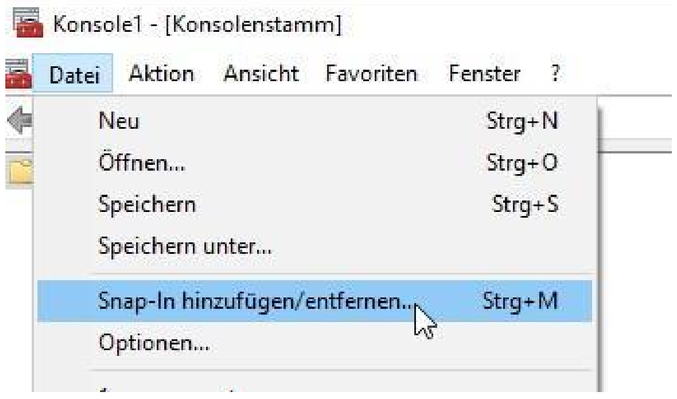
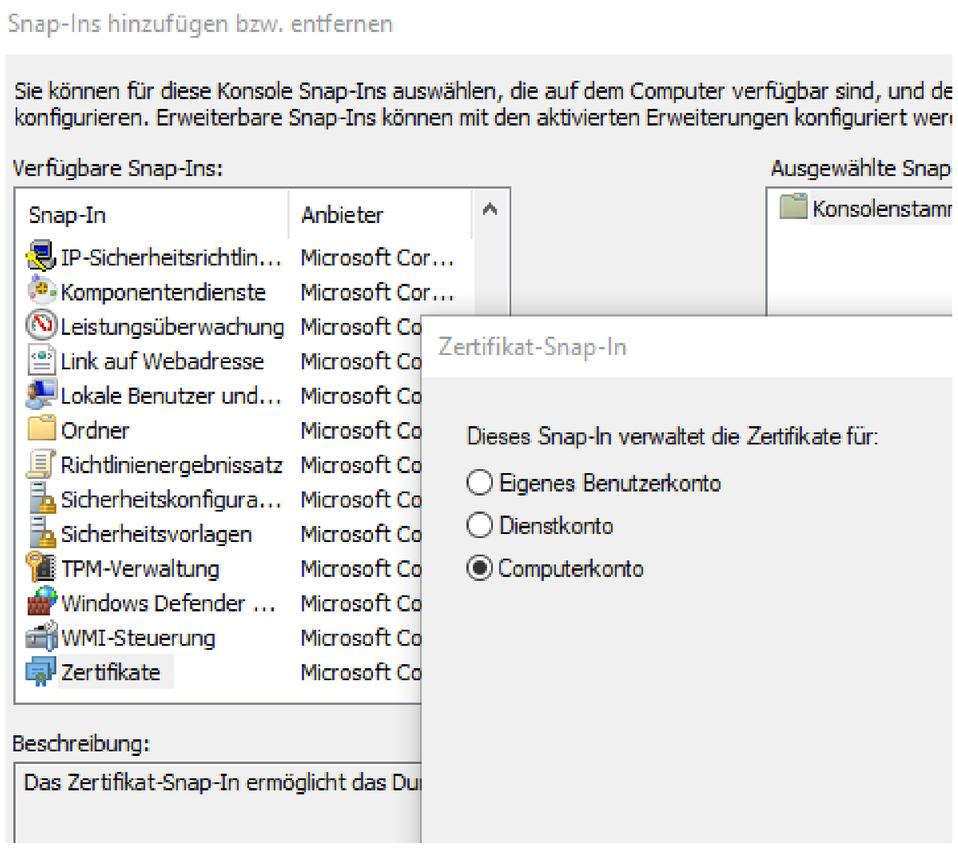
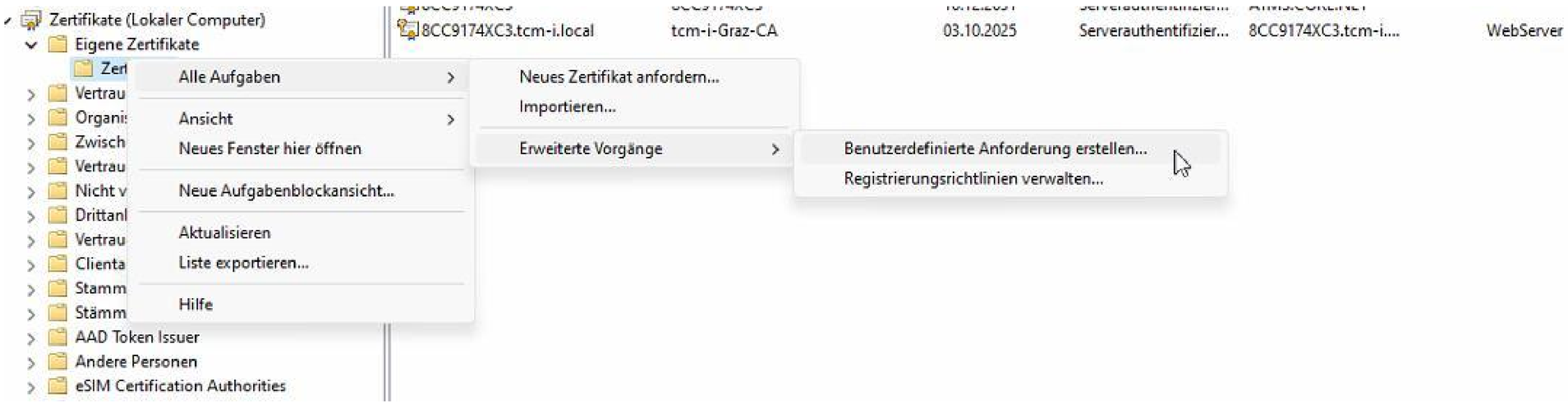
Am ATMS CORE NET Server die mmc starten

Das Snap-in Zertifikate (Lokaler Computer) hinzufügen.

