



MOBOTIX HUB – Leitfaden für Zertifikate

V2.04

Inhaltsverzeichnis

1	URheberRECHT, MARKEN UND HAFTUNGSAUSSCHLUSS	4
2	ÜBER DIESEN LEITFADEN	5
3	WANN MÜSSEN SIE ZERTIFIKATE INSTALLIEREN?	6
4	EINFÜHRUNG IN ZERTIFIKATE	7
4.1	ZERTIFIKAT VERTEILUNG	8
5	ÜBERBLICK ÜBER DIE SZENARIEN UND VORGEHENSWEISEN, DIE MIT ATTESTE	10
5.1	MOBOTIX HUB MOBILER SERVER	10
5.2	MOBOTIX HUB MANAGEMENT SERVER UND RECORDING SERVER	10
5.3	ZERTIFIKAT EINER DRITTANBIETER- ODER KOMMERZIELLEN ZERTIFIZIERUNGSSTELLE	11
5.4	DOMÄNE	11
5.5	ARBEITSGRUPPE	11
5.6	MOBOTIX HUB EREIGNISSESERVER	11
5.7	KUNDE	11
6	WELCHE CLIENTS BENÖTIGEN ZERTIFIKATE?	13
7	SERVER-KONFIGURATOR (ERKLÄRT)	15
7.1	SERVER-ZERTIFIKAT	16
7.2	EREIGNISSESERVER UND ADD-ONS	17
7.3	ZERTIFIKAT FÜR STREAMING-MEDIEN	17
7.4	ZERTIFIKAT FÜR MOBILE STREAMING-MEDIEN	17
8	POWERSHELL-SKRIPTS	18
9	MANUELLES ERSTELLEN UND VERTEILEN VON ZERTIFIKATEN	19
9.1	WICHTIG ZU WISSEN:	19
9.2	ERSTELLEN EINES CA-ZERTIFIKATS	19
10	INSTALLIEREN VON ZERTIFIKATEN AUF DEN CLIENTS	22
11	SSL-ZERTIFIKAT ERSTELLEN	30

12	SSL-ZERTIFIKAT IMPORTIEREN	32
12.1	VERWALTEN SIE PRIVATE SCHLÜSSEL	38
13	ERSTELLEN EINES SSL-ZERTIFIKATS FÜR DEN FAILOVER-MANAGEMENT-SERVER	40
14	INSTALLIEREN ATTESTE FÜR DIE KOMMUNIKATION MIT DEM MOBILE SERVER	42
14.1	HINZUFÜGEN EINER ZERTIFIZIERUNGSSTELLE ZERTIFIKAT ZUM SERVER	42
14.2	LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN	51
14.3	AKTIVIEREN DER VERSCHLÜSSELUNG AUF DEM MOBILE SERVER	55
15	INSTALLIEREN VON ZERTIFIKATEN VON DRITTANBIETERN ODER KOMMERZIELLEN ZERTIFIZIERUNGSSTELLEN FÜR DIE KOMMUNIKATION MIT DEM MANAGEMENT SERVER ODER RECORDING SERVER	57
15.1	HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER	57
15.2	LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN	66
15.3	AKTIVIEREN DER VERSCHLÜSSELUNG ZUM UND VOM MANAGEMENT-SERVER	70
15.3.1	VORAUSSETZUNGEN:	70
15.3.2	SO INSTALLIEREN SIE AD CS:.....	73
15.4	INSTALLIEREN VON ZERTIFIKATEN IN EINER DOMÄNE FÜR DIE KOMMUNIKATION MIT DER MANAGEMENT-SERVER ODER DER AUFZEICHNUNGSSERVER	83
15.4.1	HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER	84
15.4.2	LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.	94
15.5	MANUELLES INSTALLIEREN DES ZERTIFIKATS	97
15.5.1	AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER ..	100
16	INSTALLIEREN ZERTIFIKATE IN EINER WORKGROUP-UMGEBUNG FÜR DIE KOMMUNIKATION MIT DEM MANAGEMENT SERVER ODER RECORDING SERVER	102
16.1	HINZUFÜGEN EINES ZERTIFIZIERUNGSSTELLENZERTIFIKATS ZUM SERVER	102
16.1.1	LADEN SIE DIE .REQ-DATEI HOCH, UM IM GEGENZUG EIN SIGNIERTES ZERTIFIKAT ZU ERHALTEN.	111
16.1.2	MANUELLES AUSSTELLEN VON ZERTIFIKATEN.....	115
16.1.3	AKTIVIEREN DER SERVERVERSCHLÜSSELUNG FÜR MANAGEMENT-SERVER UND AUFZEICHNUNGSSERVER ..	121
16.2	INSTALLIEREN VON ZERTIFIKATEN FÜR DIE KOMMUNIKATION MIT DEM EREIGNIS SERVER	122
16.3	ERMÖGLICHEN MOBOTIX HUB EVENT SERVER-VERSCHLÜSSELUNG	122
16.3.1	VORAUSSETZUNGEN:	122
16.3.2	IMPORTIEREN VON CLIENTZERTIFIKATEN	124
16.4	ANZEIGEN DES VERSCHLÜSSELUNGSSTATUS FÜR CLIENTS	129
16.4.1	ANZEIGEN DES VERSCHLÜSSELUNGSSTATUS AUF EINEM FAILOVER-AUFZEICHNUNGSSERVER	130

1 Urheberrecht, Marken und Haftungsausschluss

Copyright © 2025 MOBOTIX AG

Handelsmarken

MOBOTIX HUB ist eine eingetragene Marke der MOBOTIX AG.

Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Marke von Google Inc.

Alle anderen Marken, die in diesem Dokument erwähnt werden, sind Marken ihrer jeweiligen Eigentümer.

Verzichtserklärung

Dieser Text dient nur zu allgemeinen Informationszwecken und wurde mit der gebotenen Sorgfalt erstellt.

Jedes Risiko, das sich aus der Verwendung dieser Informationen ergibt, liegt beim Empfänger, und nichts in diesem Dokument sollte so ausgelegt werden, dass es irgendeine Art von Garantie darstellt.

Die MOBOTIX AG behält sich das Recht vor, ohne vorherige Ankündigung Anpassungen vorzunehmen.

Alle Namen von Personen und Organisationen, die in den Beispielen in diesem Text verwendet werden, sind fiktiv.

Jede Ähnlichkeit mit einer tatsächlichen Organisation oder Person, ob lebendig oder tot, ist rein zufällig und unbeabsichtigt.

Dieses Produkt kann Software von Drittanbietern verwenden, für die möglicherweise besondere Bedingungen gelten. Wenn dies der Fall ist, finden Sie weitere Informationen in der Datei

3rd_party_software_terms_and_conditions.txt, die sich in Ihrem Installationsordner für das MOBOTIX HUB-System befindet.

2 Über diesen Leitfaden

In diesem Leitfaden erhalten Sie eine Einführung in Verschlüsselung und Zertifikate sowie Schritt-für-Schritt-Verfahren zum Installieren von Zertifikaten in einer Windows Workgroup-Umgebung.

MOBOTIX empfiehlt, eine Public Key Infrastructure (PKI) für die Erstellung und Verteilung von Zertifikaten einzurichten. Eine PKI ist eine Reihe von Rollen, Richtlinien, Hardware, Software und Verfahren, die zum Erstellen, Verwalten, Verteilen, Verwenden, Speichern und Widerrufen digitaler Zertifikate sowie zum Verwalten der Public-Key-Verschlüsselung erforderlich sind. In einer Windows-Domäne wird empfohlen, eine PKI mithilfe der Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) einzurichten.

Wenn Sie keine PKI erstellen können, entweder weil verschiedene Domänen nicht vertrauenswürdig sind oder weil Domänen überhaupt nicht verwendet werden, ist es möglich, Zertifikate manuell zu erstellen und zu verteilen.

WARNUNG: Das manuelle Erstellen und Verteilen von Zertifikaten wird als sichere Methode zum Verteilen von Zertifikaten nicht empfohlen. Wenn Sie sich für die manuelle Verteilung entscheiden, sind Sie dafür verantwortlich, die privaten Zertifikate immer sicher aufzubewahren. Wenn Sie die privaten Zertifikate sicher aufbewahren, sind die Clientcomputer, die den Zertifikaten vertrauen, weniger anfällig für Angriffe.

3 Wann müssen Sie Zertifikate installieren?

Entscheiden Sie zunächst, ob Ihr System eine verschlüsselte Kommunikation benötigt.

Verwenden Sie keine Zertifikate mit Aufzeichnungsserververschlüsselung, wenn Sie eine oder mehrere Integrationen verwenden, die die HTTPS-Kommunikation nicht unterstützen. Dies sind z. B. MIP SDK-Integrationen von Drittanbietern, die HTTPS nicht unterstützen.

Sofern die Installation nicht in einem physisch isolierten Netzwerk erfolgt, wird empfohlen, die Kommunikation mithilfe von Zertifikaten zu sichern.

In diesem Dokument wird beschrieben, wann Zertifikate verwendet werden sollten:

- Wenn Ihr MOBOTIX HUB VMS-System in einer Windows Workgroup-Umgebung eingerichtet ist
- Bevor Sie MOBOTIX HUB VMS 2019 R1 oder höher installieren oder aktualisieren, wenn Sie die Verschlüsselung während der Installation aktivieren möchten.
- Bevor Sie die Verschlüsselung aktivieren, wenn Sie MOBOTIX HUB VMS 2019 R1 oder höher ohne Verschlüsselung installiert haben
- Wenn Sie Zertifikate aufgrund von Ablauf erneuern oder ersetzen

4 Einführung in Zertifikate

Hypertext Transfer Protocol Secure (HTTPS) ist eine Erweiterung des Hypertext Transfer Protocol (HTTP) für die sichere Kommunikation über ein Computernetzwerk. Bei HTTPS wird das Kommunikationsprotokoll mit Transport Layer Security (TLS) oder seinem Vorgänger Secure Sockets Layer (SSL) verschlüsselt.

In MOBOTIX HUB VMS wird eine sichere Kommunikation durch die Verwendung von TLS/SSL mit asymmetrischer Verschlüsselung (RSA) erreicht. TLS/SSL verwendet ein Schlüsselpaar – einen privaten, einen öffentlichen – um sichere Verbindungen zu authentifizieren, zu sichern und zu verwalten.

Eine Zertifizierungsstelle (Certificate Authority, CA) ist jeder, der Stammzertifikate ausstellen kann. Dabei kann es sich um einen Internetdienst handeln, der Stammzertifikate ausstellt, oder um eine Person, die ein Zertifikat manuell generiert und verteilt. Eine Zertifizierungsstelle kann Zertifikate für Webdienste ausstellen, d. h. für jede Software, die HTTPS-Kommunikation verwendet. Dieses Zertifikat enthält zwei Schlüssel, einen privaten Schlüssel und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird auf den Clients eines Web-Service (Service-Clients) installiert, indem ein öffentliches Zertifikat installiert wird. Der private Schlüssel wird zum Signieren von Serverzertifikaten verwendet, die auf dem Server installiert werden müssen.

Jedes Mal, wenn ein Dienstclient den Webdienst aufruft, sendet der Webdienst das Serverzertifikat einschließlich des öffentlichen Schlüssels an den Client. Der Dienstclient kann das Serverzertifikat mithilfe des bereits installierten Zertifikats der öffentlichen Zertifizierungsstelle validieren. Der Client und der Server können nun über die öffentlichen und privaten Serverzertifikate einen geheimen Schlüssel austauschen und so eine sichere TLS/SSL-Verbindung aufbauen.

Bei manuell verteilten Zertifikaten müssen Zertifikate installiert werden, bevor der Client eine solche Überprüfung durchführen kann .

Weitere Informationen zu TLS [finden Sie unter](#) Transport Layer Security.

In MOBOTIX HUB-VMS können Sie die TLS/SSL-Verschlüsselung an den folgenden Speicherorten aktivieren:

- Bei der Kommunikation zwischen dem Management-Server und den Aufzeichnungsservern, Ereignisservern und mobilen Servern
- Auf dem Aufzeichnungsserver in der Kommunikation mit Clients, Servern und Integrationen, die Datenströme vom Aufzeichnungsserver abrufen.

