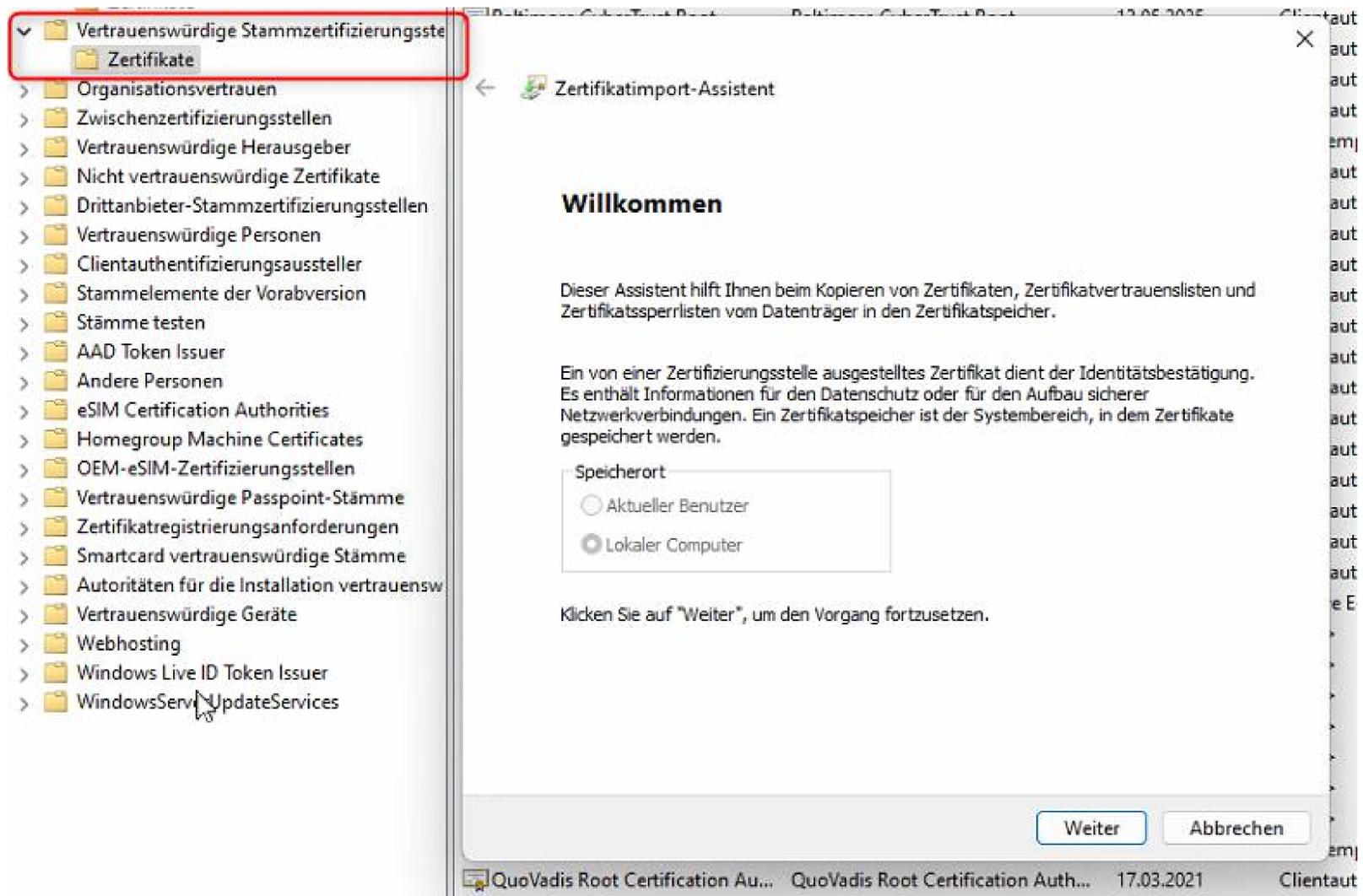
[Download der Zertifizierungsstellen-Zertifikatkette](#)