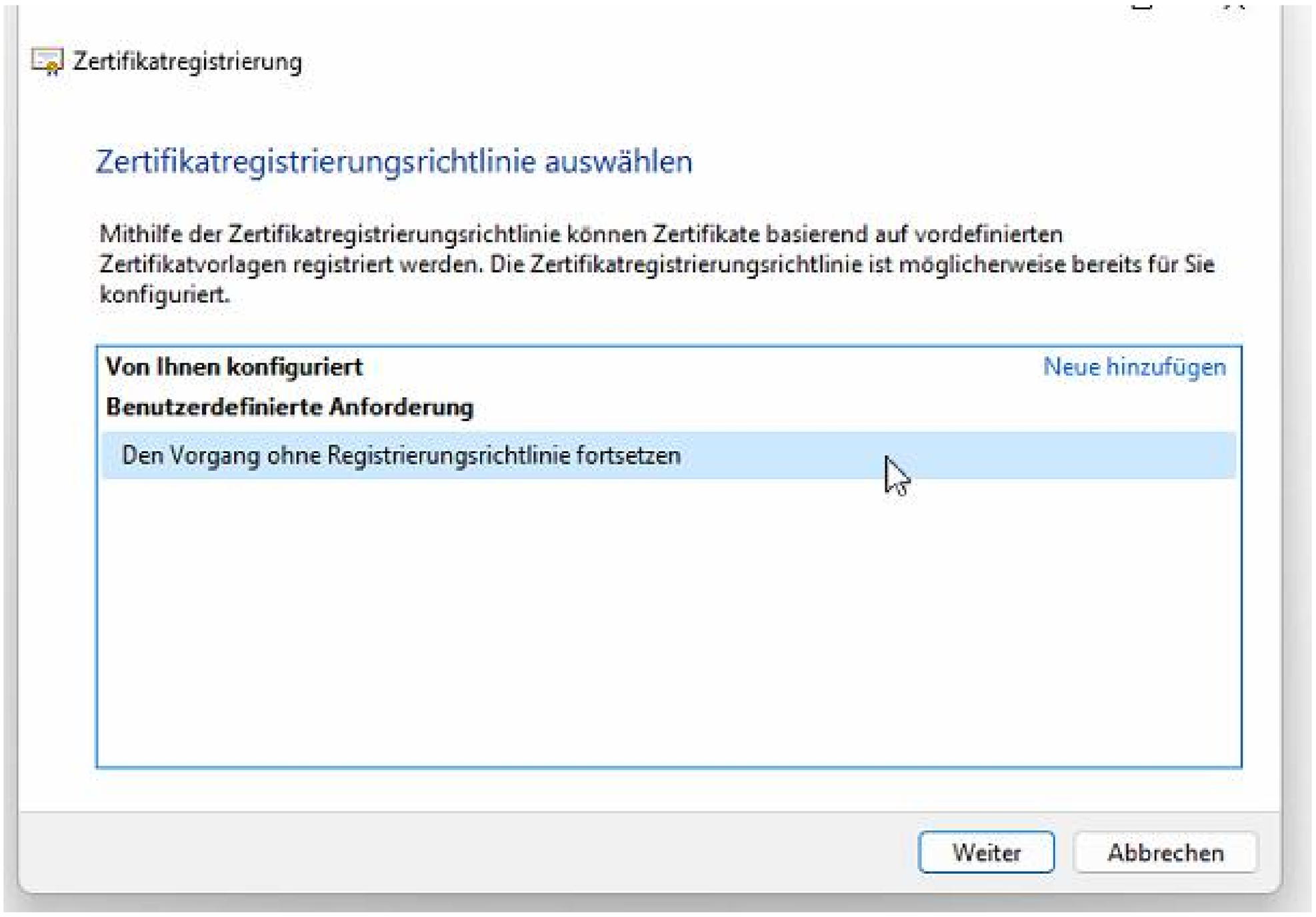




Alle Aufgaben – Erweiterte Vorgänge – Benutzerdefinierte Anforderung erstellen



Den Vorgang ohne Registrierungsrichtlinie fortsetzen



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

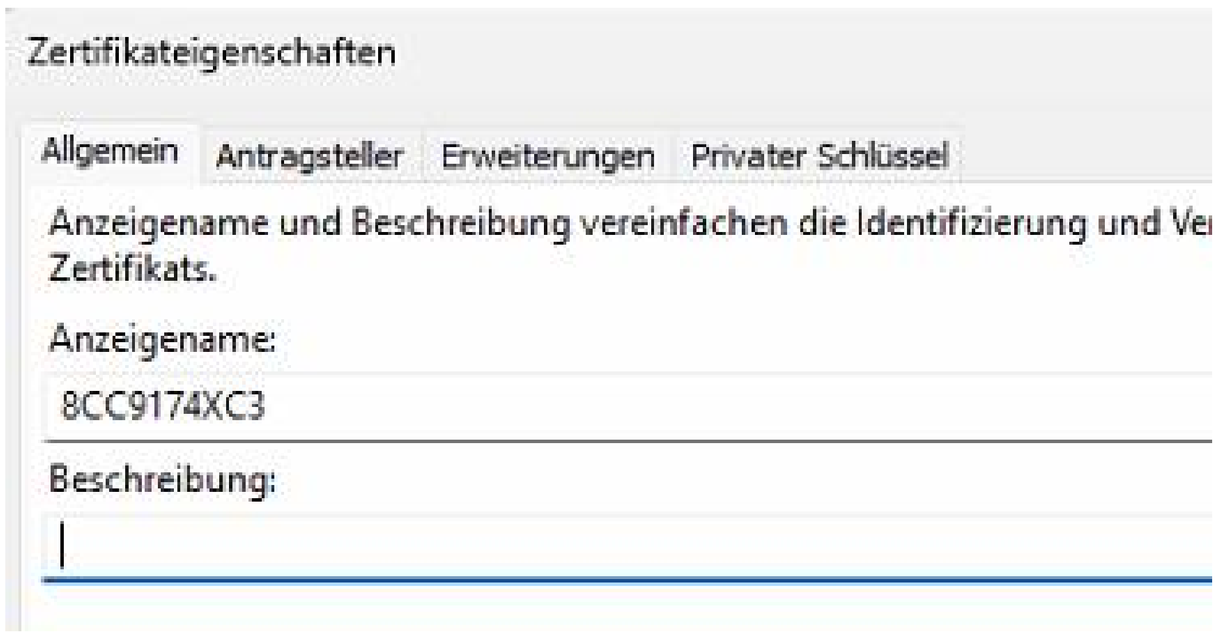
Die folgenden Optionen beschreiben die Verwendung und den Gültigkeitszeitraum, die auf diesen Zertifikattyp zutreffen:

Schlüsselverwendung:
Anwendungsrichtlinien:
Gültigkeitszeitraum (Tage):

Eigenschaften

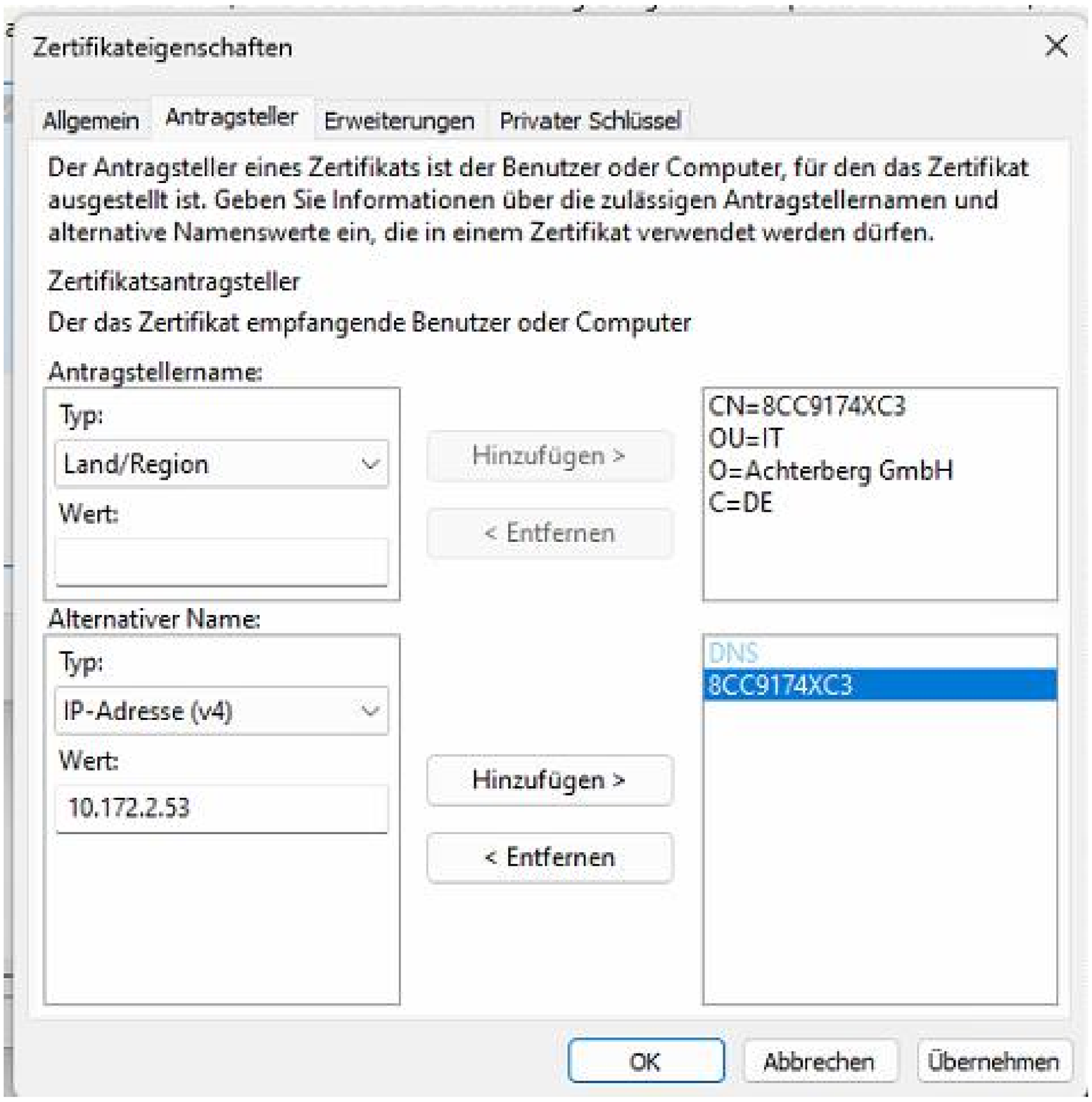
Weiter Abbrechen

Computernamen eintragen



Antragsteller Daten ausfüllen.

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



Zertifikatregistrierung

Zertifikatsinformationen

Klicken Sie auf "Weiter", um die bereits für diese Vorlage ausgewählten Optionen auszuwählen, oder klicken Sie a r".

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:

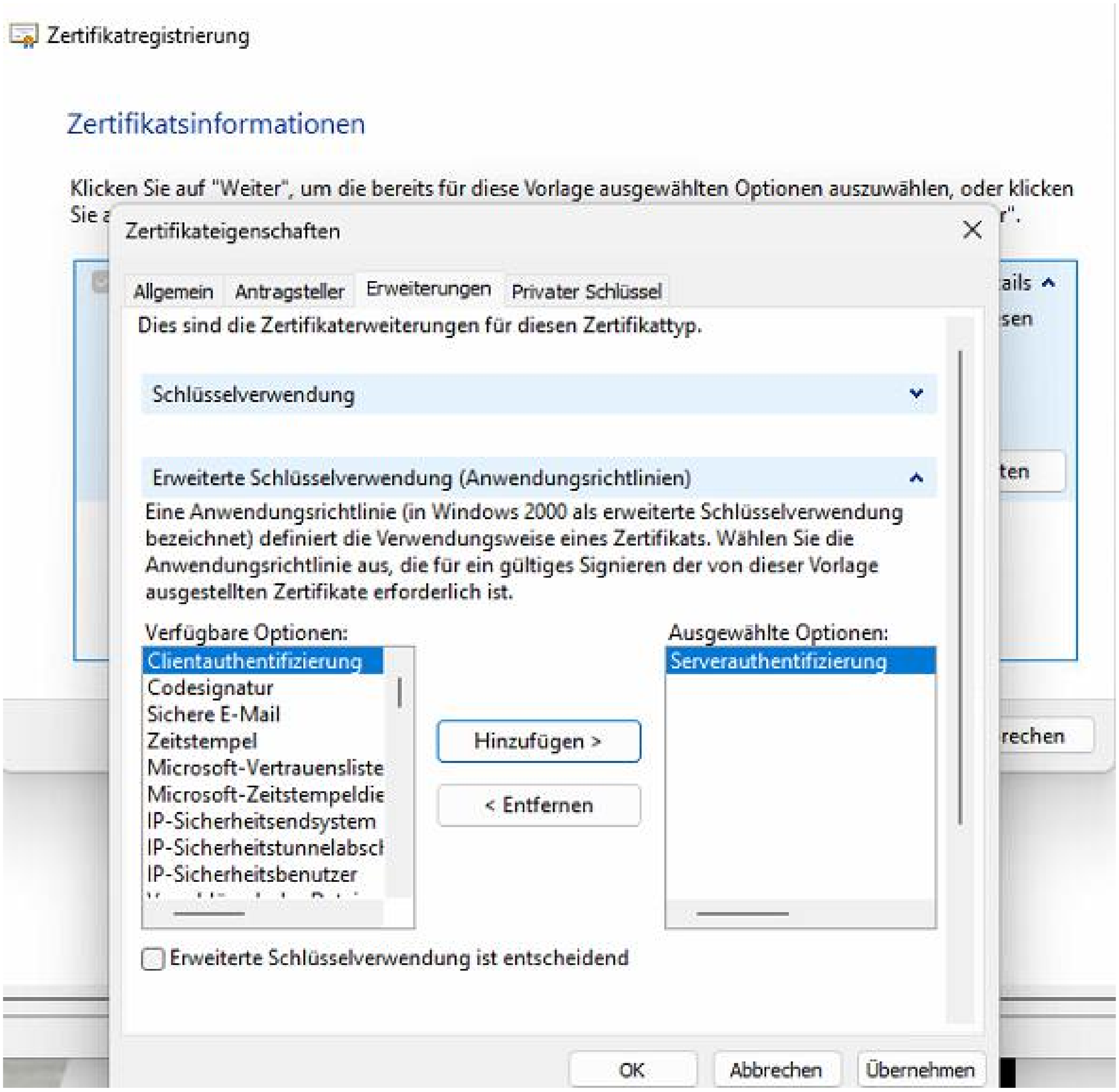
Hinzufügen >

< Entfernen

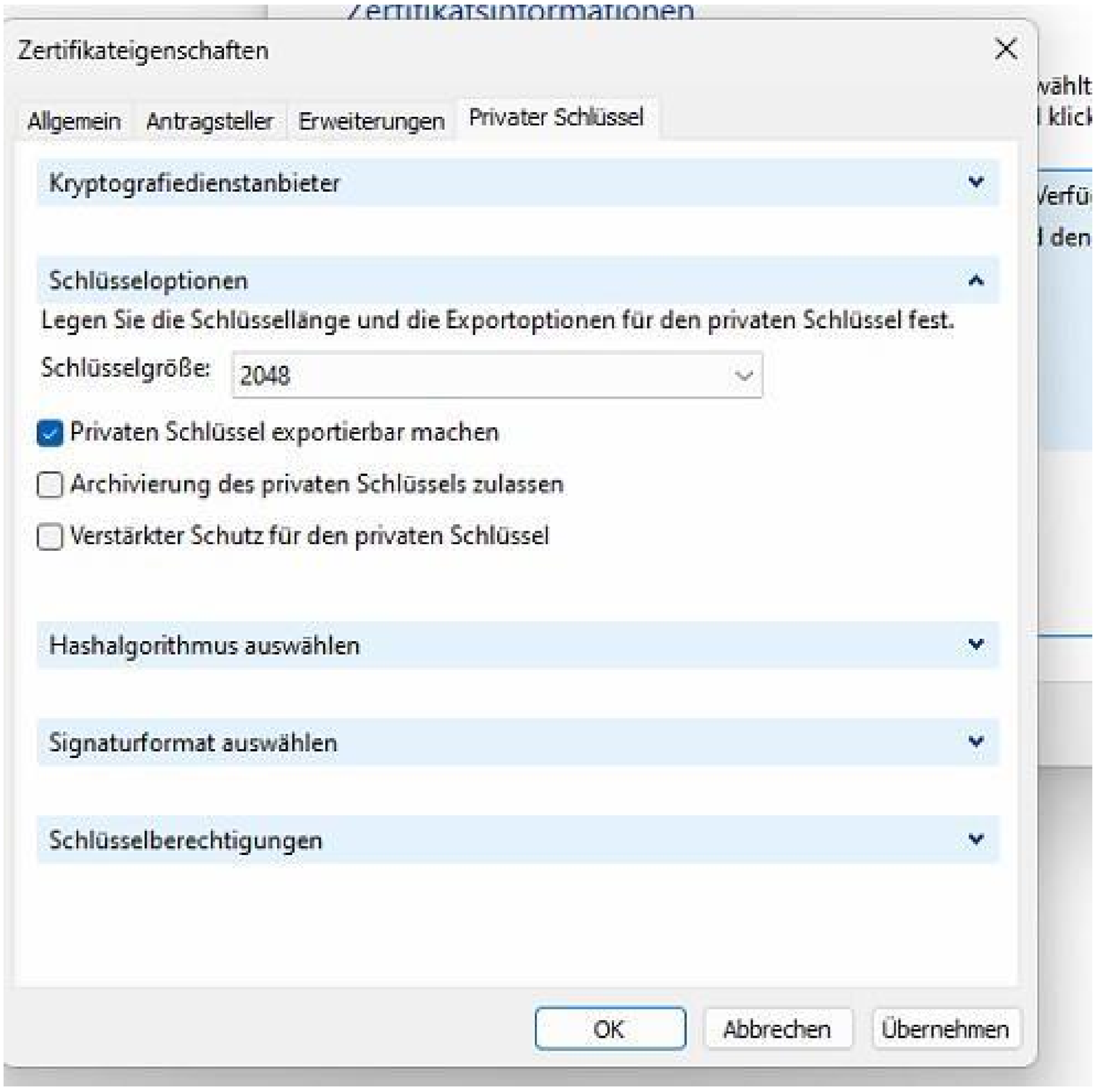
DNS
8CC9174XC3
IP-Adresse (v4)
10.172.2.53

OK | Abbrechen | Übernehmen

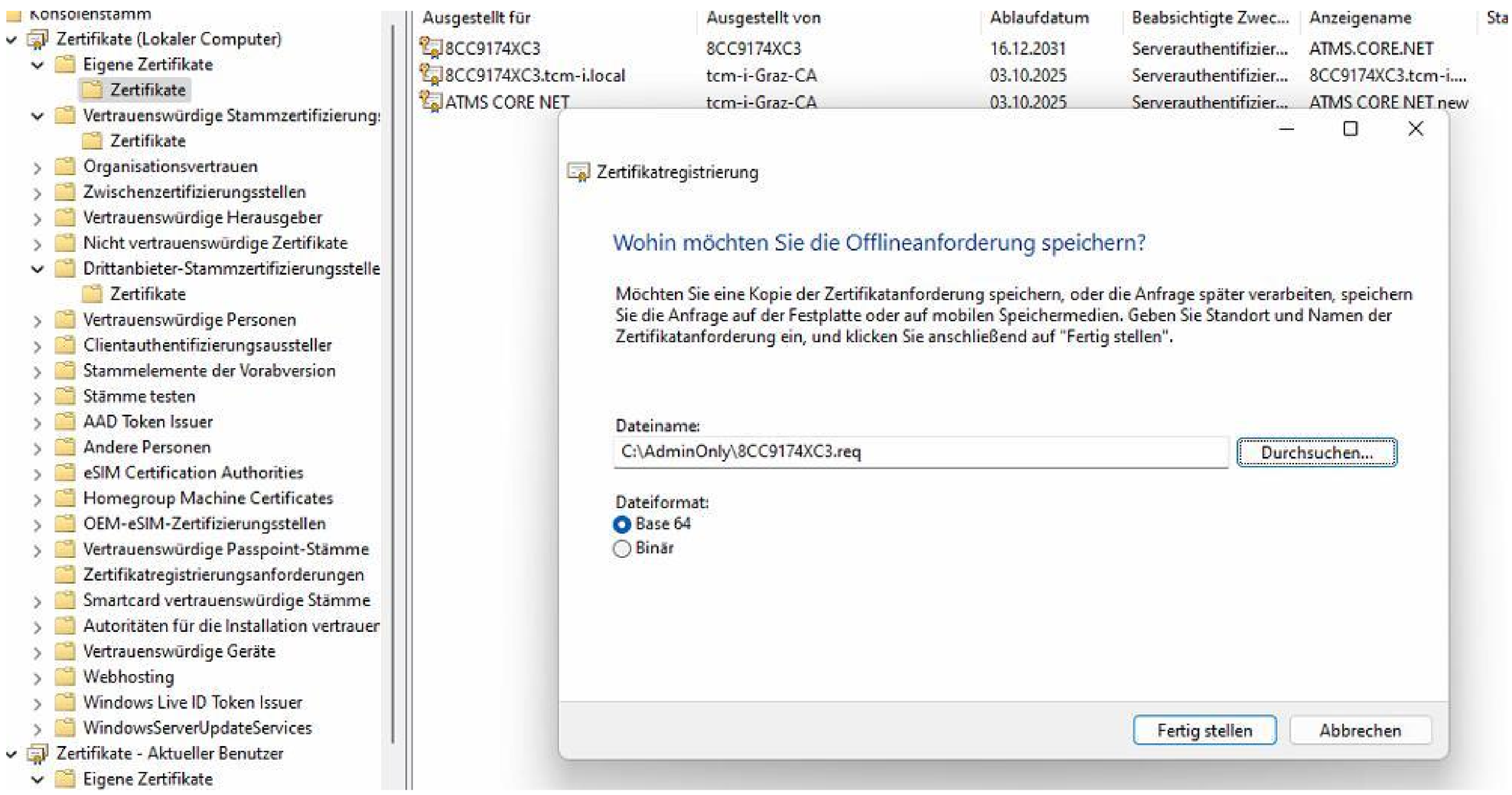
Erweiterungen – Erweiterte Schlüsselverwendung - Serverauthentifizierung



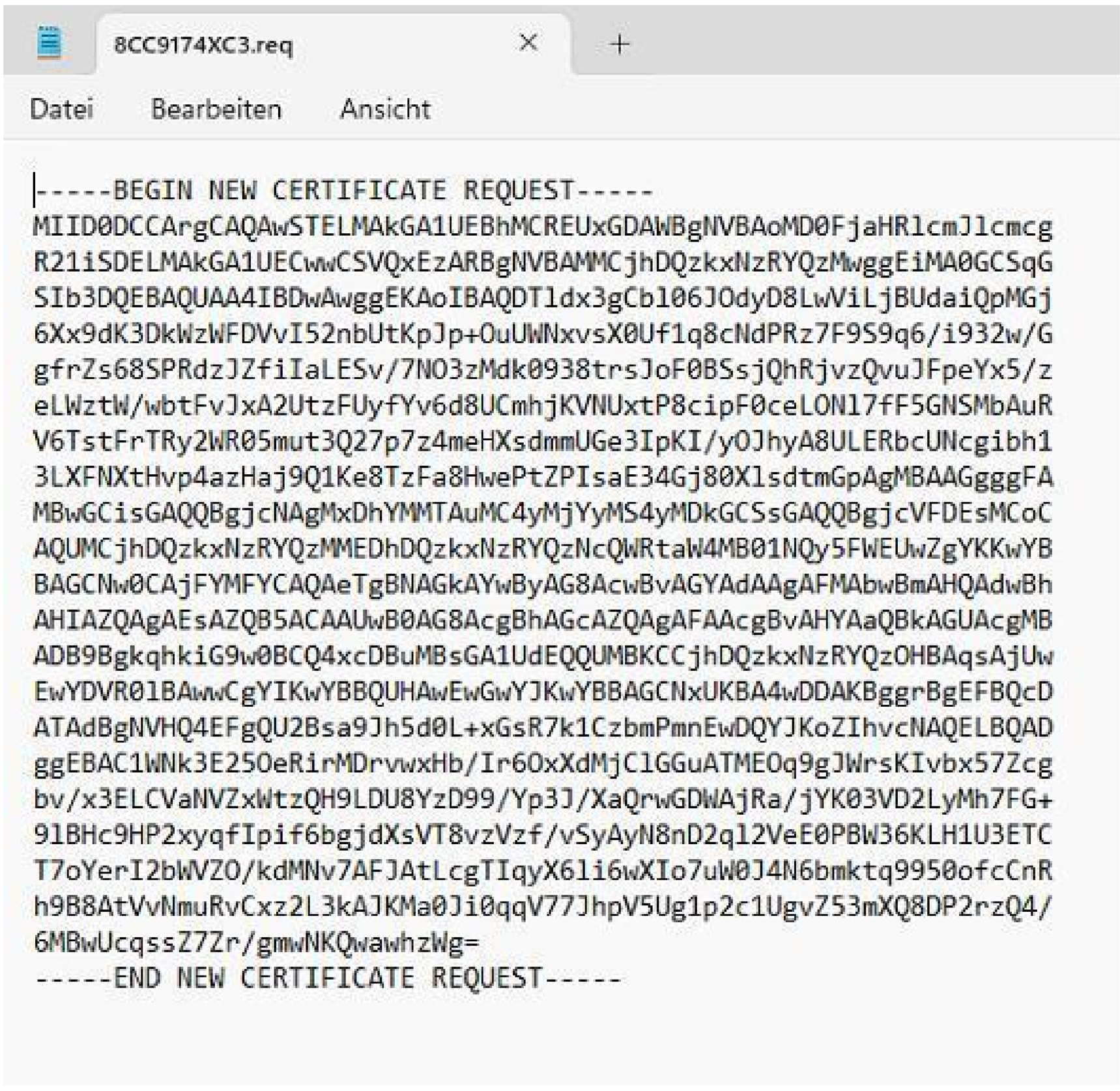
Privater Schlüssel – exportierbar machen (ermöglicht den Transfer des Schlüssels) Schlüsselgröße mind. 2048



Abspeichern der Anforderung.