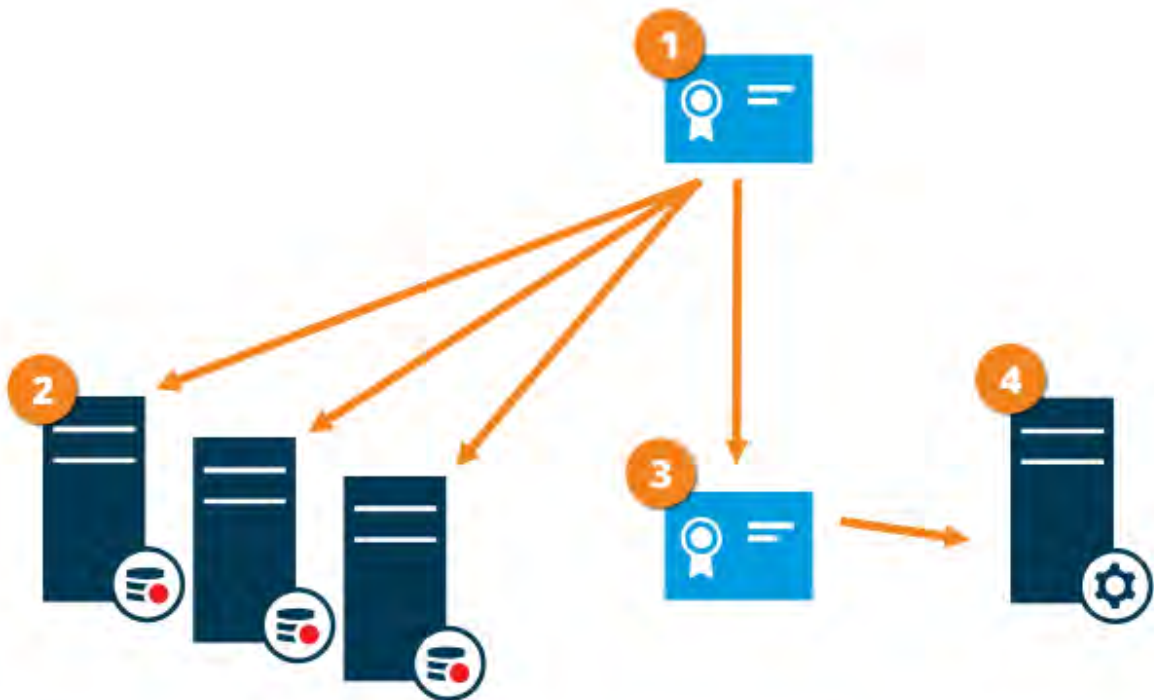
In der Kommunikation zwischen Clients und dem mobilen Server In diesem Handbuch werden die folgenden Personen als Clients bezeichnet:

- MOBOTIX HUB Desk Client
- Management-Client
- Management Server (für System Monitor und für Bilder und AVI-Videoclips in E-Mail-Benachrichtigungen)
- MOBOTIX HUB Mobiler Server
- MOBOTIX HUB Ereignisserver
- MOBOTIX HUB LPR
- MOBOTIX Open Network Bridge
- MOBOTIX HUB DLNA Server
- Sites, die Datenströme vom Aufzeichnungsserver über Milestone Interconnect abrufen
- MIP SDK-Integrationen von Drittanbietern, die HTTPS unterstützen

Für Lösungen, die mit MIP SDK 2018 R3 oder früher erstellt wurden und auf Aufzeichnungsserver zugreifen:- Wenn die Integrationen mithilfe von MIP SDK-Bibliotheken erstellt werden, müssen sie mit MIP SDK 2019 R1 neu erstellt werden- Wenn die Integrationen direkt mit den Aufzeichnungsserver-APIs kommunizieren, ohne MIP SDK-Bibliotheken zu verwenden, müssen die Integratoren selbst HTTPS-Unterstützung hinzufügen- Im Zweifelsfall Fragen Sie Ihren Anbieter, der die Integration bereitgestellt hat.

4.1 Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation mit dem Management-Server zu sichern.



- 1 Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Eigentümer (Management-Server) als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver), vertrauen
- 2 Das CA-Zertifikat muss auf allen Aufzeichnungsservern als vertrauenswürdig eingestuft werden. Auf diese Weise können die Aufzeichnungsserver die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen
- 3 Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen dem Management-Server und den Aufzeichnungsservern herzustellen
- 4 Das Zertifikat der Zertifizierungsstelle muss auf dem Computer installiert sein, auf dem der Verwaltungsserver ausgeführt wird

Anforderungen an das Zertifikat des privaten Verwaltungsservers:

- Wird für den Management-Server ausgestellt, sodass der Hostname des Management-Servers im Zertifikat enthalten ist, entweder als Antragsteller (Besitzer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird
- Vertrauenswürdig auf dem Management-Server selbst, indem das CA-Zertifikat als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde

- Vertrauenswürdig auf allen Aufzeichnungsservern, die mit dem Management-Server verbunden sind, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde



Zertifikate haben ein Ablaufdatum. Sie erhalten keine Warnung, wenn ein Zertifikat kurz vor dem Ablauf steht. Wenn ein Zertifikat abläuft, vertrauen die Clients dem Server nicht mehr mit dem abgelaufenen Zertifikat und können daher nicht mehr mit ihm kommunizieren.

Um die Zertifikate zu erneuern, führen Sie die Schritte in diesem Leitfaden wie beim Erstellen von

5 Übersicht über die Szenarien und Verfahren, die mit Zertifikaten verwendet werden

Die Verfahren für die Konfiguration der sicheren Kommunikation in einer MOBOTIX HUB VMS-Umgebung sind unterschiedlich, je nachdem, welche Art von Servern eine sichere Kommunikation erfordert.

Die Vorgehensweisen unterscheiden sich auch in einem WORKGROUP-Netzwerk von einem DOMAIN-Netzwerk.

Die Typen der MOBOTIX HUB VMS-Client-Anwendungen, die im System verwendet werden, bestimmen auch einige der erforderlichen Verfahren für eine sichere Kommunikation.



Die Verwendung von Zertifikaten für die Serverkommunikation kann in der Regel bei einer einzelnen Serverinstallation ignoriert werden, es sei denn, sie dienen als zusätzliche Sicherheit bei der Kommunikation mit dem Management-Server.

Diese Liste zeigt die verschiedenen Szenarien:

5.1 MOBOTIX HUB Mobiler Server

In MOBOTIX HUB-VMS wird die Verschlüsselung pro Mobile Server aktiviert oder deaktiviert. Sie aktivieren oder deaktivieren die Verschlüsselung entweder während der Installation des Produkts MOBOTIX HUB VMS oder mithilfe des Server-Konfigurators. Wenn Sie die Verschlüsselung auf einem Mobile Server aktivieren, verwenden Sie eine verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen, die Datenströme abrufen.

Der Mobile Server verbindet sich mit dem MOBOTIX HUB Mobile Client und dem MOBOTIX HUB Web Client.

Browser, Betriebssysteme und mobile Geräte, die diese Clients hosten, verwalten eine Liste vertrauenswürdiger CA-Stammzertifikate. Nur die Autorität kennt ihren privaten Schlüssel, aber jeder kennt ihren öffentlichen Schlüssel, der einem bestimmten Zertifikat ähnelt.

Auf diesen Clients sind dann bereits Zertifikatschlüssel installiert, und sie funktionieren mit den meisten Zertifikaten von Drittanbietern, die für die Installation auf dem Mobile Server selbst verfügbar sind.

Da jede Drittanbieter-CA ihre eigenen Anforderungen für die Beantragung eines Zertifikats hat, ist es am besten, die einzelnen Anforderungen direkt mit der CA zu erörtern.

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatsanforderung auf dem Mobile Server erstellen und das Zertifikat installieren, sobald es von der Zertifizierungsstelle ausgestellt wurde.

Siehe:

[Installieren von Zertifikaten für die Kommunikation mit dem Mobile Server auf Seite 40](#)

5.2 MOBOTIX HUB Management Server und Recording Server

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, gilt sie für Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Management-Server herstellen.

Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, müssen Sie auch die Verschlüsselung auf allen Aufzeichnungsservern aktivieren. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Management-Server und allen Aufzeichnungsservern, einschließlich Failover-Aufzeichnungsservern, installieren.

5.3 Zertifikat einer Drittanbieter- oder kommerziellen Zertifizierungsstelle

Das Verfahren zum Anfordern von Zertifikaten von Zertifizierungsstellen von Drittanbietern für die Verwendung mit Management-Servern und Aufzeichnungsservern ist identisch mit dem für den Mobile Server. Der einzige Unterschied ist die Konfiguration mit dem Server Konfigurator.

Siehe:

[Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder Recording Server auf Seite 57](#)

5.4 Domäne

Wenn Client- und Serverendpunkte alle in einer Domänenumgebung mit einer eigenen Zertifizierungsstelleninfrastruktur betrieben werden, ist es nicht erforderlich, CA-Zertifikate an Client-Workstations zu verteilen. Solange Sie über eine Gruppenrichtlinie innerhalb der Domäne verfügen, die die automatische Verteilung aller Zertifikate der vertrauenswürdigen Zertifizierungsstelle an alle Benutzer und Computer in der Domäne verarbeitet.

Das Anfordern eines Zertifikats und das Installieren eines Serverzertifikats ist identisch mit dem in einer Arbeitsgruppe.

Siehe:

[Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86](#)

5.5 Arbeitsgruppe

Beim Betrieb in einer Workgroup-Umgebung wird davon ausgegangen, dass keine Infrastruktur für Zertifizierungsstellen vorhanden ist. Zum Verteilen von Zertifikaten ist es erforderlich, eine Zertifizierungsstelleninfrastruktur zu erstellen. Es ist auch erforderlich, die Zertifikatsschlüssel an Client-Workstations zu verteilen. Abgesehen von diesen Anforderungen ähnelt der Prozess zum Anfordern und Installieren eines Zertifikats auf einem Server sowohl dem Domänen- als auch dem Drittanbieterszenario.

Siehe:

[Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104](#)

5.6 MOBOTIX HUB Ereignisserver

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln. Wenn Sie die Verschlüsselung auf dem Ereignisserver aktivieren, gilt sie für Verbindungen von allen Komponenten, die eine Verbindung mit dem Ereignisserver herstellen. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Ereignisserver und allen Verbindungskomponenten installieren.

Siehe:

[Installieren von Zertifikaten für die Kommunikation mit dem Ereignisserver auf Seite 126](#)

5.7 Kunde

In den Szenarien Drittanbieter/Kommerziell und Domäne müssen Clients keine Zertifikatschlüssel installieren. Sie müssen Clientzertifikatschlüssel nur in einer Arbeitsgruppenumgebung installieren.

Wenn Sie die Verschlüsselung auf einem Aufzeichnungsserver aktivieren, wird die Kommunikation mit allen Clients, Servern und Integrationen, die Datenströme vom Aufzeichnungsserver abrufen, verschlüsselt.

In diesem Dokument werden diese als "Clients" für den Aufzeichnungsserver bezeichnet:

- MOBOTIX HUB Desk Client
- Management-Client
- Management Server (für System Monitor und für Bilder und AVI-Videoclips in E-Mail-Benachrichtigungen)
- MOBOTIX HUB Mobiler Server
- MOBOTIX HUB Ereignisserver
- MOBOTIX HUB LPR
- MOBOTIX Netzwerkbrücke
- MOBOTIX HUB DLNA Server
- Standorte, die Datenströme vom Aufzeichnungsserver über MOBOTIX Interconnect abrufen
- Einige MIP SDK-Integrationen von Drittanbietern



Für Lösungen, die mit MIP SDK 2018 R3 oder früher erstellt wurden und auf Aufzeichnungsserver zugreifen: Wenn die Integrationen mithilfe von MIP SDK-Bibliotheken erstellt werden, müssen sie mit MIP SDK 2019 R1 neu erstellt werden. Wenn die Integrationen direkt mit den Aufzeichnungsserver-APIs kommunizieren, ohne MIP SDK-Bibliotheken zu verwenden, müssen die Integrierten selbst HTTPS-

Siehe:

[Welche Clients benötigen Zertifikate? auf Seite 11](#)

[Importieren von Client-Zertifikaten auf Seite 129](#)


6 Welche Clients benötigen Zertifikate?

Auf welchen Clients müssen Zertifikate installiert werden? Wie planen wir das? Was können wir tun, um uns vorzubereiten?

Für webbrowsersbasierte Clients und Clients, die über einen öffentlichen Anwendungsverteilungsdienst oder -store eines Drittanbieters, z. B. Google Play oder Apple AppStore, vertrieben werden, sollten Sie kein Zertifikat installieren müssen. MOBOTIX HUB Mobile verwendet keine installierten Zertifikate. MOBOTIX HUB Mobile kann nur vertrauenswürdige Zertifikate von Drittanbietern verwenden.

Wenn die MOBOTIX HUB-Server (Management Server und Recording Server) auf Computern installiert sind, die der Domäne beigetreten sind, und die Benutzer, die sich beim Desk Client anmelden, alle Domänenbenutzer sind, übernimmt die Domäne die Verteilung und Authentifizierung öffentlicher Schlüssel, die für die Einrichtung einer sicheren Kommunikation erforderlich sind.

Third Party CA/ Domain	Self Signed CA / Domain
Third Party CA/ Non-Domain	Self Signed CA/ Non-Domain

 No Public Key Distribution Needed

 Public Key Distribution Needed

Nur in einem Szenario, in dem Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) zum Erstellen selbstsignierter Zertifikate verwendet werden und die Ressourcen (Benutzer und Computer) in einer Nicht-Domänenumgebung ausgeführt werden, besteht die Notwendigkeit, öffentliche Schlüssel an Clientarbeitsstationen zu verteilen.

Siehe auch [Installieren von Zertifikaten auf den Clients auf Seite 19](#) und [Importieren von Client-Zertifikaten auf Seite 129](#).

7 Server-Konfigurator (erklärt)

Verwenden Sie den Server-Konfigurator, um Zertifikate auf lokalen Servern für die verschlüsselte Kommunikation auszuwählen und Serverdienste zu registrieren, um sie für die Kommunikation mit den Servern zu qualifizieren.

Die folgenden Servertypen in MOBOTIX HUB VMS benötigen Zertifikate für eine sichere Kommunikation:

- Verwaltungsserver
- Aufzeichnen von Servern
- Ereignisserver
- Mobile Server

Diese Server arbeiten mit dem Server-Konfigurator zusammen, um die sichere Kommunikation zu verwalten.