[Download der aktuellen Basissperrliste](#)

[Download der aktuellen Deltasperrliste](#)

Root CA am ATMS CORE NET Server importieren:

mmc Zertifikate (Computer)



Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Speicherort

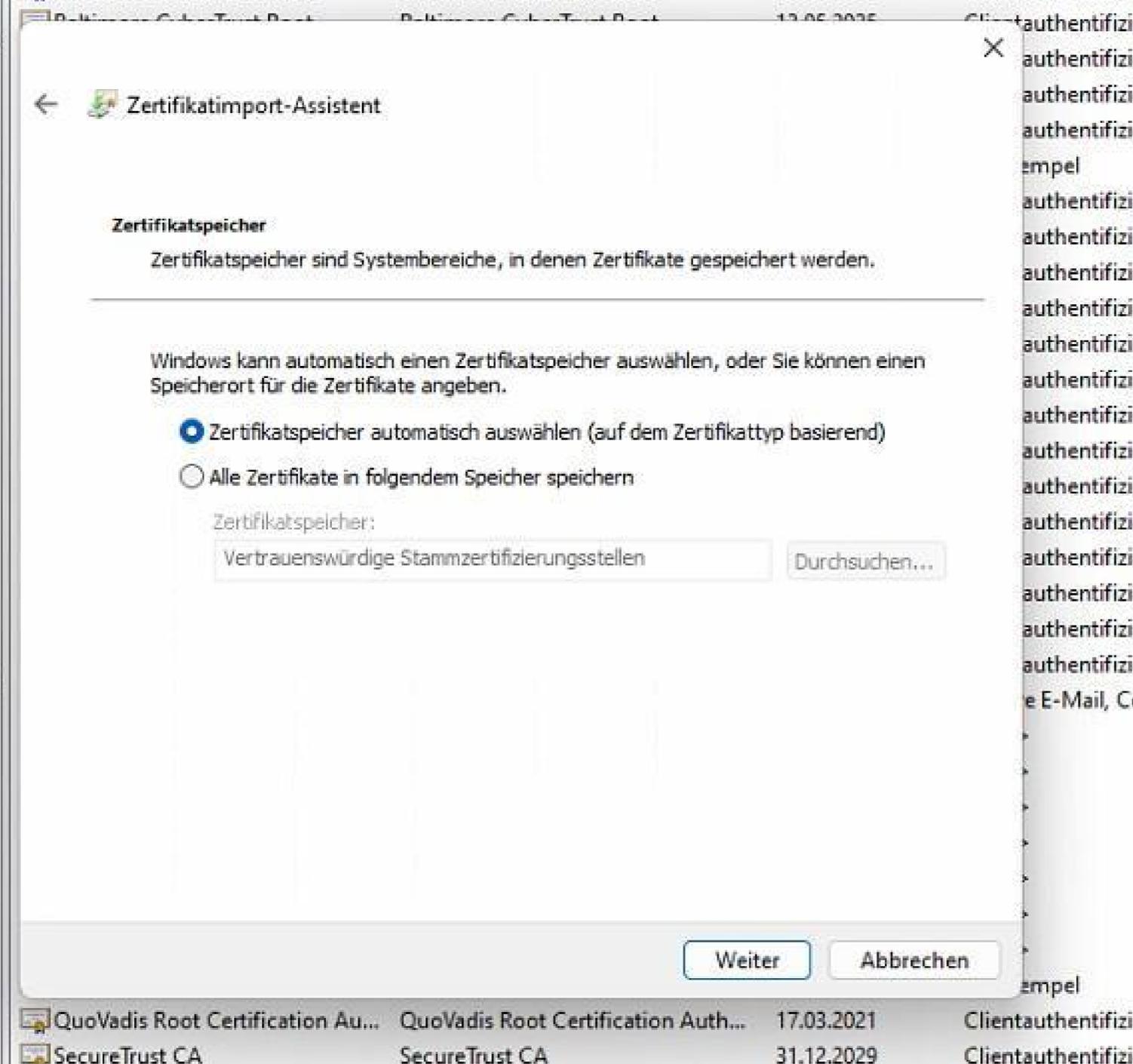
Aktueller Benutzer

Lokaler Computer