Konsolenstamm
Zertifikate (Lokaler Computer)
Eigene Zertifikate
Zertifikate
Vertrauenswürdige Stammzertifizierung
Zertifikate
Organisationsvertrauen
Zwischenzertifizierungsstellen
Vertrauenswürdige Herausgeber
Nicht vertrauenswürdige Zertifikate
Drittanbieter-Stammzertifizierungsstelle
Zertifikate
Vertrauenswürdige Personen
Clientauthentifizierungsaussteller
Stammelemente der Vorabversion
Stämme testen
AAD Token Issuer
Andere Personen
eSIM Certification Authorities
Homegroup Machine Certificates
OEM-eSIM-Zertifizierungsstellen
Vertrauenswürdige Passpoint-Stämme
Zertifikatregistrierungsanforderungen
Smartcard vertrauenswürdige Stämme
Autoritäten für die Installation vertrauer
Vertrauenswürdige Geräte
Webhosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
Zertifikate - Aktueller Benutzer
Eigene Zertifikate
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

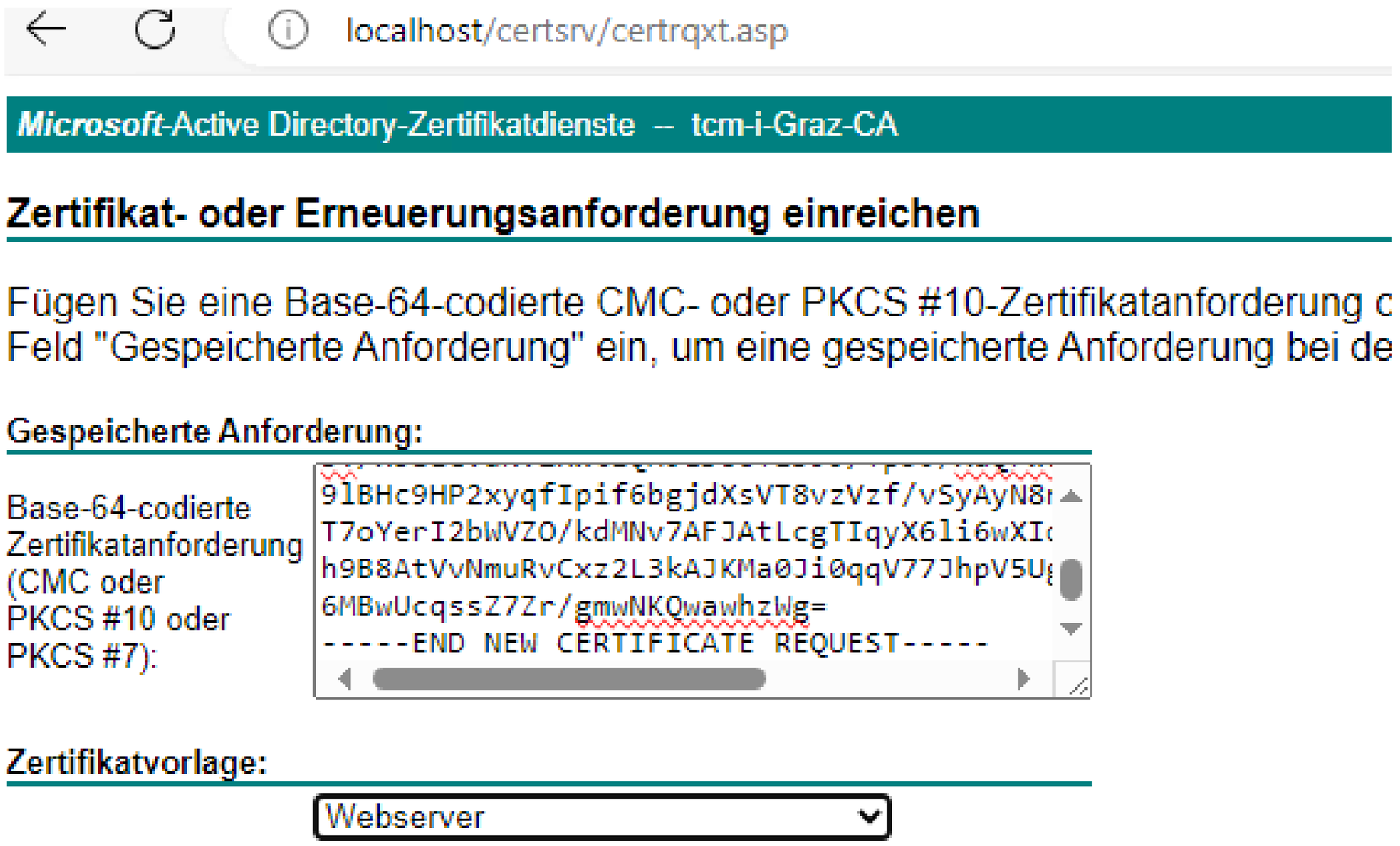
Datei mit Editor öffnen. Text kopieren.



Am Zertifizierungsstellen Server die Web Anwendung mit Browser öffnen

Text aus Zwischenablage in Feld gespeicherte Anforderung einfügen.

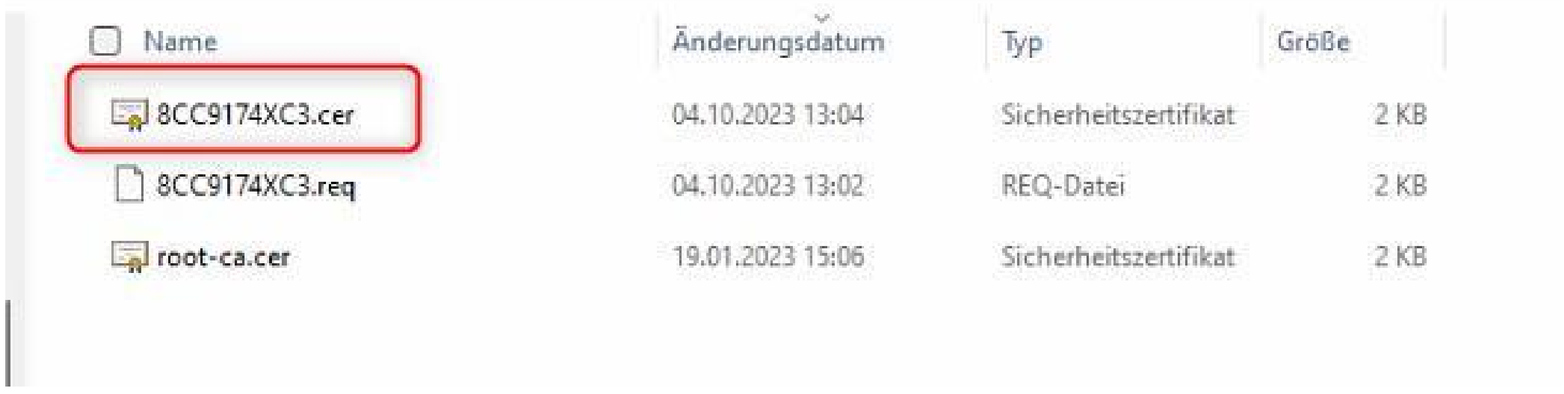
Auswahl Webserver



Einsenden.

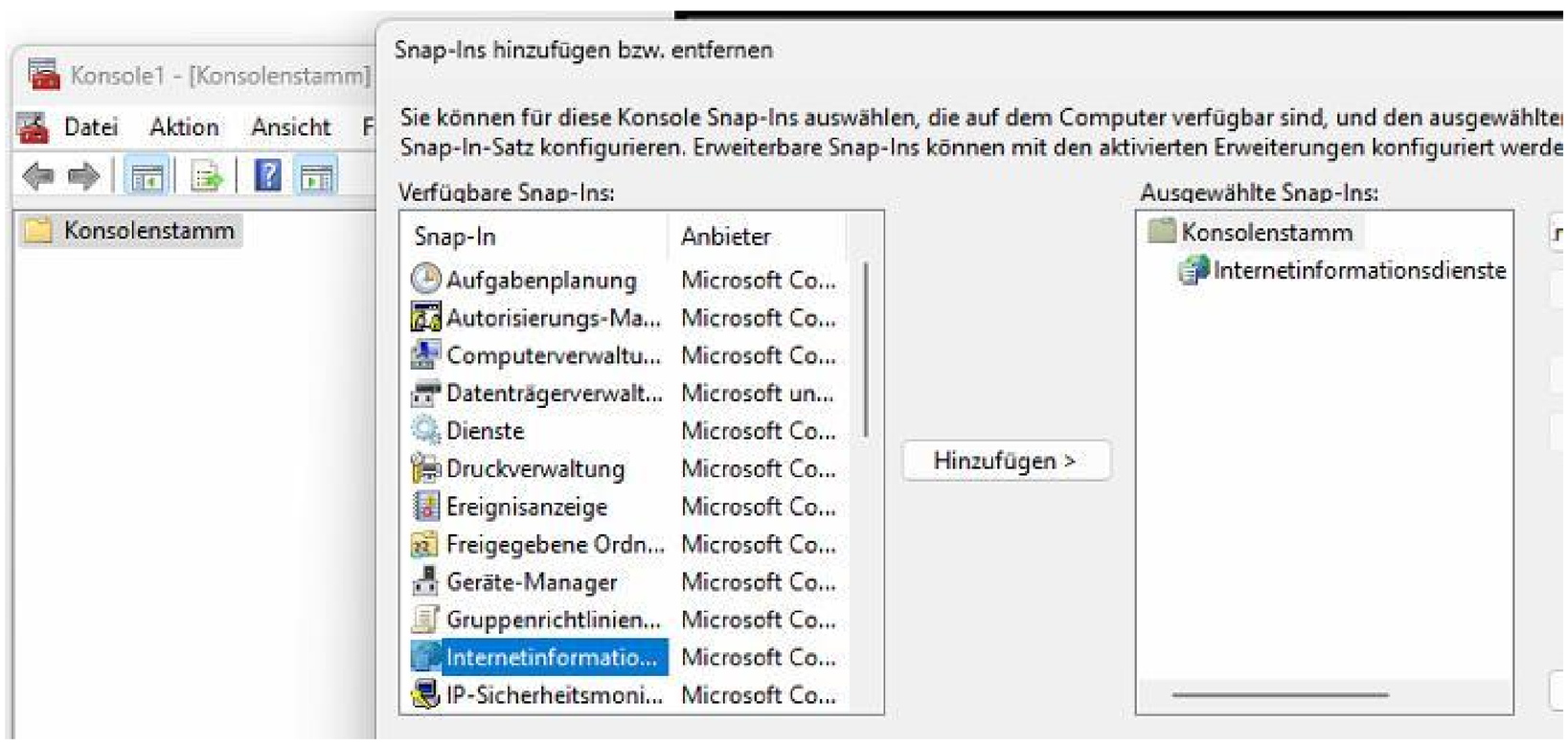
Download des Zertifikates. Empfehlung Base 64 codiert.