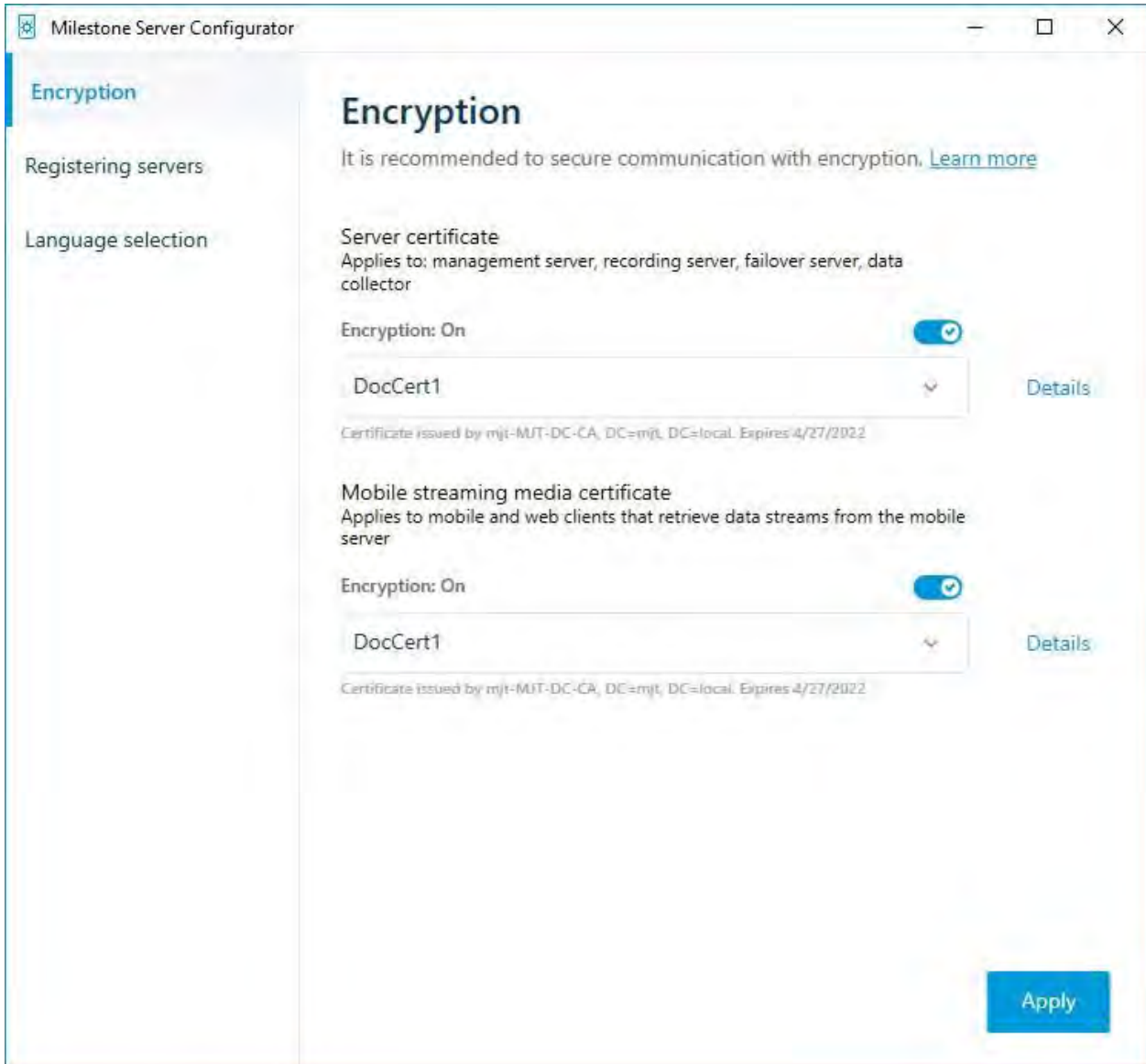
Verwenden Sie den Server-Konfigurator, um festzulegen, ob die MOBOTIX HUB-Server eine sichere verschlüsselte Kommunikation verwenden oder nicht, und um die Zertifikate zu verwalten, die von den MOBOTIX HUB-Servern verwendet werden.

Der Server Configurator wird standardmäßig auf jedem Computer installiert, auf dem ein MOBOTIX HUB-Server gehostet wird. Öffnen Sie den Server-Konfigurator über:

- Das Windows-Startmenü

oder

- Den MOBOTIX HUB-Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken und Server-Konfigurator auswählen



Verwenden Sie den Server-Konfigurator, um die Zertifikate auszuwählen, die die MOBOTIX HUB-Server verwenden, um die Kommunikation mit ihren Client-Anwendungen zu sichern, und um zu überprüfen, ob die Verschlüsselungseinstellungen ordnungsgemäß konfiguriert sind.

7.1 Server-Zertifikat

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der bidirektionalen Verbindung zwischen dem Management-Server und den folgenden Servern verwendet werden soll:

- Aufzeichnungsserver
- Ereignisserver
- Protokollserver
- LPR-Server
- Mobiler Server

7.2 Ereignisserver und Add-ons

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der bidirektionalen Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verwendet werden soll.

7.3 Zertifikat für Streaming-Medien

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der Kommunikation zwischen den Aufzeichnungsservern und allen Clients, Servern und Integrationen verwendet werden soll, die Datenströme von den Aufzeichnungsservern abrufen.

7.4 Zertifikat für mobile Streaming-Medien

Wählen Sie das Zertifikat aus, das zum Verschlüsseln der Kommunikation zwischen dem mobilen Server und den mobilen und Web-Clients verwendet werden soll, die Datenströme vom mobilen Server abrufen.

Registrieren Sie im Abschnitt **Server Registering servers (Server registrieren)** des Server Configurator die Server, die auf dem Computer ausgeführt werden, mit dem angegebenen Management-Server.

Um die Server zu registrieren, überprüfen Sie die Adresse des Management-Servers, und wählen Sie **Registrieren** aus.

8 PowerShell-Skripts

Sie können PowerShell und das Milestone PSTools-Modul verwenden, um die laufende Wartung und die erforderlichen Konfigurationsprozesse von großen, komplexen und technisch fortschrittlichen MOBOTIX HUB VMS-Systemen zu installieren, zu integrieren, zu vereinfachen, zu überwachen und zu automatisieren.

Nichtsdestotrotz empfiehlt MOBOTIX, dass Administratoren, Installateure und Techniker wissen, wie sie die MOBOTIX HUB VMS-Umgebung ihres Kunden manuell konfigurieren können. Sie lernen mit Erfahrung, wann Sie PowerShell-Skripte anstelle von manuellen Konfigurationen verwenden sollten. PowerShell-Skripts finden Sie an den folgenden Speicherorten:

- PowerShell-Prozess/Video für [mobile Server und Lets Encrypt](#)
- [Github-Repository](#) für Milestone PSTools Informationen, Dokumentation und Skripte.

9 Manuelles Erstellen und Verteilen von Zertifikaten

9.1 Wichtig zu wissen:



Das manuelle Erstellen und Verteilen von Zertifikaten wird als sichere Methode zum Verteilen von Zertifikaten nicht empfohlen. Wenn Sie sich für die manuelle Verteilung entscheiden, sind Sie dafür verantwortlich, die privaten Zertifikate jederzeit sicher zu halten. Wenn Sie die privaten Zertifikate sicher aufbewahren, sind die Clientcomputer, die den Zertifikaten vertrauen, weniger anfällig für Angriffe.

In einigen Situationen kann Windows Update in regelmäßigen Abständen Zertifikate entfernen, die nicht von einer "vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters" stammen.

Um sicherzustellen, dass Ihre Zertifikate nicht von Windows Update entfernt werden, müssen Sie die Option Automatisches Update für Stammzertifikate deaktivieren aktivieren. Bevor Sie diese Änderung vornehmen, sollten Sie sicherstellen, dass die Änderung den Sicherheitsrichtlinien Ihres Unternehmens entspricht.

1. Aktivieren Sie dies, indem Sie den Editor für **lokale Gruppenrichtlinien** auf dem Computer öffnen (klicken Sie auf die Windows-Startleiste und geben Sie **gpedit.msc ein**).
2. Navigieren Sie **im** Windows-Editor für lokale Gruppenrichtlinien **zu Computerkonfiguration > Administrative Vorlagen > System > Internetkommunikationsverwaltung > Internetkommunikationseinstellungen**.
3. Doppelklicken Sie auf **Automatische Aktualisierung des Stammzertifikats deaktivieren**, und wählen Sie **Aktiviert** aus.
4. Klicken Sie auf **OK**.

Beachten Sie, dass diese Einstellung möglicherweise durch eine Domänenrichtlinie gesteuert wird. In diesem Fall muss sie auf dieser Ebene deaktiviert werden.

Ihr Zertifikat verbleibt jetzt auf dem Computer, obwohl es nicht von einer "vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters" stammt, da Windows Update die Windows Update-Website nicht kontaktiert, um zu überprüfen, ob Microsoft die Zertifizierungsstelle zu seiner Liste der vertrauenswürdigen Zertifizierungsstellen hinzugefügt hat.

9.2 Erstellen eines CA-Zertifikats

Führen Sie dieses Skript auf einem Computer mit eingeschränktem Zugriff, der nicht mit Ihrem MOBOTIX HUB-System verbunden ist, einmal aus, um ein CA-Zertifikat zu erstellen.



Auf dem Computer, den Sie zum Erstellen von Zertifikaten verwenden, muss Windows 10 oder Windows Server OS 2016 oder höher ausgeführt werden.



Beachten Sie, dass beim Erstellen von Zertifikaten auf diese Weise die Zertifikate mit dem Computer verknüpft sind, auf dem sie installiert sind. Wenn sich der Computernamen ändert, kann der virtuelle Computer erst gestartet werden, wenn die Zertifikate erneut erstellt und auf dem Computer neu

Mit diesem Skript werden zwei Zertifikate erstellt:

- Ein privates Zertifikat: Nach dem Ausführen des Skripts ist nur im Speicher für persönliche Zertifikate für den aktuellen Benutzer vorhanden . Es wird empfohlen, eine Sicherung zu erstellen, die auf einem Medium (USB) an einem sicheren Ort aufbewahrt wird, und vorzugsweise zwei Sicherungen, die an physisch unterschiedlichen Orten aufbewahrt werden. Mit Ausnahme der Sicherungen sollte dieses Zertifikat niemals den Computer verlassen, auf dem Sie das Zertifikat erstellt haben
 - Ein öffentliches Zertifikat, das als vertrauenswürdigen Zertifikat auf allen Clientcomputern importiert werden soll
1. In Anhang A am Ende dieses Handbuchs finden Sie ein Skript zum Erstellen des Zertifizierungsstellenzertifikats. Kopieren Sie den Inhalt.
 2. Öffnen Sie Editor, und fügen Sie den Inhalt ein.

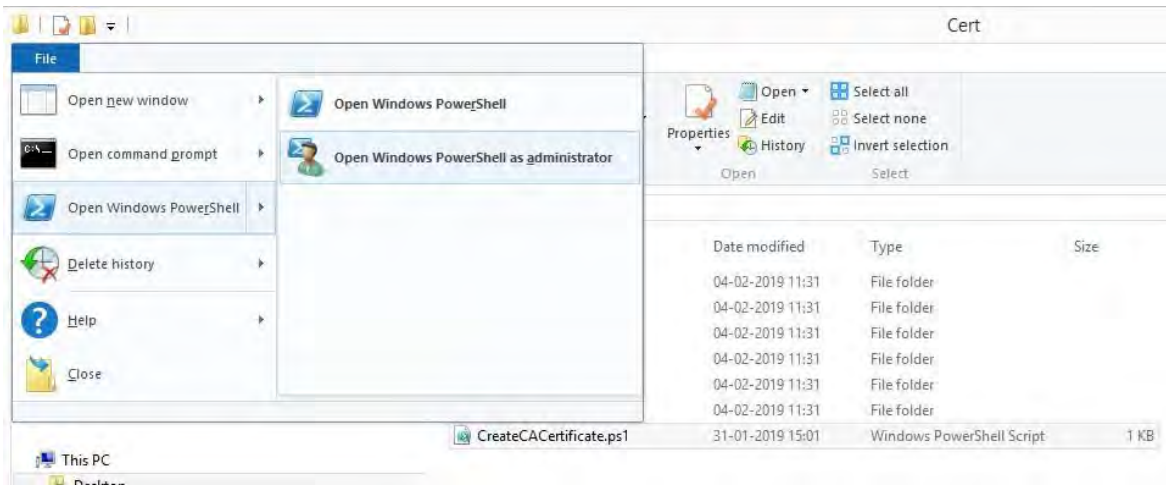


Es ist sehr wichtig, dass die Linien an den gleichen Stellen wie in Anhang A unterbrochen werden. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen , den Inhalt erneut kopieren und in Notepad

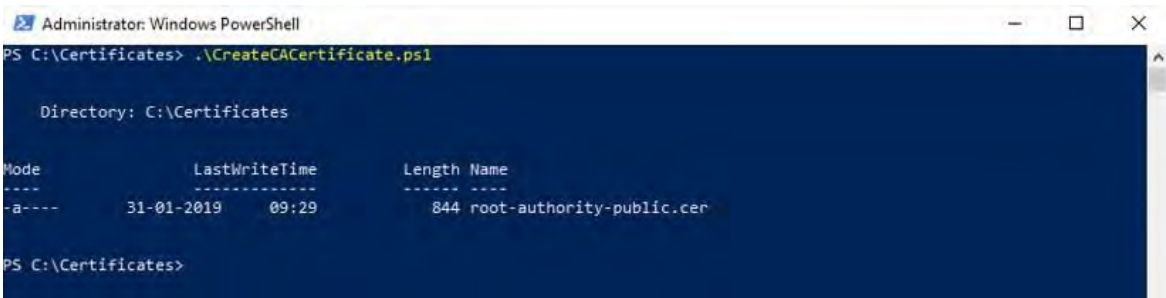
```
File Edit Format View Help
# Run this script once, to create a certificate that can sign multiple recording server certificates
# Private certificate for signing other certificates (in certificate store)
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS Certificate Authority' -KeyUsageProperty All -
-KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS CA Certificate'
# Thumbprint of private certificate used for signing other certificates
Set-Content -Path "$PSScriptRoot\ca_thumbprint.txt" -Value $ca_certificate.Thumbprint
# Public CA certificate to trust (Third-Party Root Certification Authorities)
Export-Certificate -Cert "Cert:\CurrentUser\My\${$ca_certificate.Thumbprint}" -FilePath "$PSScriptRoot\root-authority-public.cer"
```

3. Klicken Sie im Editor auf **Datei -> Speichern unter**, nennen Sie die Datei **CreateCACertificate.ps1**, und speichern Sie sie lokal wie folgt:
C:\Certificates\CreateCACertificate.ps1.
4. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die **Datei CreateCACertificate.ps1** aus.