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Weiter **Abbrechen**

| 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 |



Zertifikatimport-Assistent

Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

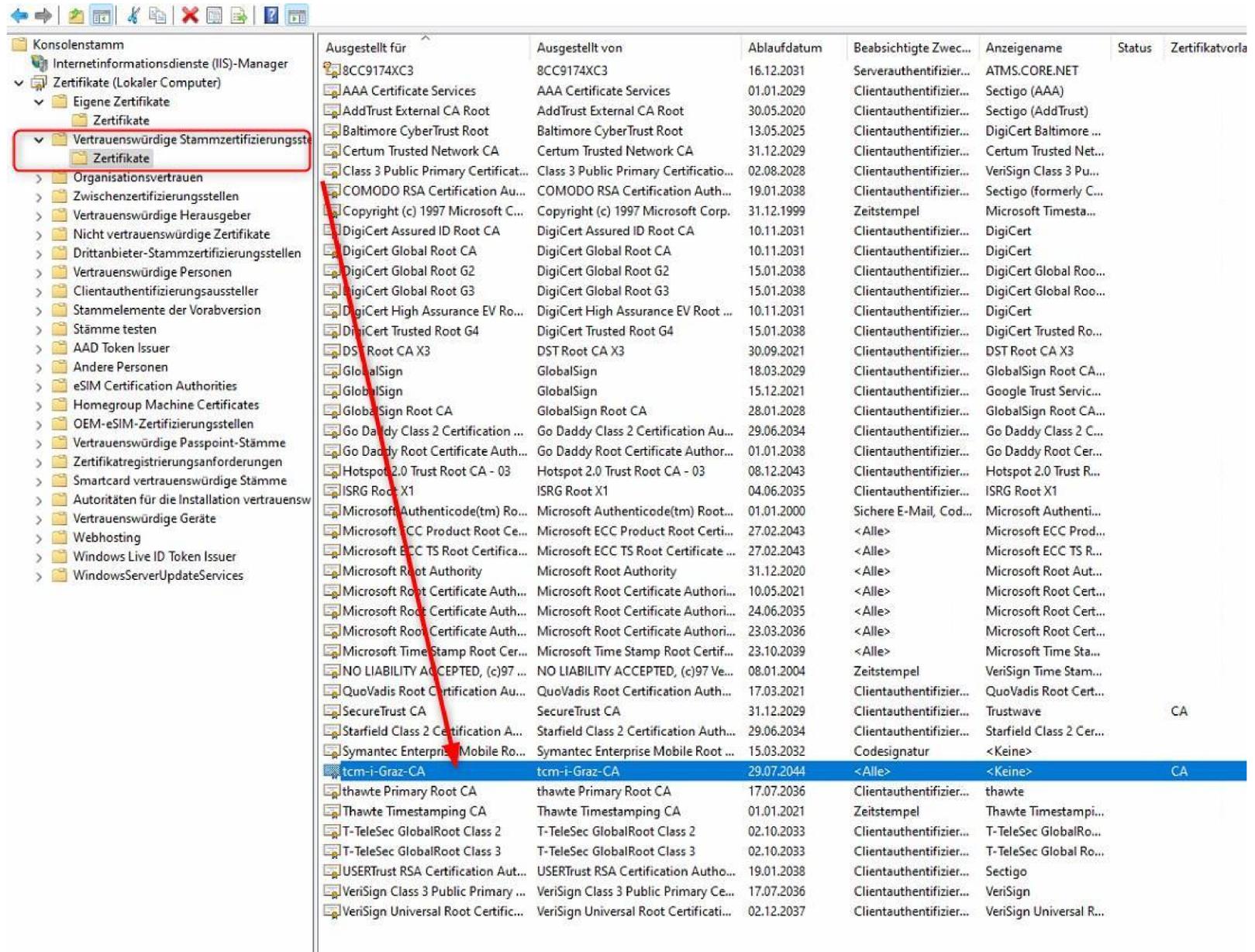
Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:
Vertrauenswürdige Stammzertifizierungsstellen Durchsuchen...