Transfer der cer Datei zum ATMS CORE NET Server.

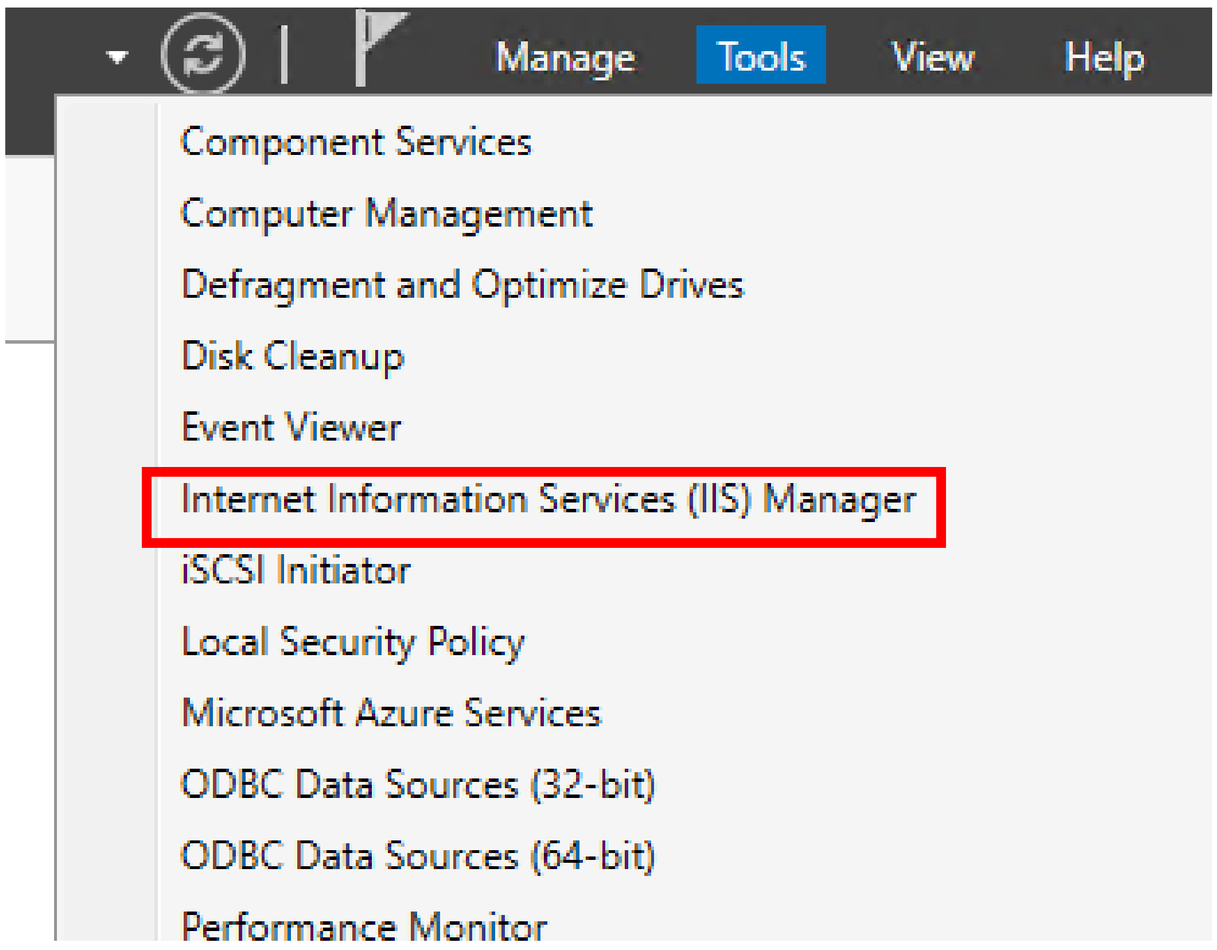


Client Betriebssysteme:

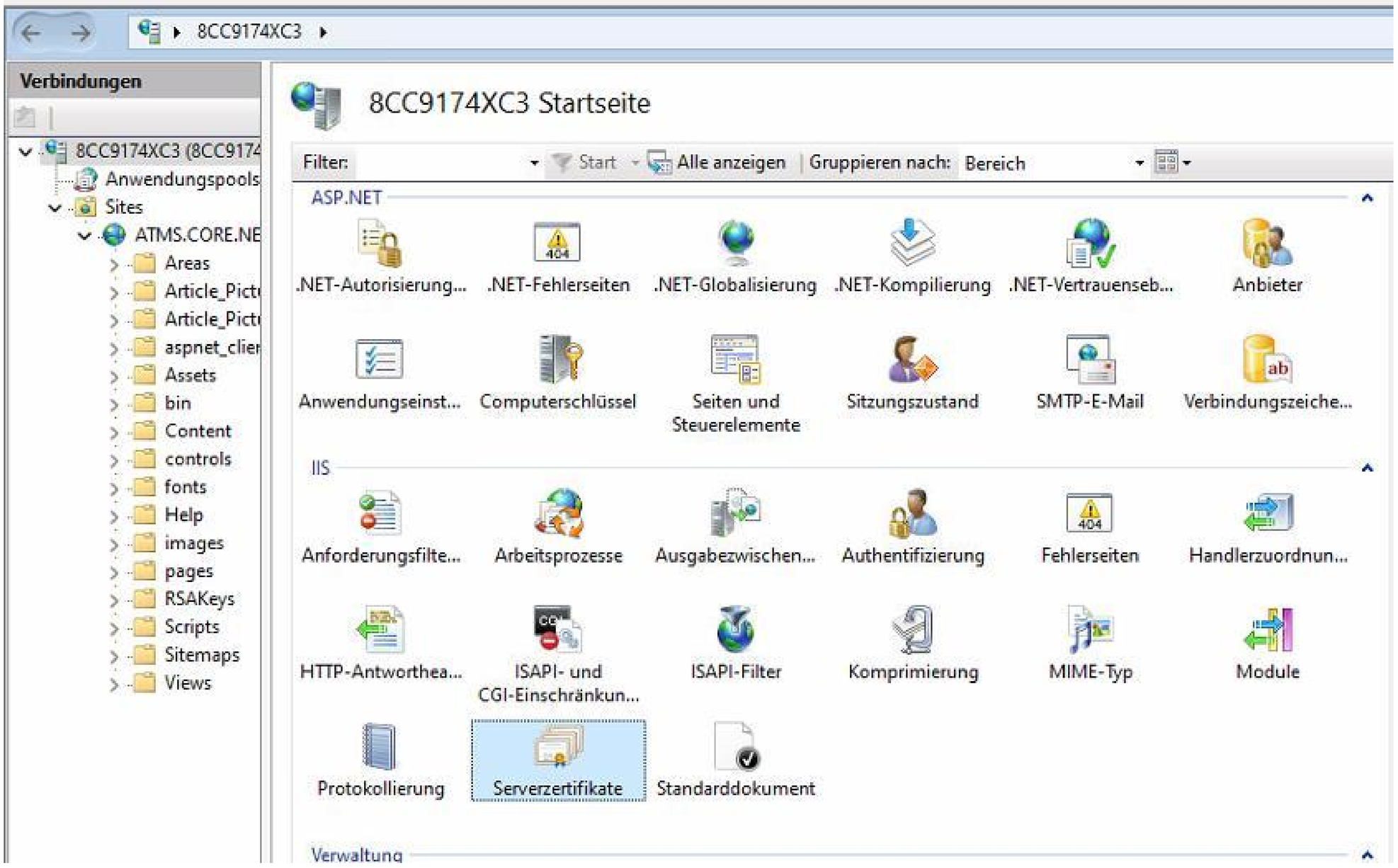
IIS Verwaltung Snap-in zu mmc hinzufügen.



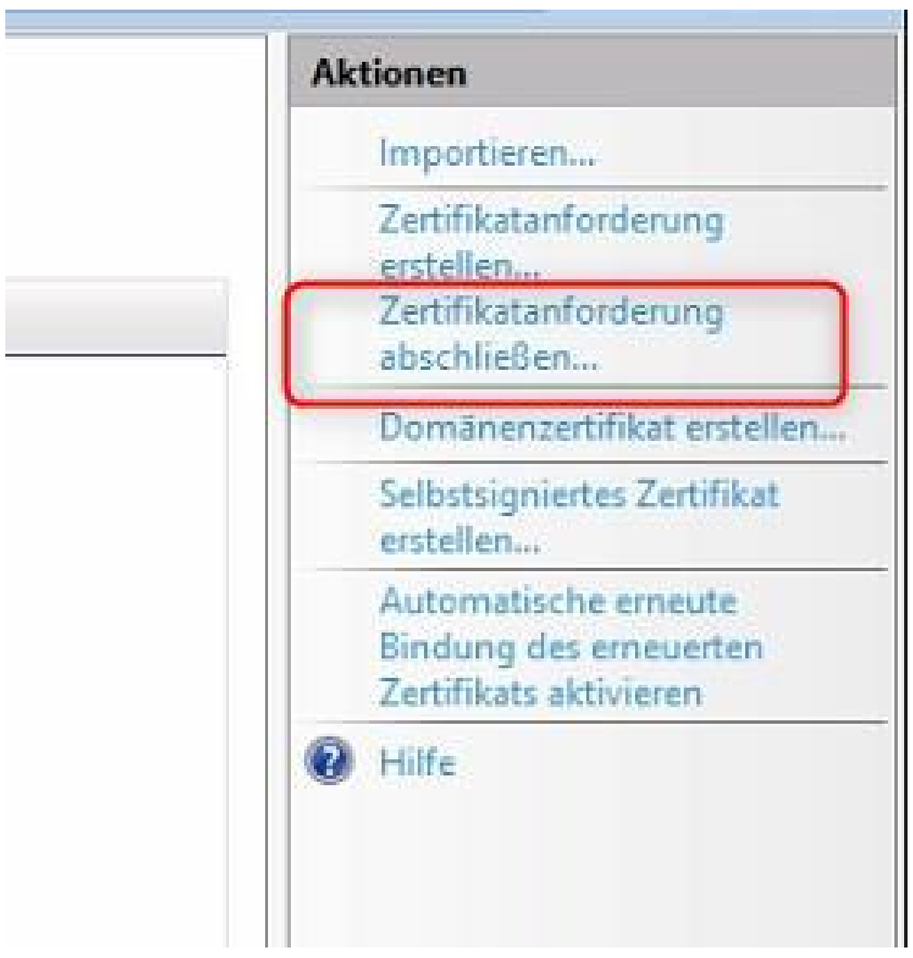
Server Betriebssysteme: Im Servermanager den Eintrag aufrufen.