- 5. Wählen Sie im **Menü Datei** die Option **Windows PowerShell öffnen** und dann **Windows PowerShell als Administrator öffnen** aus.



- 6. Geben Sie in PowerShell an der Eingabeaufforderung **.\CreateCACertificate.ps1** ein, und drücken Sie die **EINGABETASTE**.



- 7. Vergewissern Sie sich, dass die **root-authority-public.cer** Datei in dem Ordner angezeigt wird, in dem Sie das Skript ausgeführt haben.

 Auf Ihrem Computer ist es möglicherweise erforderlich, dass Sie die PowerShell-Ausführungsrichtlinie ändern. Wenn ja, geben Sie **Set-ExecutionPolicy RemoteSigned** ein. Drücken Sie die **Eingabetaste** und wählen Sie **A**.

10 Installieren von Zertifikaten auf den Clients

Nachdem Sie das Zertifikat der Zertifizierungsstelle erstellt haben, vertrauen Sie dem Zertifikat der öffentlichen Zertifizierungsstelle, indem Sie es auf allen Computern installieren, die als Clients für den Dienst fungieren, wie in den Beschreibungen unter Einführung in Zertifikate auf Seite 5 beschrieben.

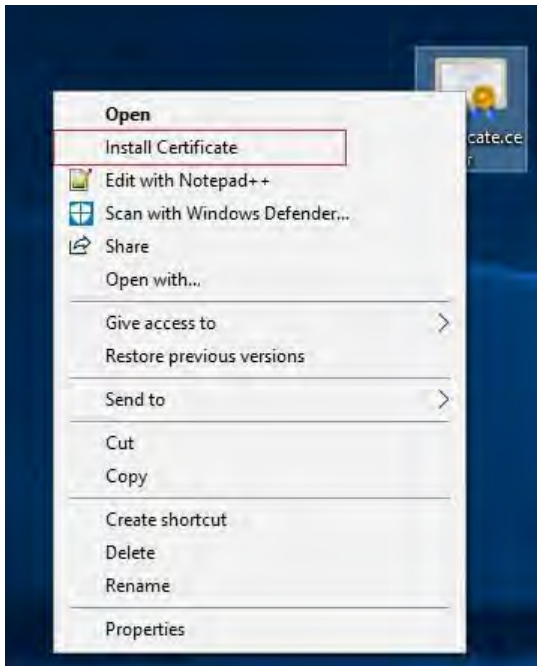


Siehe [Importieren von Client-Zertifikaten auf Seite 129](#) für ein alternatives Verfahren zur manuellen Installieren von Zertifikaten auf Clients.

8. Kopieren Sie die Datei `root-authority-public.cer` Datei von dem Computer aus, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben (`C:\Zertifikate\root-authority-public.cer`) auf den Computer, auf dem der MOBOTIX HUB-Client installiert ist.



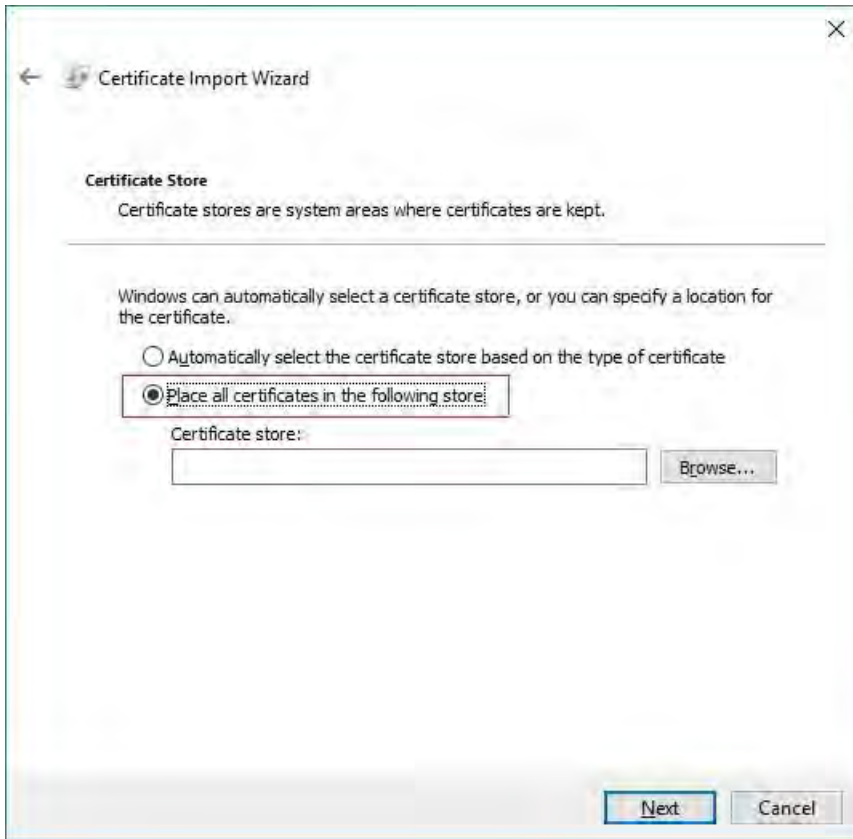
Informationen darüber, welche Client- und Serverdienste und Integrationen Fordern Sie das Zertifikat an, siehe [Einführung in die Zertifikate auf Seite 5](#).



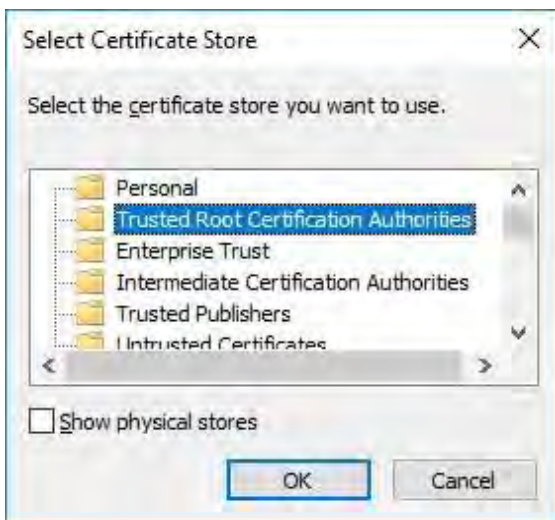
9. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Zertifikat installieren** aus.




10. Wählen Sie im **Zertifikatimport-Assistenten** aus, ob das Zertifikat im Speicher des lokalen Computers installiert werden soll, und klicken Sie auf **Weiter**.
11. Wählen Sie diese Option aus, um den Speicher, in dem das Zertifikat installiert werden soll, manuell zu suchen.

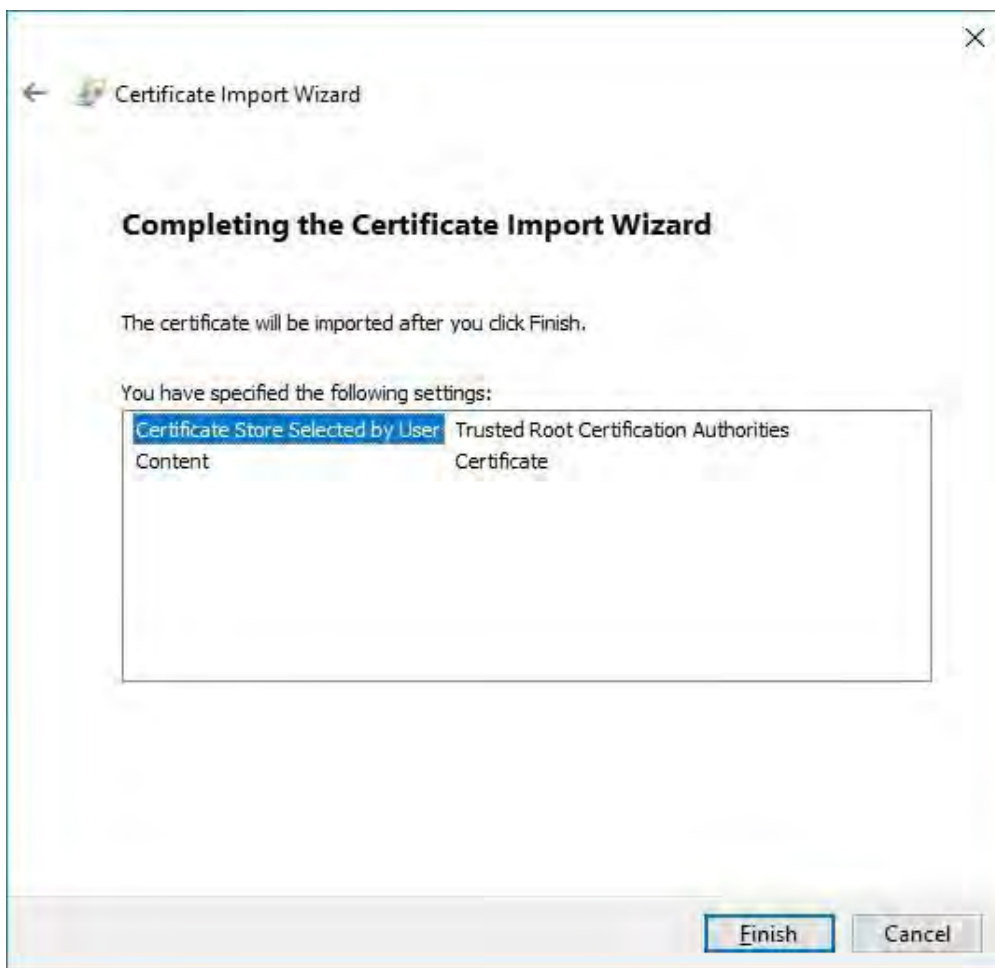


12. Klicken Sie auf Durchsuchen, wählen Sie Vertrauenswürdige Stammzertifizierungsstellen aus, und klicken Sie auf OK. Klicken Sie dann auf Weiter.



13. Klicken Sie im Dialogfeld Abschließen des Zertifikatimport-Assistenten auf Fertig stellen.

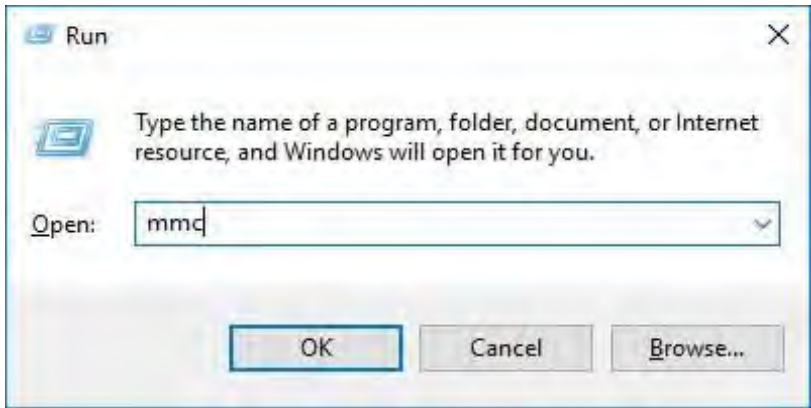
 Wenn Sie eine Sicherheitswarnung erhalten, dass Sie ein Stammzertifikat installieren möchten, klicken Sie auf **Ja**, um fortzufahren.



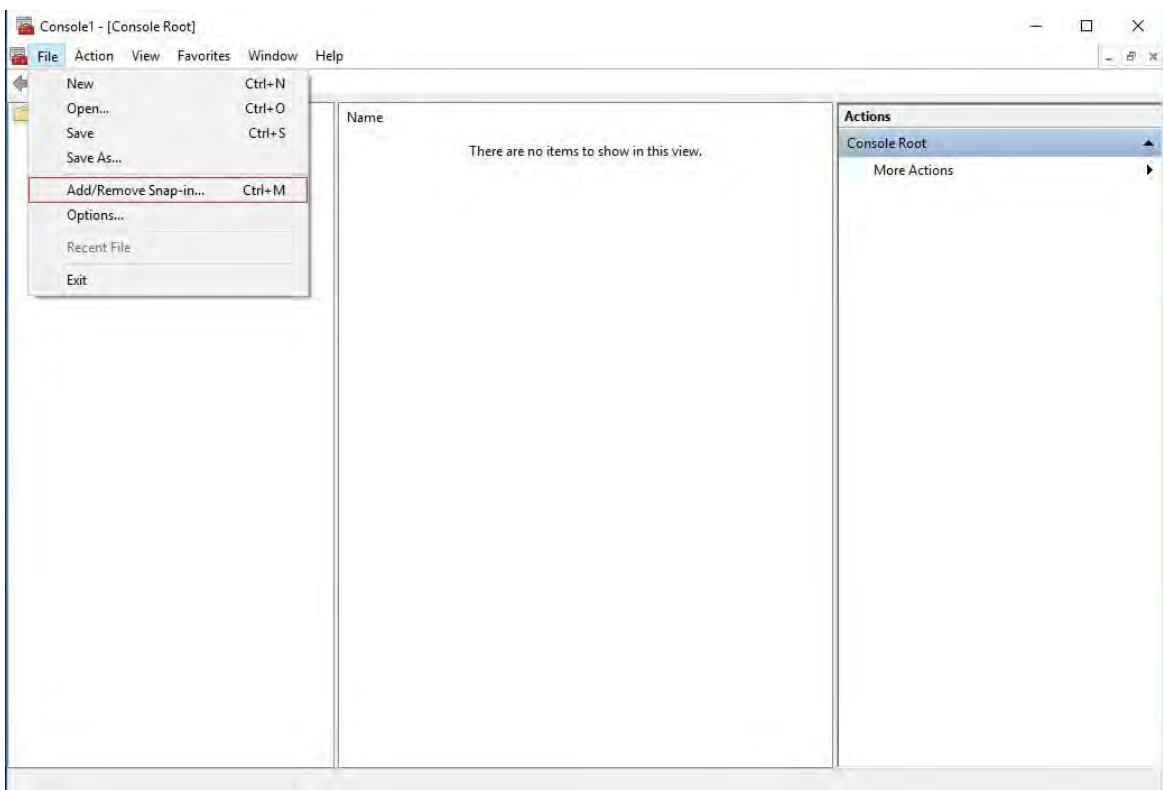
14. Sie erhalten einen Bestätigungsdialog über den erfolgreichen Import.