Weiter Abbrechen

| | | | |
|-----------------------------------|-------------------------------------|------------|-------------------------|
| QuoVadis Root Certification Au... | QuoVadis Root Certification Auth... | 17.03.2021 | Clientauthentifizierung |
| SecureTrust CA | SecureTrust CA | 31.12.2029 | Clientauthentifizierung |

Kontrolle des Imports



| Ausgestellt für | Ausgestellt von | Ablaufdatum | Beabsichtigte Zweck... | Anzeigenname | Status | Zertifikatvorla |
|--------------------------------------|---|-------------|-------------------------|--------------------------|--------|-----------------|
| 8CC9174XC3 | 8CC9174XC3 | 16.12.2031 | Serverauthentifizier... | ATMS.CORE.NET | | |
| AAA Certificate Services | AAA Certificate Services | 01.01.2029 | Clientauthentifizier... | Sectigo (AAA) | | |
| AddTrust External CA Root | AddTrust External CA Root | 30.05.2020 | Clientauthentifizier... | Sectigo (AddTrust) | | |
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 13.05.2025 | Clientauthentifizier... | DigiCert Baltimore ... | | |
| Certum Trusted Network CA | Certum Trusted Network CA | 31.12.2029 | Clientauthentifizier... | Certum Trusted Net... | | |
| Class 3 Public Primary Certificat... | Class 3 Public Primary Certificatio... | 02.08.2028 | Clientauthentifizier... | VeriSign Class 3 Pu... | | |
| COMODO RSA Certification Au... | COMODO RSA Certification Auth... | 19.01.2038 | Clientauthentifizier... | Sectigo (formerly C... | | |
| Copyright (c) 1997 Microsoft C... | Copyright (c) 1997 Microsoft Corp. | 31.12.1999 | Zeitstempel | Microsoft Timesta... | | |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 10.11.2031 | Clientauthentifizier... | DigiCert | | |
| DigiCert Global Root CA | DigiCert Global Root CA | 10.11.2031 | Clientauthentifizier... | DigiCert | | |
| DigiCert Global Root G2 | DigiCert Global Root G2 | 15.01.2038 | Clientauthentifizier... | DigiCert Global Roo... | | |
| DigiCert Global Root G3 | DigiCert Global Root G3 | 15.01.2038 | Clientauthentifizier... | DigiCert Global Roo... | | |
| DigiCert High Assurance EV Ro... | DigiCert High Assurance EV Root ... | 10.11.2031 | Clientauthentifizier... | DigiCert | | |
| DigiCert Trusted Root G4 | DigiCert Trusted Root G4 | 15.01.2038 | Clientauthentifizier... | DigiCert Trusted Ro... | | |
| DST Root CA X3 | DST Root CA X3 | 30.09.2021 | Clientauthentifizier... | DST Root CA X3 | | |
| GlobalSign | GlobalSign | 18.03.2029 | Clientauthentifizier... | GlobalSign Root CA... | | |
| GlobalSign | GlobalSign | 15.12.2021 | Clientauthentifizier... | Google Trust Servic... | | |
| GlobalSign Root CA | GlobalSign Root CA | 28.01.2028 | Clientauthentifizier... | GlobalSign Root CA... | | |
| Go Daddy Class 2 Certification ... | Go Daddy Class 2 Certification Au... | 29.06.2034 | Clientauthentifizier... | Go Daddy Class 2 C... | | |
| Go Daddy Root Certificate Auth... | Go Daddy Root Certificate Author... | 01.01.2038 | Clientauthentifizier... | Go Daddy Root Cer... | | |