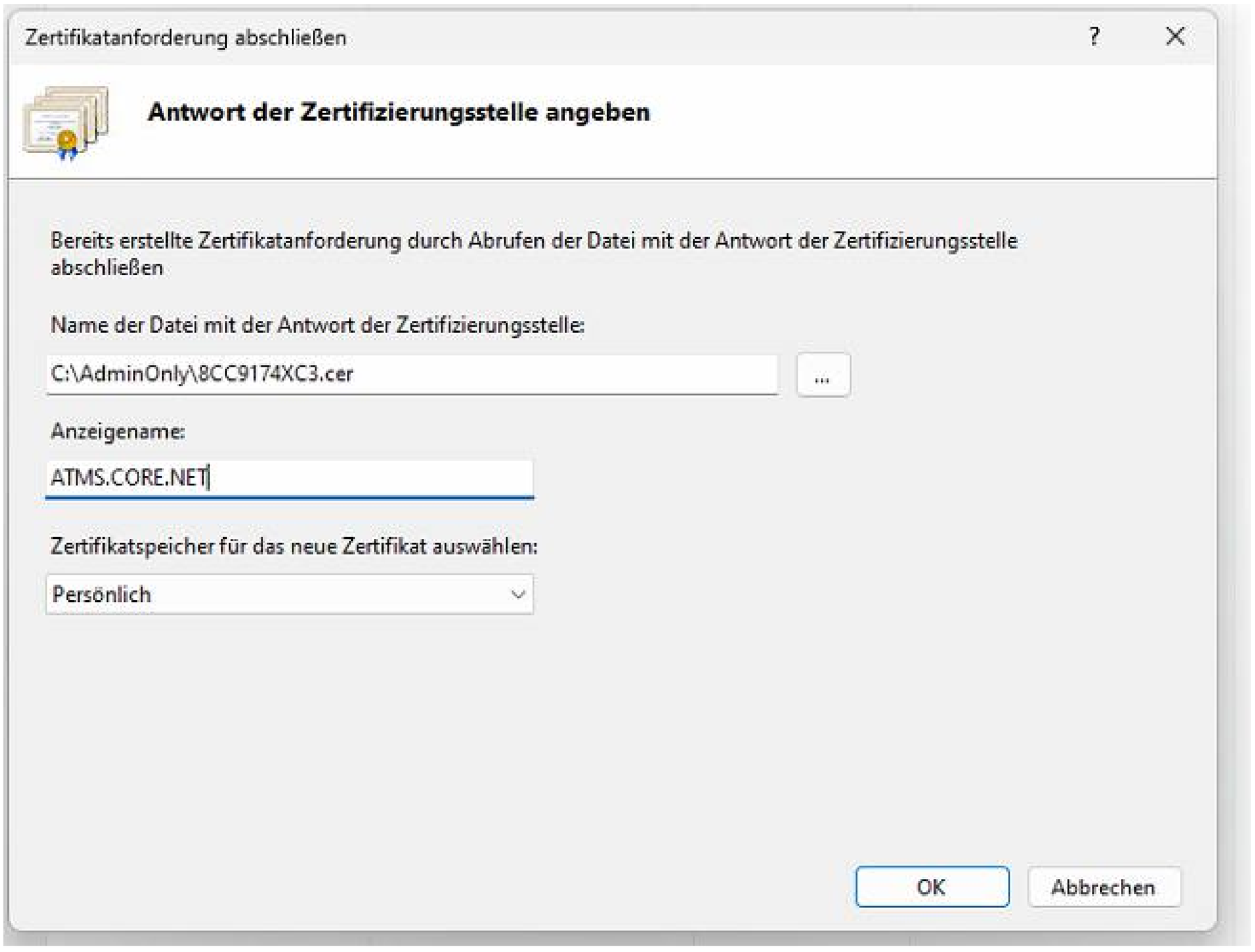


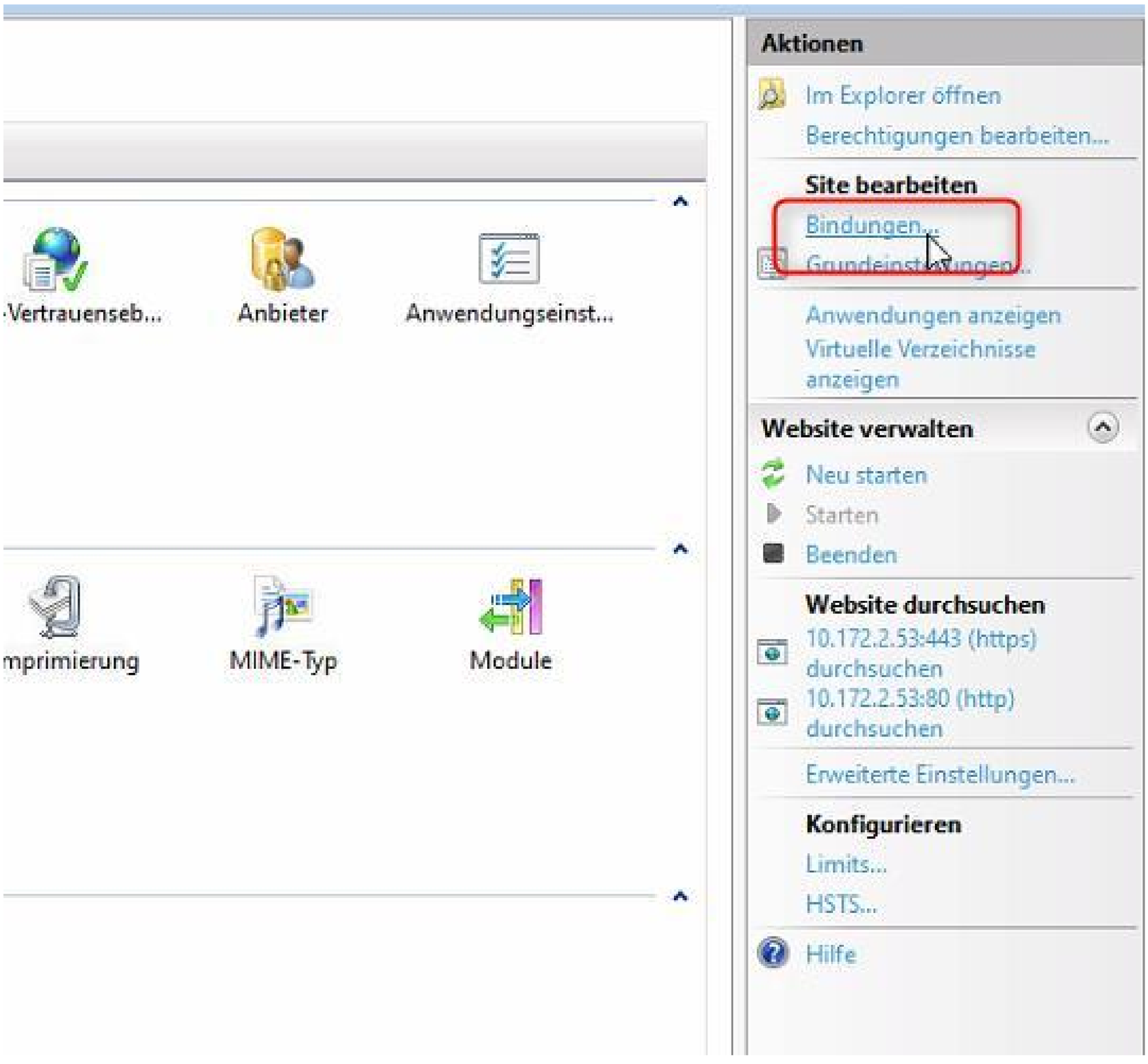
Server Zertifikate öffnen

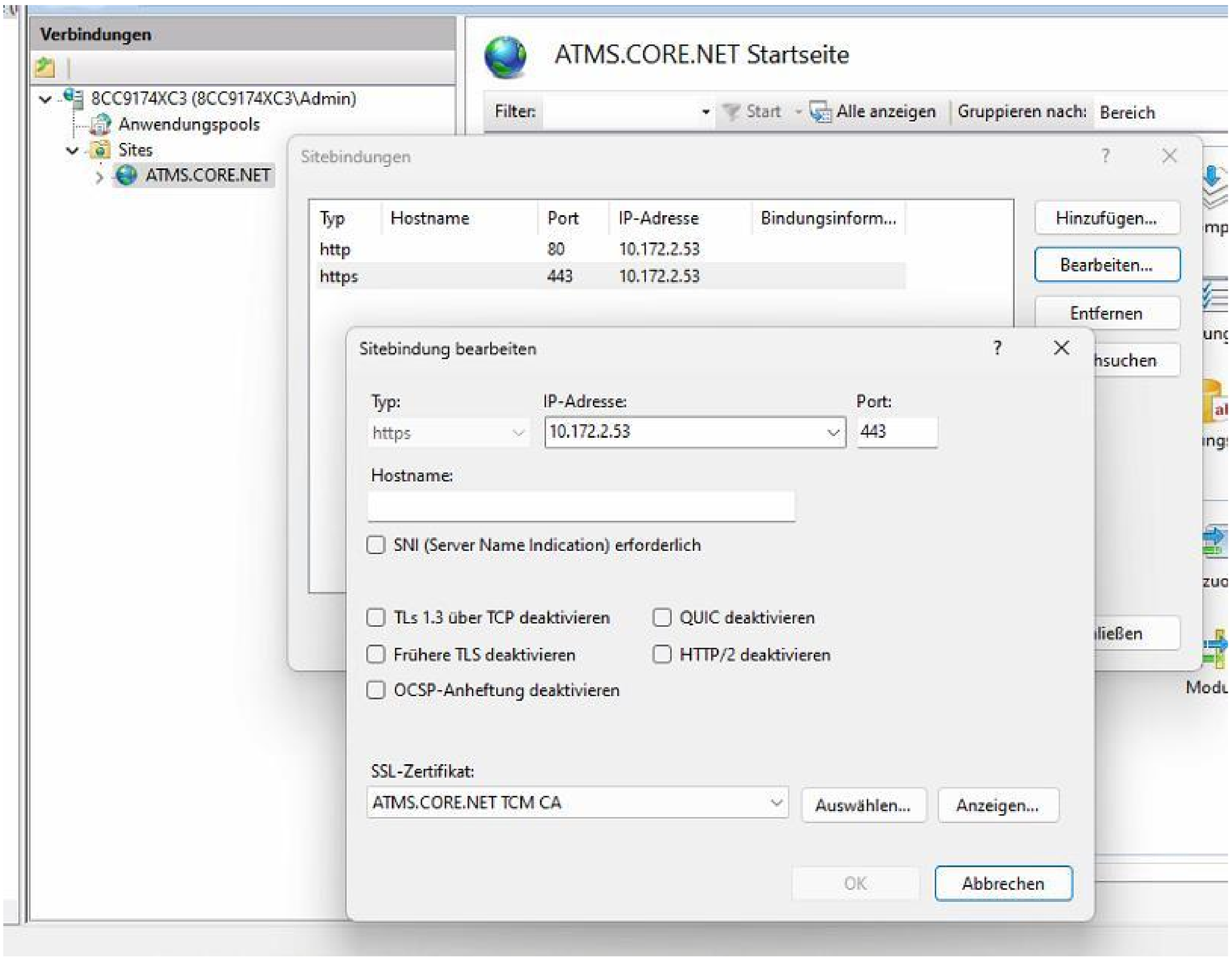


Zertifikatsanforderung abschließen…




Zertifikatanforderung abschließen
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:
C:\AdminOnly\8CC9174XC3.cer
...
Anzeigename:
ATMS.CORE.NET
Zertifikatspeicher für das neue Zertifikat auswählen:
Persönlich
OK
Abbrechen

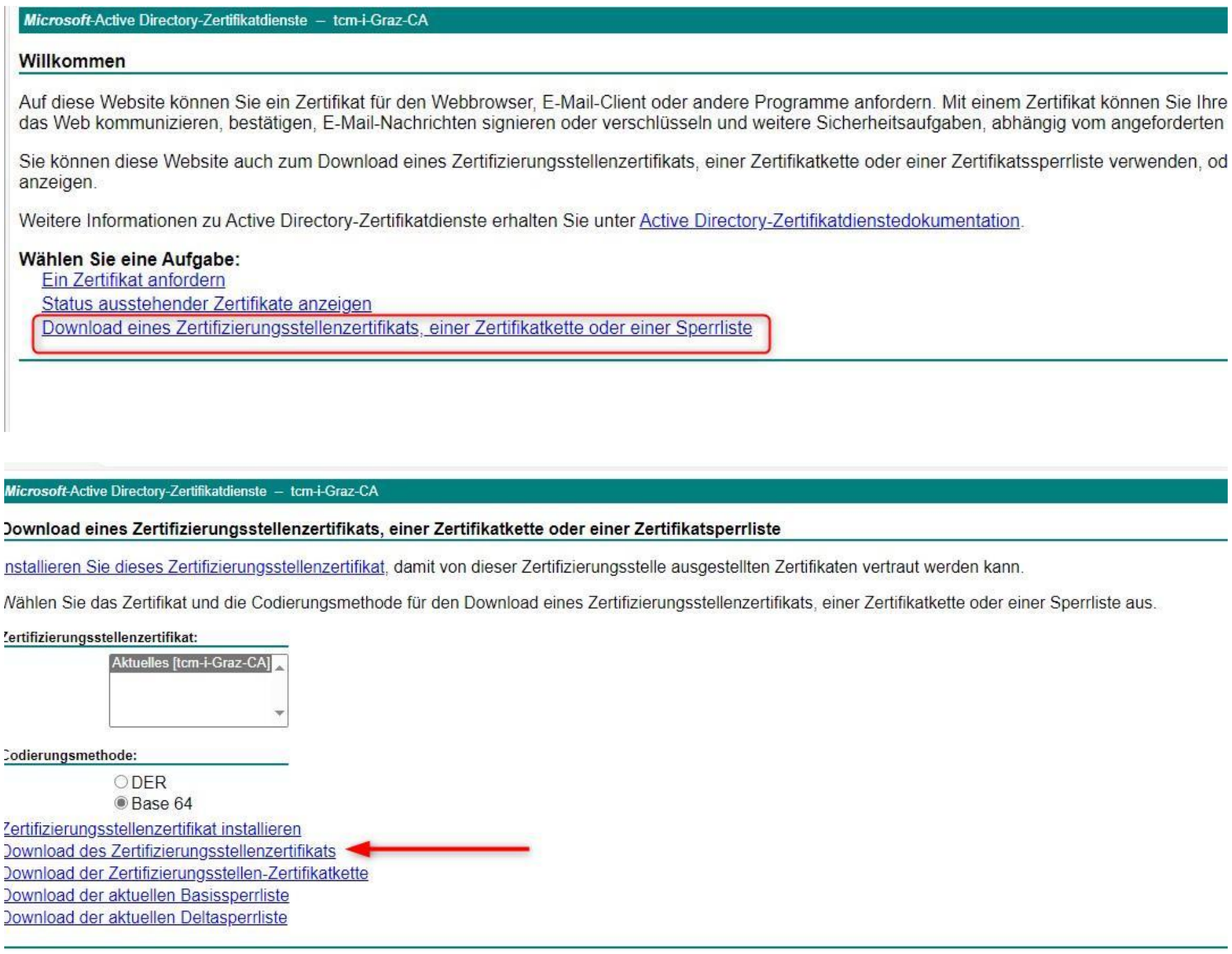

Aktionen
Im Explorer öffnen
Berechtigungen bearbeiten...
Site bearbeiten
Bindungen...
Grundeinstellungen...
Anwendungen anzeigen
Virtuelle Verzeichnisse anzeigen
Website verwalten
Neu starten
Starten
Beenden
Website durchsuchen
10.172.2.53:443 (https) durchsuchen
10.172.2.53:80 (http) durchsuchen
Erweiterte Einstellungen...