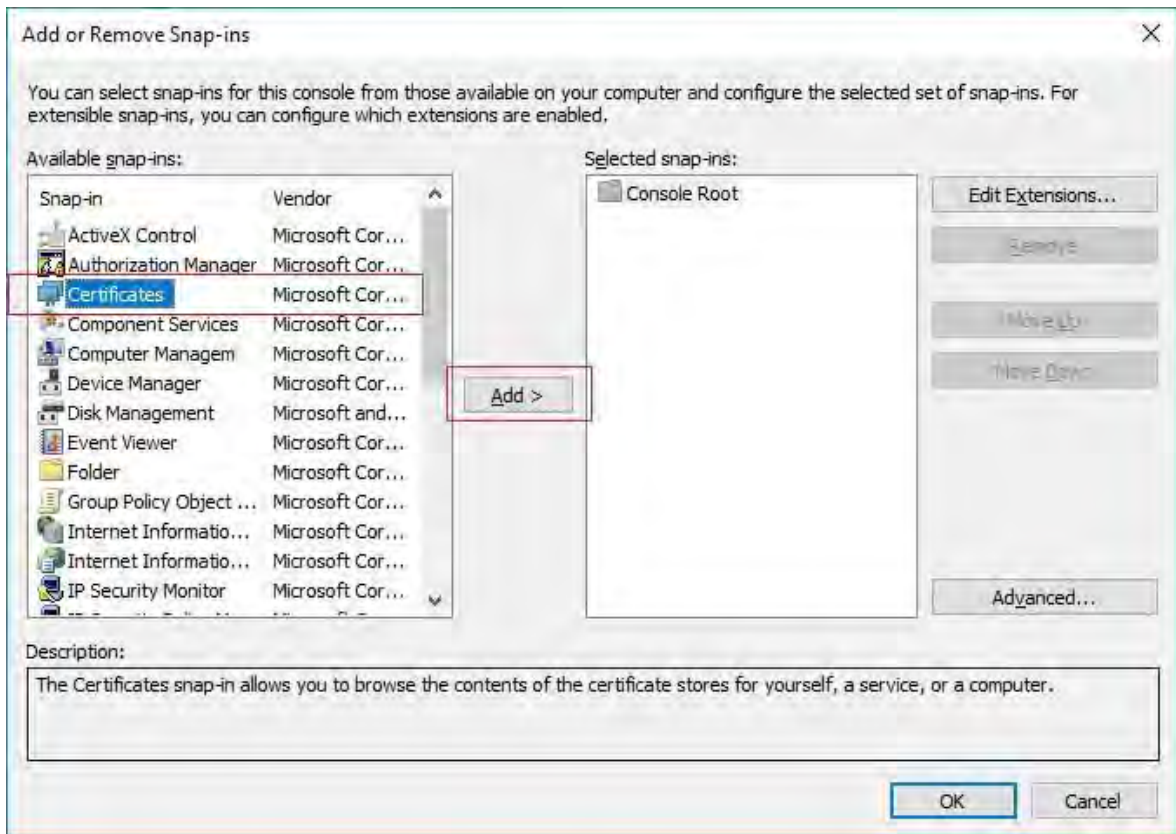
15. Um zu überprüfen, ob das Zertifikat importiert wurde, starten Sie die Microsoft Management Console.



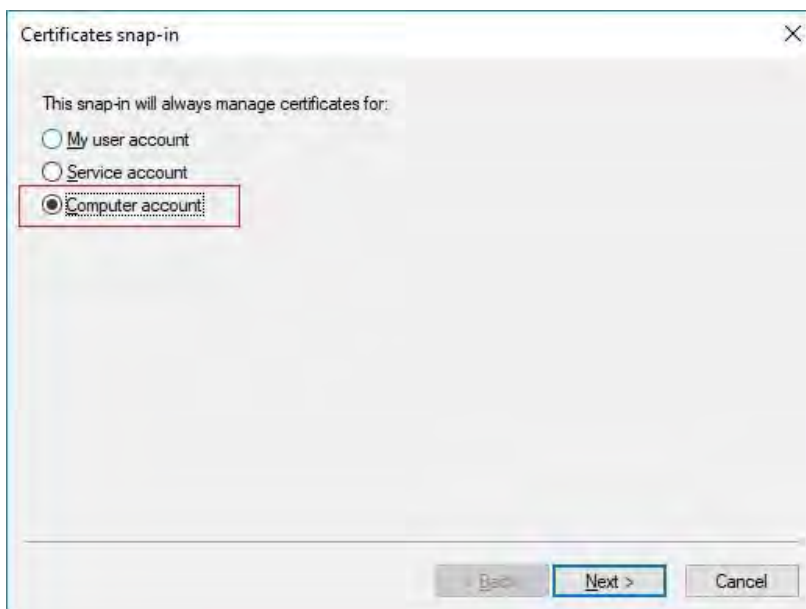
16. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In hinzufügen/entfernen...**



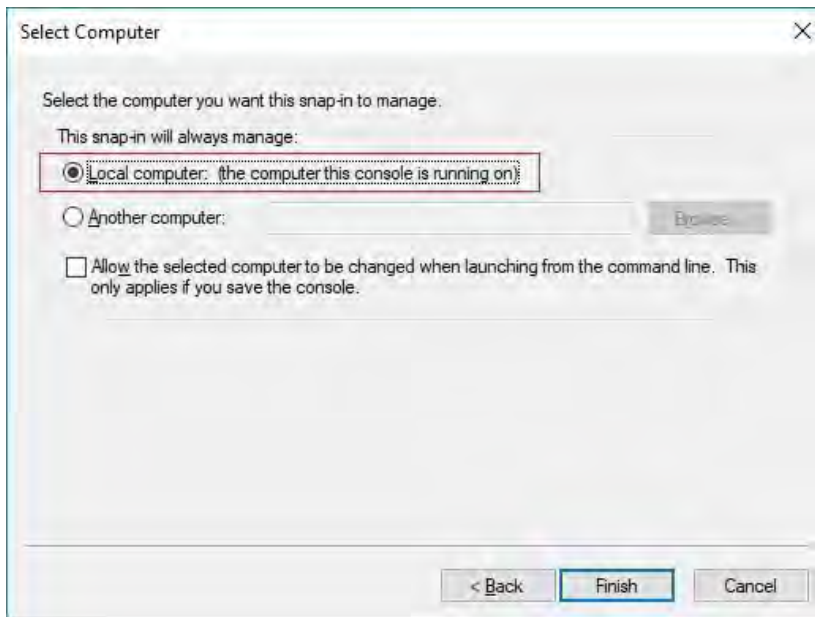
17. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf **Hinzufügen**.



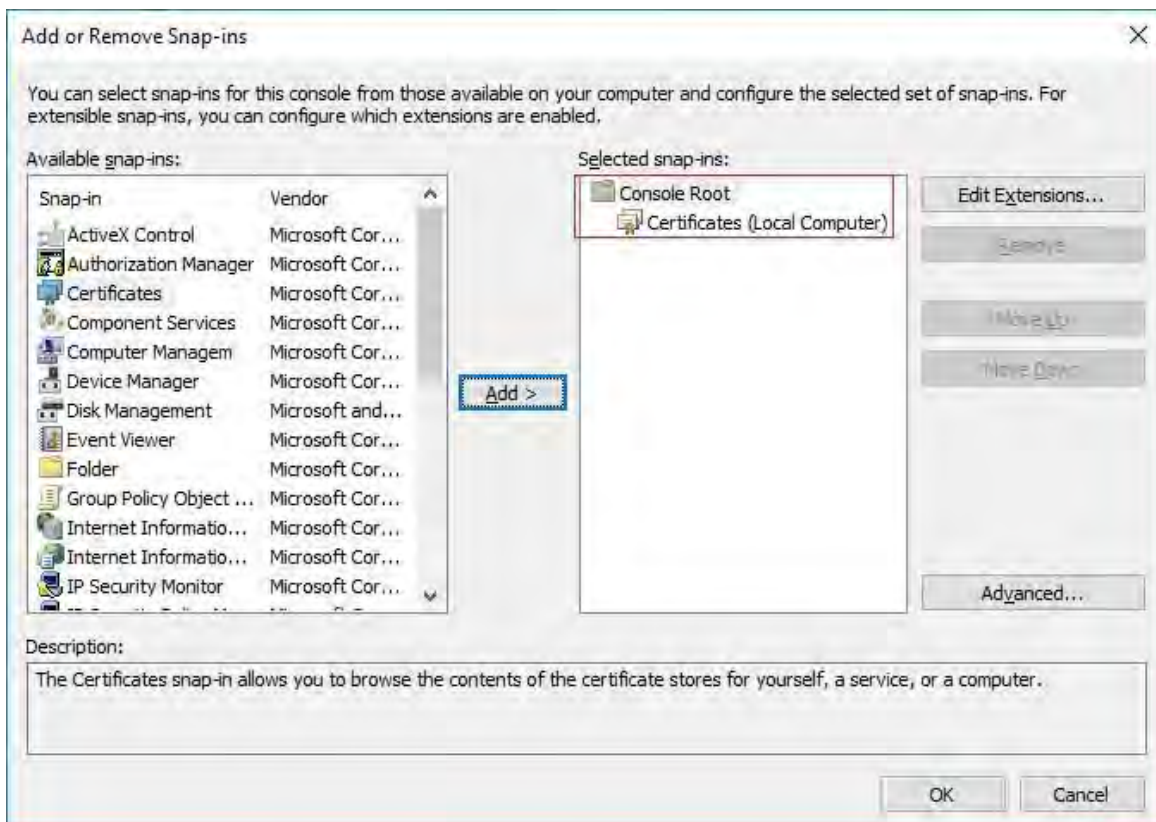
18. Wählen Sie aus, dass das Snap-In Zertifikate für das **Computerkonto verwalten muss**.



19. Wählen Sie **Lokaler Computer** als den Computer aus, den das Snap-In verwalten soll, und klicken Sie auf **Fertig stellen**.

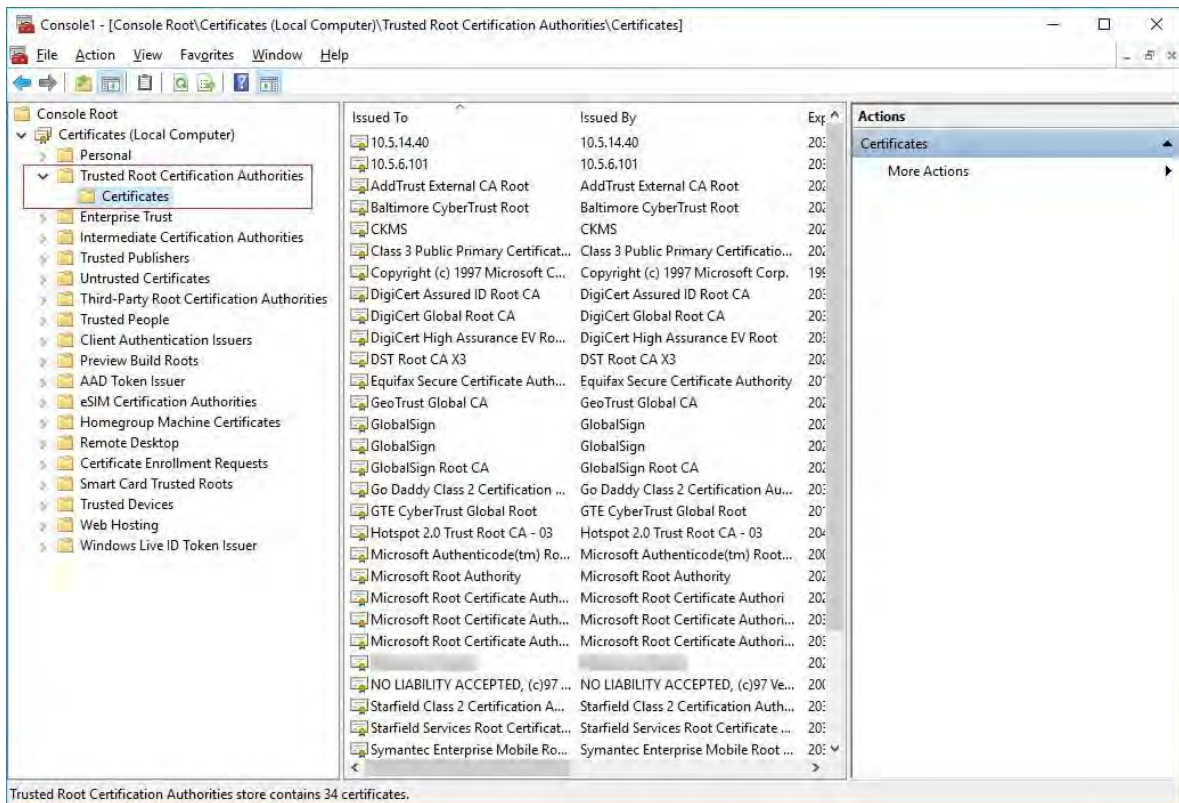


20. Klicken Sie auf **OK**, nachdem das Snap-In hinzugefügt wurde.



21. Stellen Sie sicher, dass das Zertifikat in der mittleren Ansicht der **vertrauenswürdigen Stammzertifizierungsstellen** aufgeführt ist.