| Hotspot 2.0 Trust Root CA - 03 | Hotspot 2.0 Trust Root CA - 03 | 08.12.2043 | Clientauthentifizier... | Hotspot 2.0 Trust R... | | |
| ISRG Root X1 | ISRG Root X1 | 04.06.2035 | Clientauthentifizier... | ISRG Root X1 | | |
| Microsoft Authenticode(tm) Ro... | Microsoft Authenticode(tm) Root... | 01.01.2000 | Sichere E-Mail, Cod... | Microsoft Authenti... | | |
| Microsoft ECC Product Root Ce... | Microsoft ECC Product Root Certi... | 27.02.2043 | <Alle> | Microsoft ECC Prod... | | |
| Microsoft ECC TS Root Certifica... | Microsoft ECC TS Root Certificate ... | 27.02.2043 | <Alle> | Microsoft ECC TS R... | | |
| Microsoft Root Authority | Microsoft Root Authority | 31.12.2020 | <Alle> | Microsoft Root Aut... | | |
| Microsoft Root Certificate Auth... | Microsoft Root Certificate Authori... | 10.05.2021 | <Alle> | Microsoft Root Cert... | | |
| Microsoft Root Certificate Auth... | Microsoft Root Certificate Authori... | 24.06.2035 | <Alle> | Microsoft Root Cert... | | |
| Microsoft Root Certificate Auth... | Microsoft Root Certificate Authori... | 23.03.2036 | <Alle> | Microsoft Root Cert... | | |
| Microsoft Time Stamp Root Cer... | Microsoft Time Stamp Root Certif... | 23.10.2039 | <Alle> | Microsoft Time Sta... | | |
| NO LIABILITY ACCEPTED, (c)97 ... | NO LIABILITY ACCEPTED, (c)97 Ve... | 08.01.2004 | Zeitstempel | VeriSign Time Stam... | | |
| QuoVadis Root Certification Au... | QuoVadis Root Certification Auth... | 17.03.2021 | Clientauthentifizier... | QuoVadis Root Cert... | | |
| SecureTrust CA | SecureTrust CA | 31.12.2029 | Clientauthentifizier... | Trustwave | | CA |
| Starfield Class 2 Certification A... | Starfield Class 2 Certification Auth... | 29.06.2034 | Clientauthentifizier... | Starfield Class 2 Cer... | | |
| Symantec Enterprise Mobile Ro... | Symantec Enterprise Mobile Root ... | 15.03.2032 | Codesignatur | <Keine> | | |
| tcm-i-Graz-CA | tcm-i-Graz-CA | 29.07.2044 | <Alle> | <Keine> | | CA |
| thawte Primary Root CA | thawte Primary Root CA | 17.07.2036 | Clientauthentifizier... | thawte | | |
| Thawte Timestamping CA | Thawte Timestamping CA | 01.01.2021 | Zeitstempel | Thawte Timestampi... | | |
| T-TeleSec GlobalRoot Class 2 | T-TeleSec GlobalRoot Class 2 | 02.10.2033 | Clientauthentifizier... | T-TeleSec GlobalRo... | | |
| T-TeleSec GlobalRoot Class 3 | T-TeleSec GlobalRoot Class 3 | 02.10.2033 | Clientauthentifizier... | T-TeleSec Global Ro... | | |
| USERTrust RSA Certification Aut... | USERTrust RSA Certification Autho... | 19.01.2038 | Clientauthentifizier... | Sectigo | | |
| VeriSign Class 3 Public Primary ... | VeriSign Class 3 Public Primary Ce... | 17.07.2036 | Clientauthentifizier... | VeriSign | | |
| VeriSign Universal Root Certific... | VeriSign Universal Root Certificati... | 02.12.2037 | Clientauthentifizier... | VeriSign Universal R... | | |



Test der Webseite am ATMS CORE NET Server:

Es darf keine Warnung angezeigt werden.