Konfigurieren
Limits...
HSTS...
Hilfe
Vertrauenseb...
Anbieter
Anwendungseinst...
mprimierung
MIME-Typ
Module


Verbindungen
8CC9174XC3 (8CC9174XC3\Admin)
Anwendungspools
Sites
ATMS.CORE.NET
ATMS.CORE.NET Startseite
Filter:
Start
Alle anzeigen
Gruppieren nach:
Bereich
Sitebindungen
Typ
Hostname
Port
IP-Adresse
Bindungsinform...
http
80
10.172.2.53
https
443
10.172.2.53
Hinzufügen...
Bearbeiten...
Entfernen
Sitebindung bearbeiten
Typ:
IP-Adresse:
Port:
https
10.172.2.53
443
Hostname:
SNI (Server Name Indication) erforderlich
TLs 1.3 über TCP deaktivieren
QUIC deaktivieren
Frühere TLS deaktivieren
HTTP/2 deaktivieren
OCSP-Anheftung deaktivieren
SSL-Zertifikat:
ATMS.CORE.NET TCM CA
Auswählen...
Anzeigen...
OK
Abbrechen

ATMSCORE

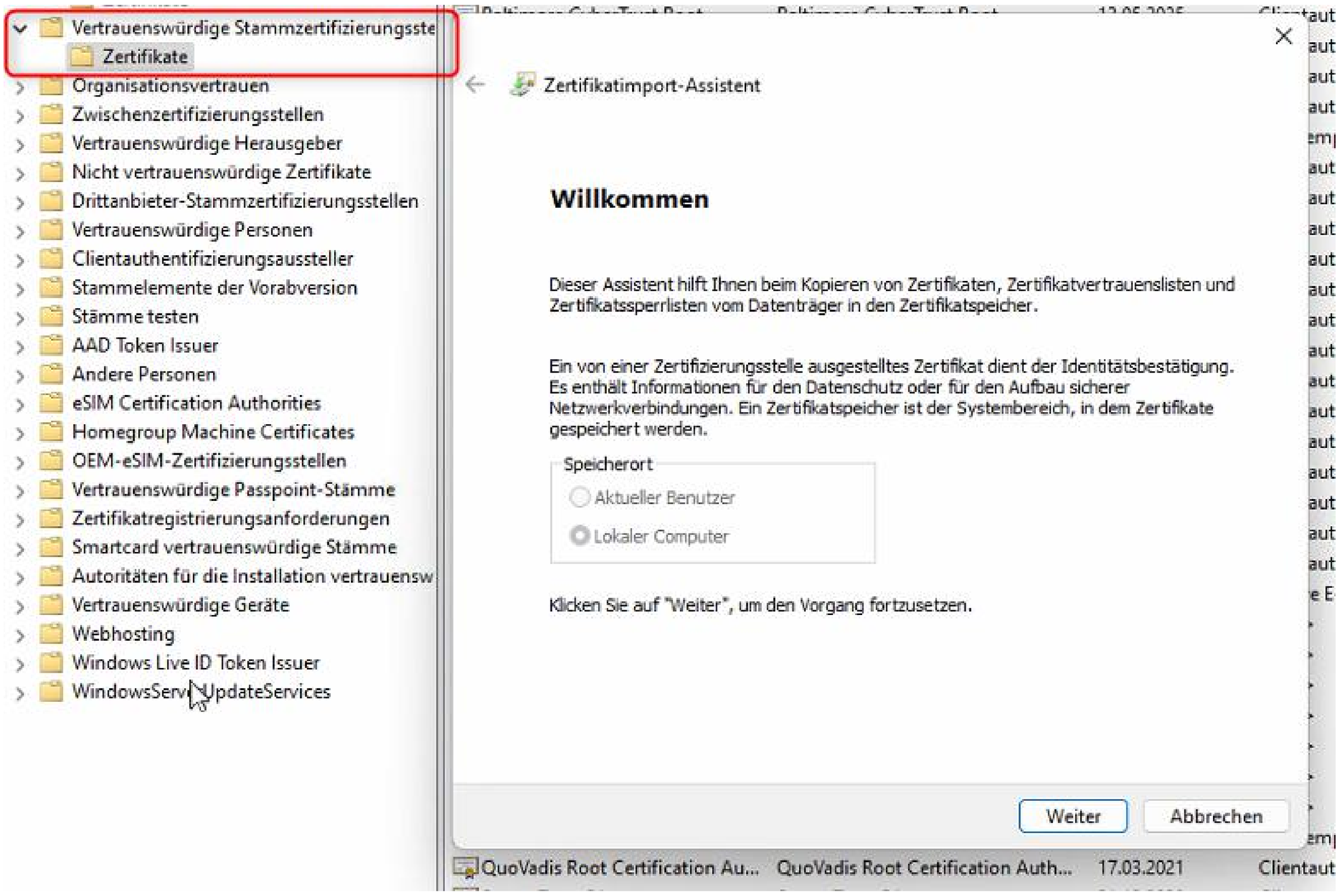
Root CA exportieren:

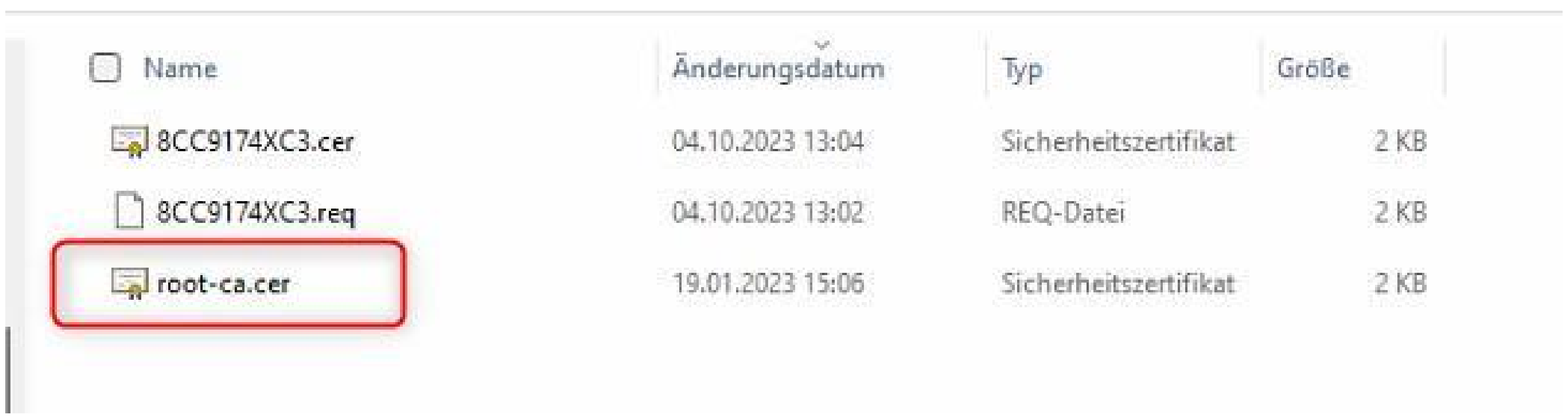
Am Zertifizierungsstellen Server mit Webanwendung

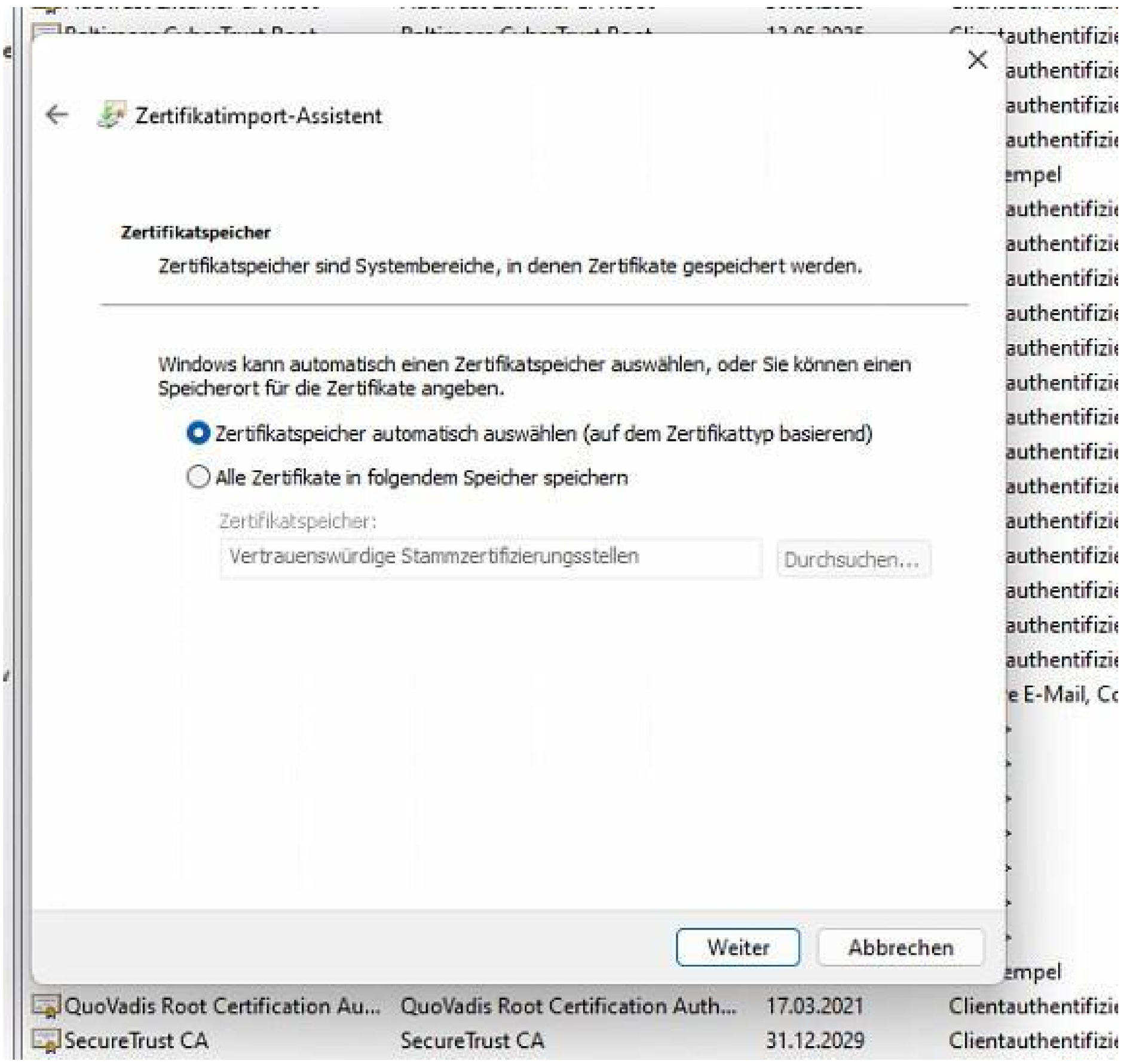


Root CA am ATMS CORE NET Server importieren:

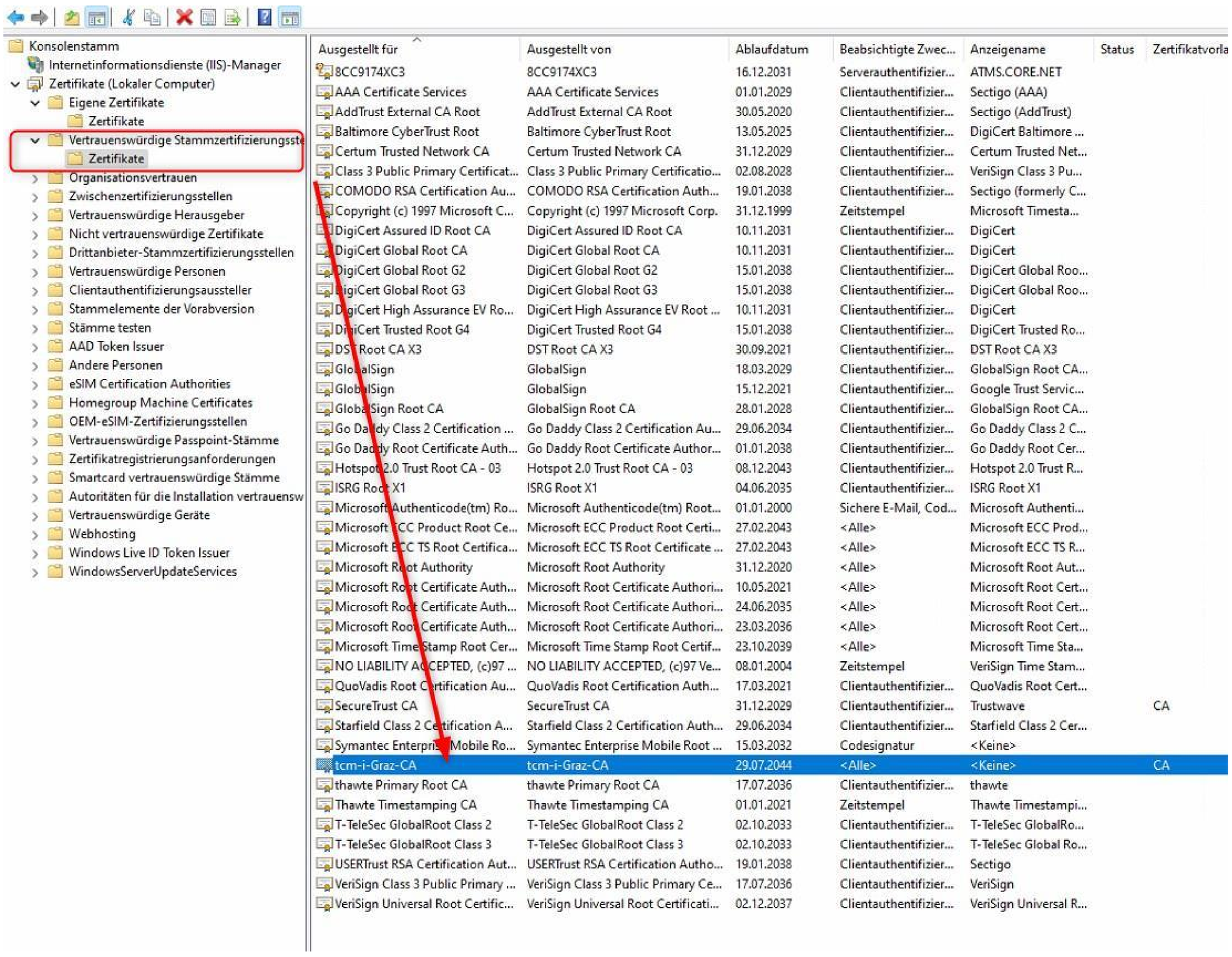
mmc Zertifikate (Computer)






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
SecureTrust CA
SecureTrust CA
31.12.2029

Kontrolle des Imports



Test der Webseite am ATMS CORE NET Server:

Es darf keine Warnung angezeigt werden.