Teilbaum.



22. Wiederholen Sie die Schritte auf dem nächsten Computer, der als Client für den Dienst ausgeführt wird, für den die Verschlüsselung aktiviert ist, bis Sie das Zertifikat auf allen relevanten Computern installiert haben.

11 SSL-Zertifikat erstellen

Nachdem Sie das Zertifizierungsstellenzertifikat auf allen Clients installiert haben, können Sie Zertifikate erstellen, die auf allen Computern installiert werden, auf denen Server ausgeführt werden (Aufzeichnungsserver, Verwaltungsserver, mobile Server oder Failoverserver).



Auf dem Computer, den Sie zum Erstellen von Zertifikaten verwenden, muss Windows 10 oder Windows Server 2016 oder höher ausgeführt werden.

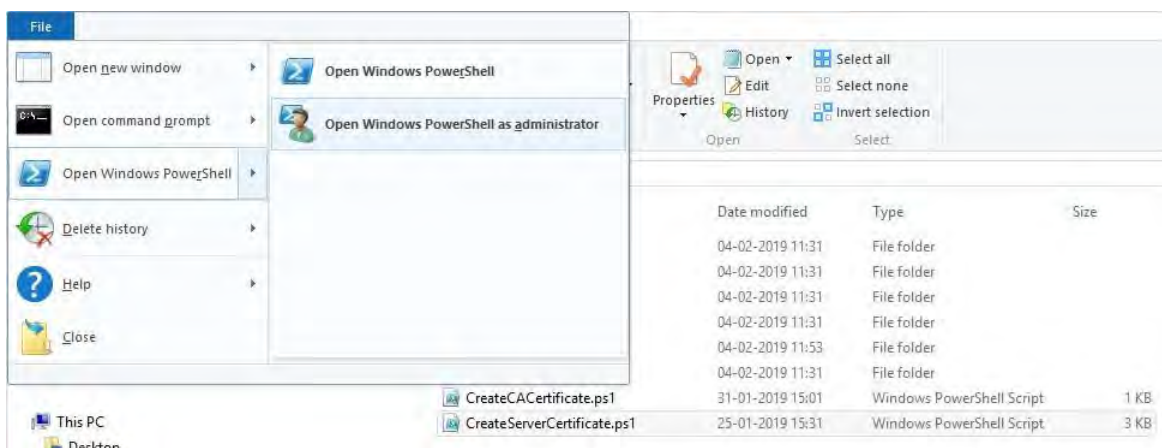
Führen Sie auf dem Computer, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben, in dem Ordner, in dem Sie das Zertifizierungsstellenzertifikat abgelegt haben, das **Serverzertifikatskript** aus, um SSL-Zertifikate für alle Server zu erstellen. In Anhang B am Ende dieses Handbuchs finden Sie ein Skript zum Erstellen von Serverzertifikaten.

1. Öffnen Sie Editor, und fügen Sie den Inhalt ein.



Es ist sehr wichtig, dass die Linien an den gleichen Stellen wie in Anhang B unterbrochen werden. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen, den Inhalt erneut kopieren und in Notepad

2. Klicken Sie im Editor auf **Datei -> Speichern unter**, nennen Sie die Datei **CreateServerCertificate.ps1**, und speichern Sie sie lokal im selben Ordner wie das Zertifizierungsstellenzertifikat, wie folgt:
C:\Certificates\CreateServerCertificate.ps1.
3. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die **Datei CreateServerCertificate.ps1** aus.
4. Wählen Sie im Menü Datei die Option Windows PowerShell öffnen und dann Windows PowerShell als Administrator öffnen aus.



5. Geben Sie in PowerShell an der Eingabeaufforderung **.\CreateServerCertificate.ps1 ein**, und drücken Sie die **INGABETASTE**.

6. Geben Sie den DNS-Namen für den Server ein. Wenn der Server mehrere Namen hat, z.B. für den internen und externen Gebrauch, fügen Sie diese hier durch ein Leerzeichen getrennt hinzu. Drücken Sie **die** Eingabetaste.



Um den DNS-Namen zu finden, öffnen Sie den Datei-Explorer auf dem Computer, auf dem der Aufzeichnungsserver-Dienst ausgeführt wird. Klicken Sie mit der rechten Maustaste auf **Dieser PC**, und wählen Sie **Eigenschaften aus**. Verwenden Sie den

```
Administrator: Windows PowerShell
PS C:\Certificates> .\CreateServerCertificate.ps1
DNS names for server SSL certificate (delimited by space - 1st entry is also subject of certificate):
```

7. Geben Sie die IP-Adresse des Servers ein. Wenn der Server mehrere IP-Adressen hat, zum Beispiel für den internen und externen Gebrauch, fügen Sie diese hier durch ein Leerzeichen getrennt hinzu. Drücken Sie **die** Eingabetaste.



Um die IP-Adresse zu finden, können Sie die Eingabeaufforderung auf dem Computer öffnen, auf dem der Aufzeichnungsserverdienst ausgeführt wird. Geben Sie **ipconfig /all ein**. Wenn Sie das MOBOTIX HUB-System installiert haben, können Sie den Management Client öffnen, zum Server navigieren und die IP-Adresse auf der

8. Geben Sie ein Kennwort für das Zertifikat an, und drücken Sie **die Eingabetaste**, um die Erstellung abzuschließen.



Sie verwenden dieses Kennwort, wenn Sie das Zertifikat auf den Server importieren.

Die Datei Subjectname.pfx wird in dem Ordner angezeigt, in dem Sie das Skript ausgeführt haben.

9. Führen Sie das Skript aus, bis Sie über Zertifikate für alle Server verfügen.

12 SSL-Zertifikat importieren

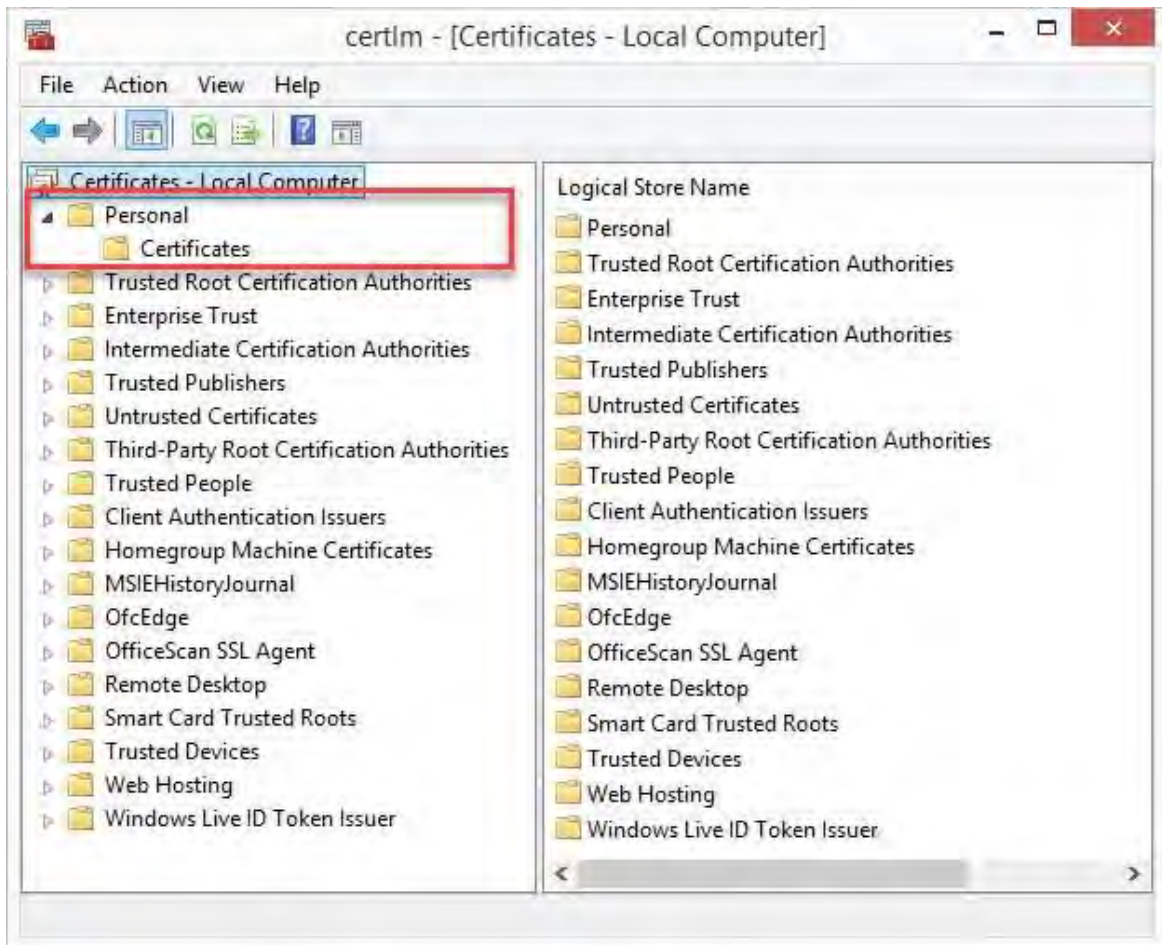
Nachdem Sie die SSL-Zertifikate erstellt haben, installieren Sie sie auf den Computern, auf denen der Serverdienst



Denken Sie daran, dass jedes Zertifikat auf einem bestimmten Server erstellt wird.

ausgeführt wird.

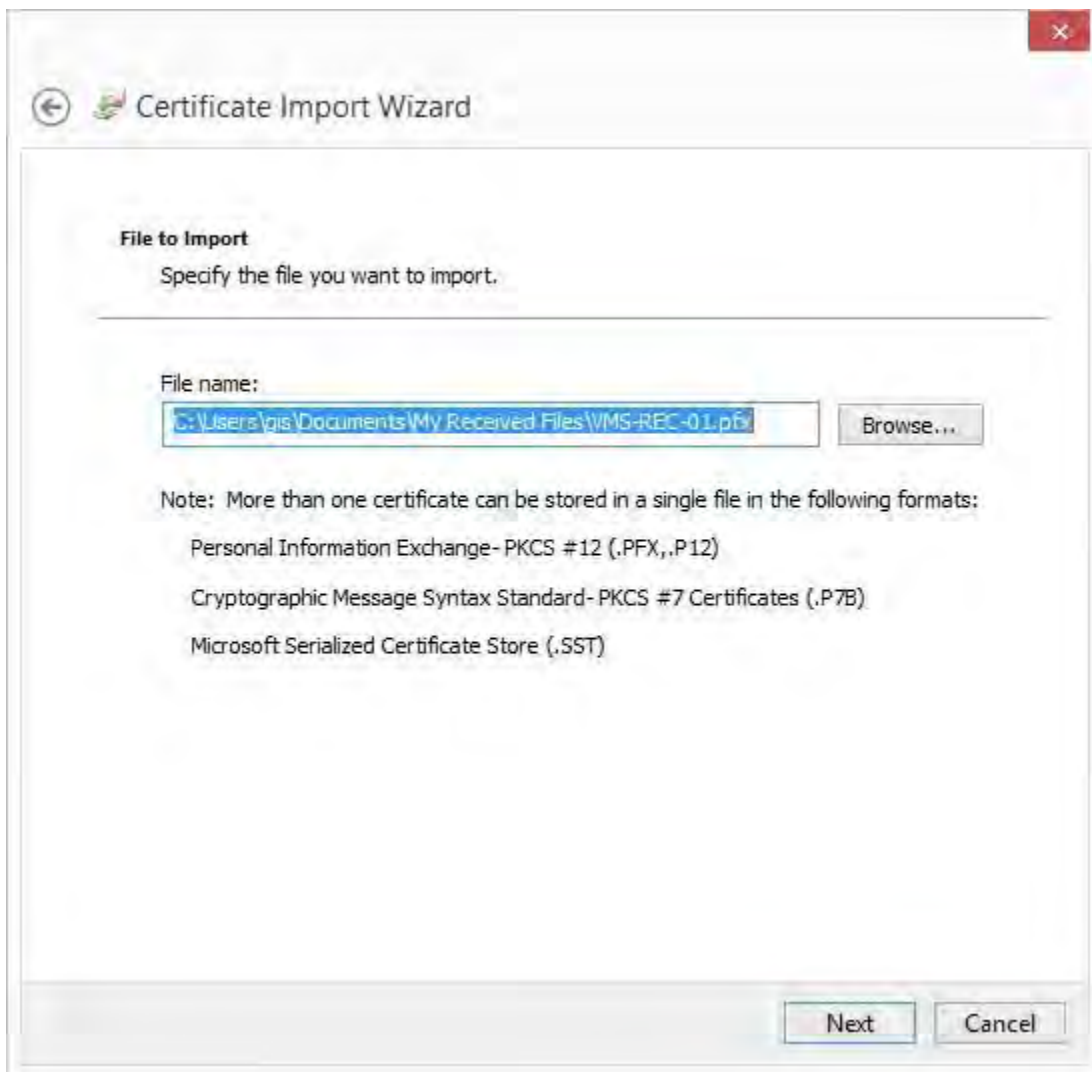
10. Kopieren Sie die entsprechende Datei "Subjectname.pfx" von dem Computer, auf dem Sie das Zertifikat erstellt haben, auf den entsprechenden Serverdienstcomputer.
11. Starten Sie auf dem Serverdienstcomputer **Computerzertifikate verwalten**.
12. Klicken Sie auf **Persönlich**, klicken Sie mit der rechten Maustaste auf **Zertifikate** und wählen Sie **Alle Aufgaben > Importieren**.



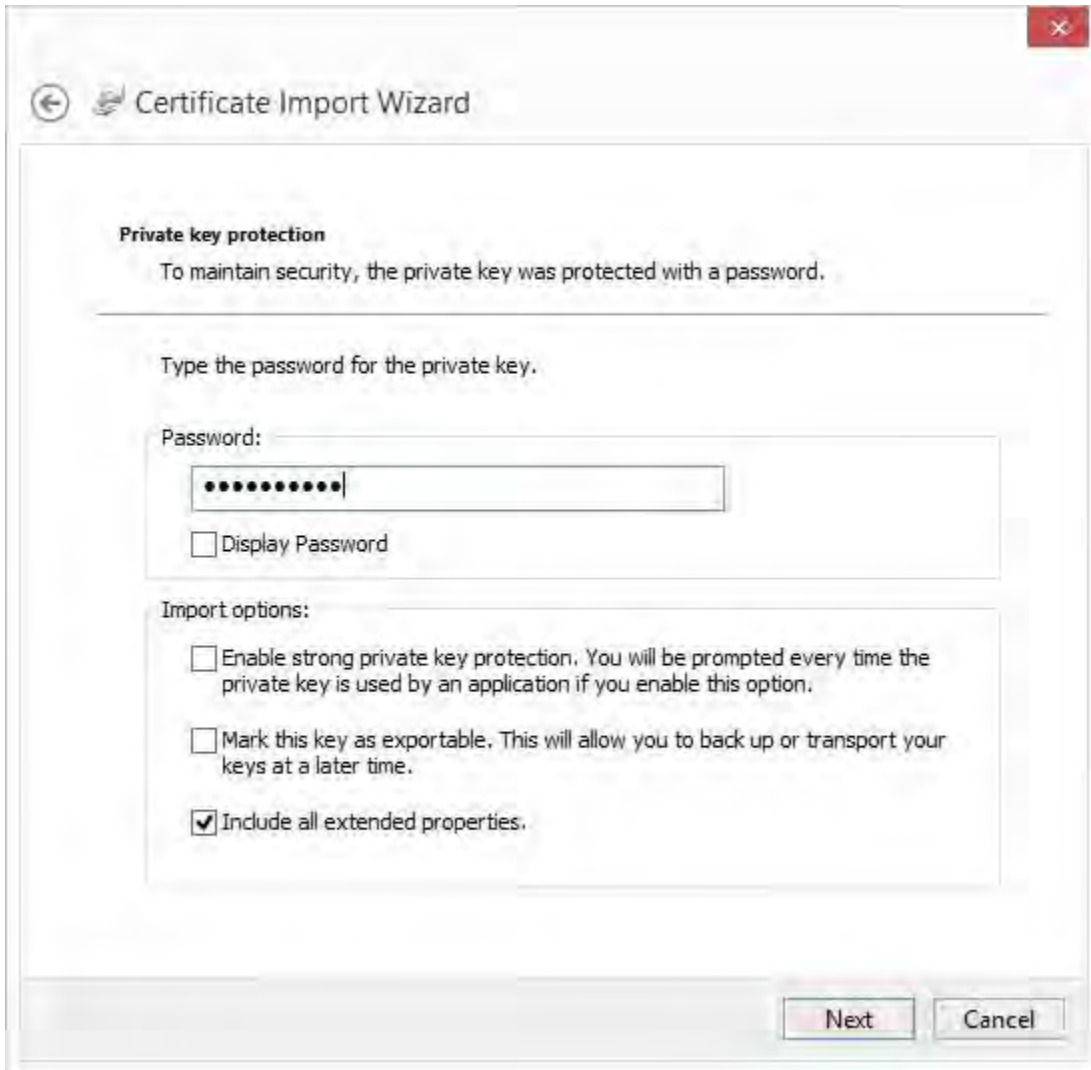
13. Wählen Sie diese Option aus, um das Zertifikat in den Speicher des **lokalen Computers zu importieren**, und klicken Sie auf **Weiter**.



14. Navigieren Sie zur Zertifikatsdatei, und klicken Sie auf **Weiter**.



15. Geben Sie das Kennwort für den privaten Schlüssel ein, das Sie beim Erstellen des Serverzertifikats angegeben haben, und klicken Sie dann auf **Weiter**.



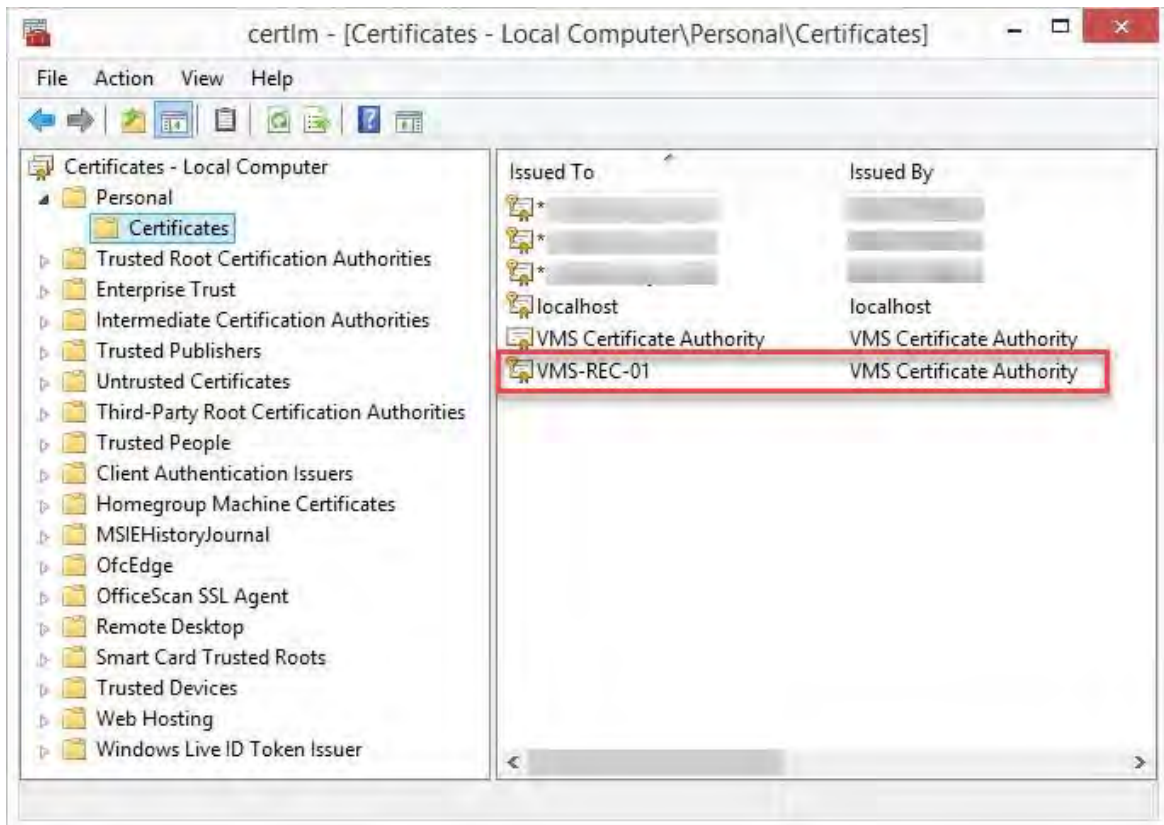
16. Legen Sie die Datei im **Zertifikatsspeicher: Persönlich** ab, und klicken Sie dann auf **Weiter**.



17. Überprüfen Sie die Informationen und klicken Sie auf **Fertig stellen** , um das Zertifikat zu importieren.

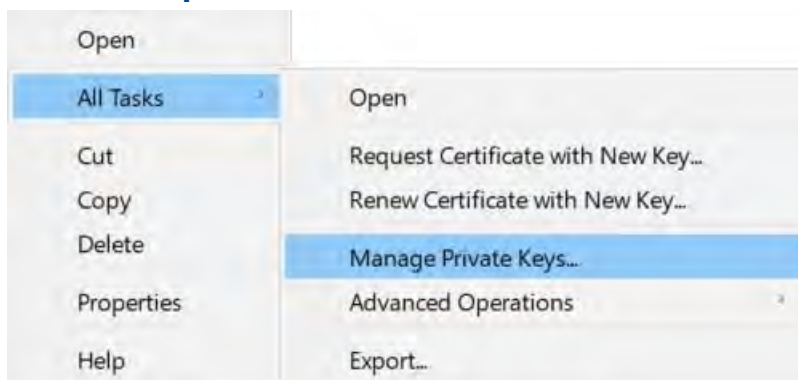


Das importierte Zertifikat wird in der Liste angezeigt.

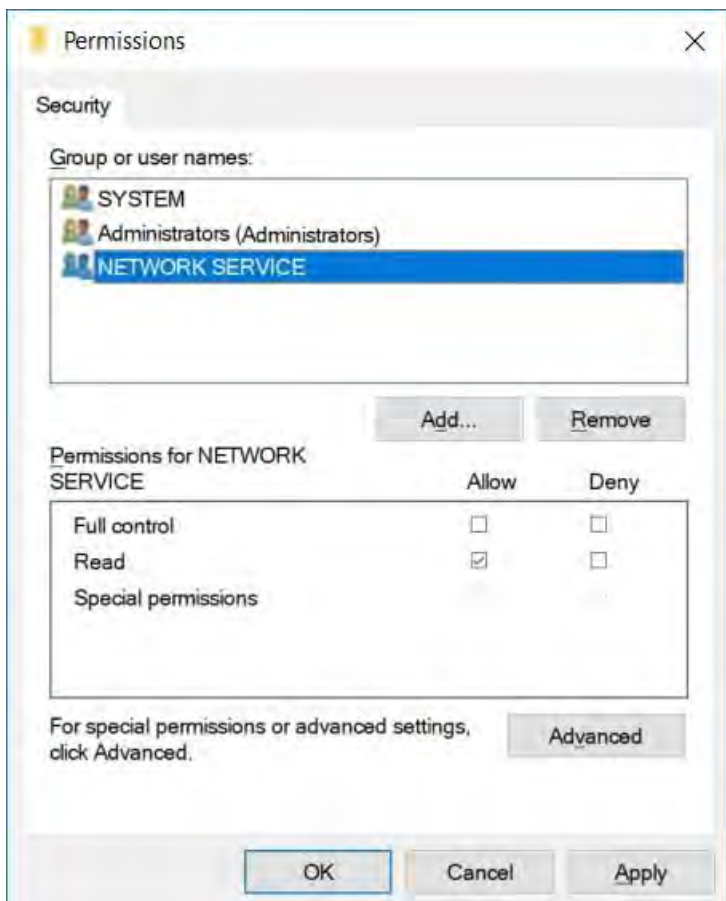


18. Um einem Dienst die Verwendung des privaten Schlüssels des Zertifikats zu gestatten, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **Alle Aufgaben** >

12.1 Verwalten Sie private Schlüssel.



1. Fügen Sie Leseberechtigungen für den Benutzer hinzu, der die MOBOTIX HUB-VMS-Dienste ausführt, die das Serverzertifikat verwenden müssen .



2. Fahren Sie mit dem nächsten Computer fort, bis Sie alle Serverzertifikate installiert haben.

13 Erstellen eines SSL-Zertifikats für den Failover-Management-Server

MOBOTIX HUB Management Server Failover wird auf zwei Computern konfiguriert. Um sicherzustellen, dass die Clients dem ausgeführten Verwaltungsserver vertrauen, installieren Sie das SSL-Zertifikat auf dem primären und dem sekundären Computer.

Um das SSL-Zertifikat für den Failovercluster zu erstellen und zu installieren, müssen Sie zuerst das Zertifizierungsstellenzertifikat installieren.

Führen Sie auf dem Computer, auf dem Sie das Zertifizierungsstellenzertifikat erstellt haben, in dem Ordner, in dem Sie das Zertifizierungsstellenzertifikat abgelegt haben, das **Skript für das Failoververwaltungsserverzertifikat** aus, um ein SSL-Zertifikat für den primären und den sekundären Computer zu erstellen.



Auf dem Computer, den Sie zum Erstellen von Zertifikaten verwenden, muss Windows 10 oder Windows Server 2016 oder höher ausgeführt werden.

3. Kopieren Sie in Anhang C dieses Handbuchs das Skript zum Erstellen von Zertifikaten für den Failover-Verwaltungsserver.
4. Öffnen Sie Editor, und fügen Sie das Skript ein.

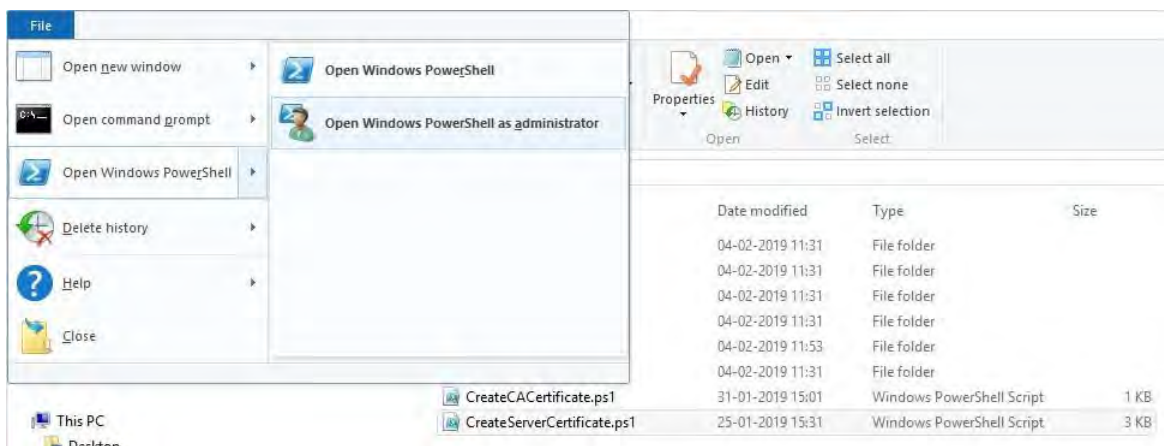


Es ist sehr wichtig, dass die Linien an den gleichen Stellen brechen, wie im Anhang gezeigt C. Sie können die Zeilenumbrüche in Notepad hinzufügen oder alternativ diese PDF-Datei mit Google Chrome erneut öffnen, den Inhalt erneut kopieren und in Notepad

5. Wählen Sie im Editor Datei -> Speichern unter aus, nennen Sie die Datei CreateFailoverCertificate.ps1, und speichern Sie sie lokal im selben Ordner wie das Zertifizierungsstellenzertifikat:

Beispiel: C:\Certificates\CreateFailoverCertificate.ps1.

6. Wechseln Sie im Datei-Explorer zu C:\Zertifikate, und wählen Sie die Datei CreateFailoverCertificate.ps1 aus.
7. Wählen Sie im Menü Datei die Option Windows PowerShell öffnen und dann Windows PowerShell als Administrator öffnen aus.



8. Geben Sie in PowerShell **an der Eingabeaufforderung .\CreateFailoverCertificate.ps1** ein, und drücken Sie **die EINGABETASTE**.

9. Geben Sie die FQDNs und die Hostnamen für den primären und den sekundären Computer an, getrennt durch ein Komma.
Beispiel: pc1host,pc1host.domain,pc2host,pc2host.domain.
10. Drücken Sie **die** Eingabetaste.
11. Geben Sie die virtuelle IP-Adresse des Failoverclusters an. Drücken Sie **die** Eingabetaste.
12. Geben Sie ein Kennwort für das Zertifikat an, und drücken Sie **die Eingabetaste** , um die Erstellung abzuschließen.



Sie verwenden dieses Kennwort, wenn Sie das Zertifikat auf den Server importieren.

Die Datei [virtualIP].pfx wird in dem Ordner angezeigt, in dem Sie das Skript ausgeführt haben. Importieren Sie das Zertifikat auf die gleiche Weise, wie Sie ein SSL-Zertifikat importieren würden, siehe [Importieren eines SSL-Zertifikats auf Seite 29](#). Importieren Sie das Zertifikat auf dem primären und dem sekundären Computer.

14 Installieren von Zertifikaten für die Kommunikation mit dem Mobile Server

Um ein HTTPS-Protokoll zum Herstellen einer sicheren Verbindung zwischen dem mobilen Server und Clients und Diensten zu verwenden, müssen Sie ein gültiges Zertifikat auf dem Server anwenden. Das Zertifikat bestätigt, dass der Zertifikatsinhaber berechtigt ist, sichere Verbindungen herzustellen.

In MOBOTIX HUB-VMS wird die Verschlüsselung pro Mobile Server aktiviert oder deaktiviert. Sie aktivieren oder deaktivieren die Verschlüsselung entweder während der Installation des Produkts MOBOTIX HUB VMS oder mithilfe des Server-Konfigurators. Wenn Sie die Verschlüsselung auf einem Mobile Server aktivieren, verwenden Sie eine verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen, die



Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

Datenströme abrufen.



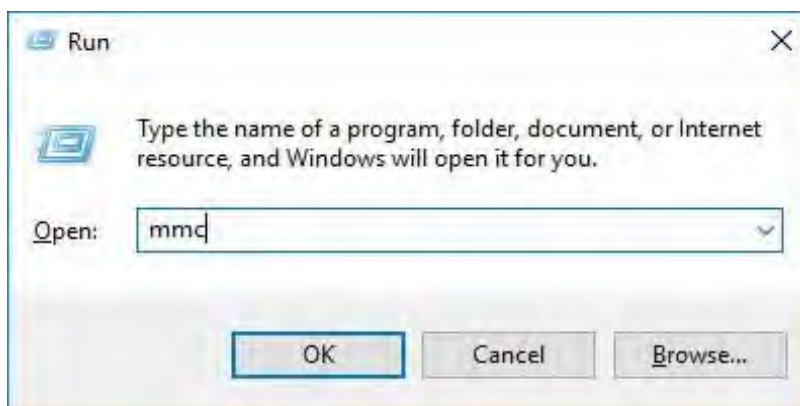
Zertifikate, die von einer Zertifizierungsstelle (CA) ausgestellt wurden, verfügen über eine Kette von Zertifikaten, und im Stammverzeichnis dieser Kette befindet sich das Stammzertifikat der Zertifizierungsstelle. Wenn ein Gerät oder Browser dieses Zertifikat sieht, vergleicht es sein Stammzertifikat mit den auf dem Betriebssystem (Android, iOS, Windows usw.) vorinstallierten Zertifikaten. Wenn das Stammzertifikat in der Liste der vorinstallierten Zertifikate aufgeführt ist, stellt das Betriebssystem dem Benutzer sicher, dass

14.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

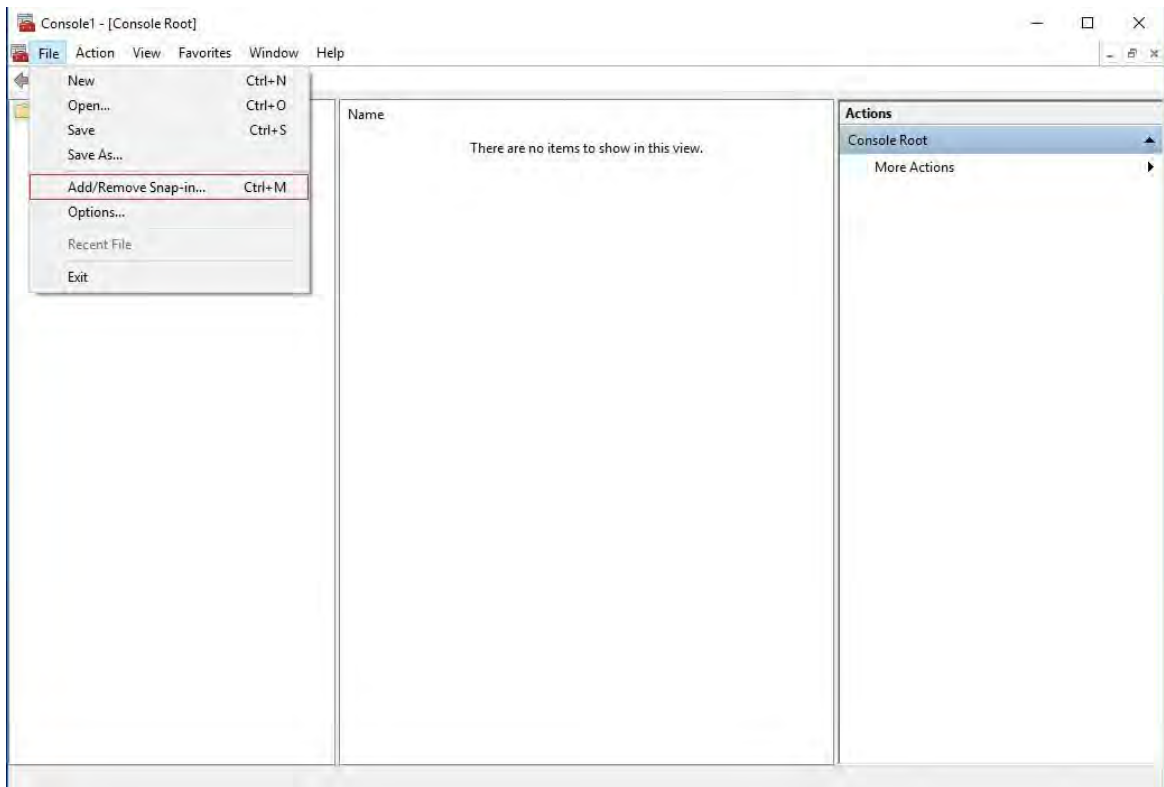
Fügen Sie das Zertifizierungsstellenzertifikat zum Mobile Server hinzu, indem Sie wie folgt vorgehen: Öffnen Sie auf dem Computer, auf dem der Mobile Server gehostet wird, die Microsoft Management Console.



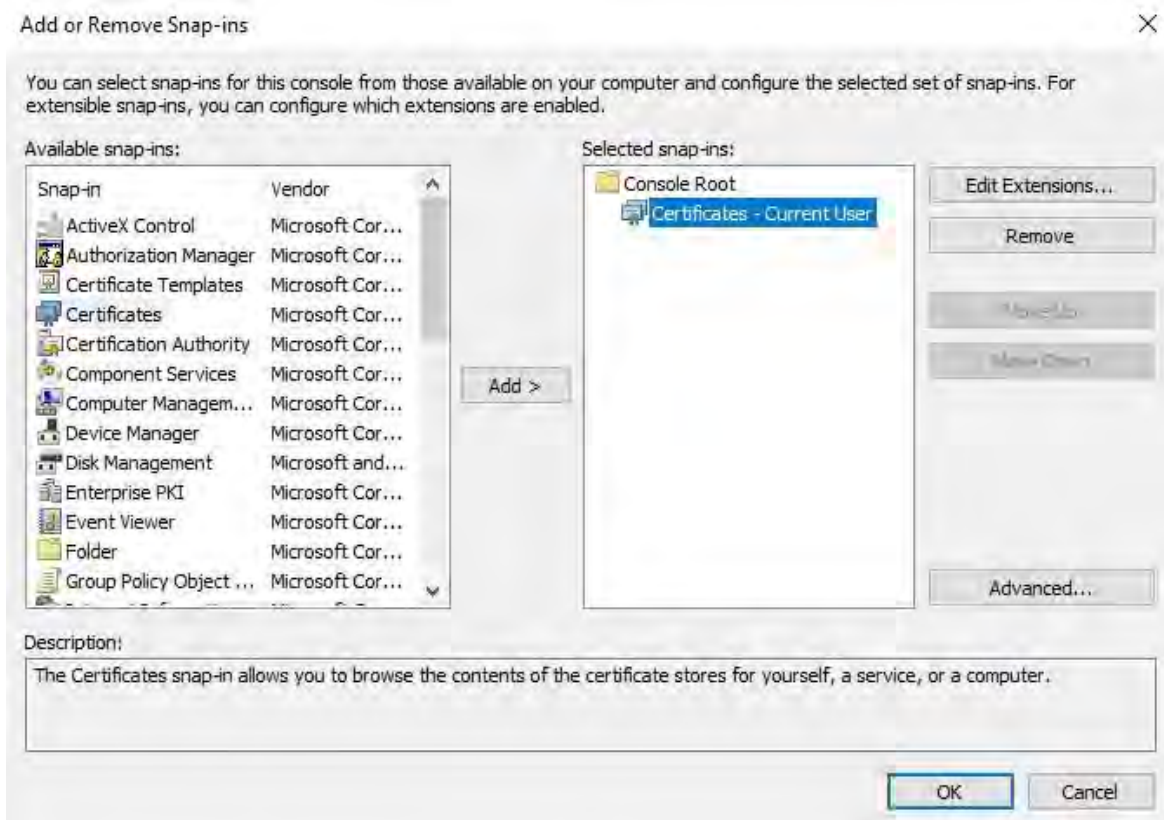
Bestimmte Parameter hängen von der Zertifizierungsstelle ab. Lesen Sie die Dokumentation Ihrer Zertifizierungsstelle, bevor Sie fortfahren.



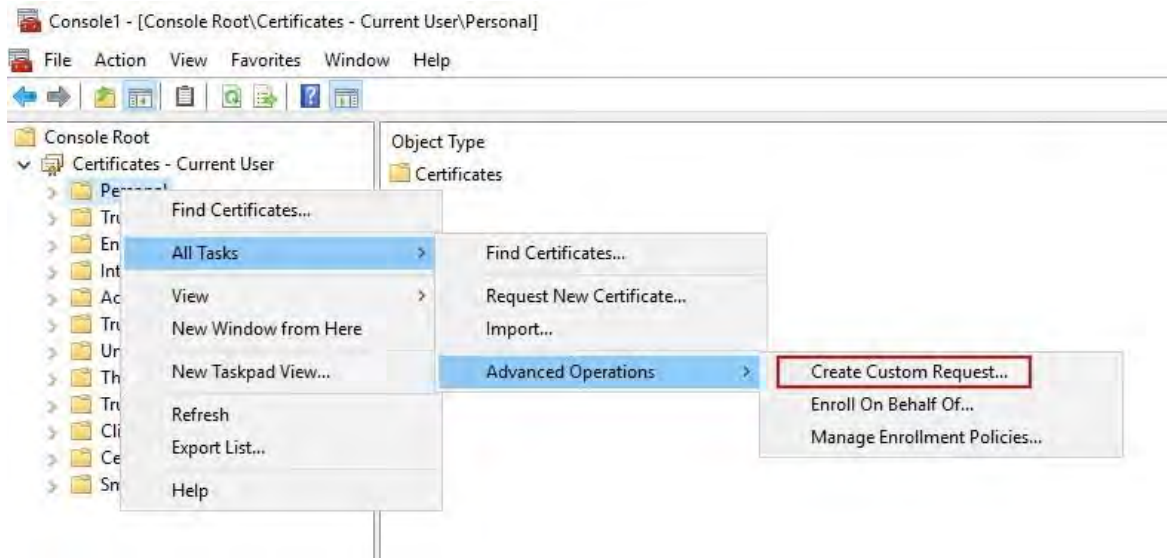
1. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In hinzufügen/entfernen....**



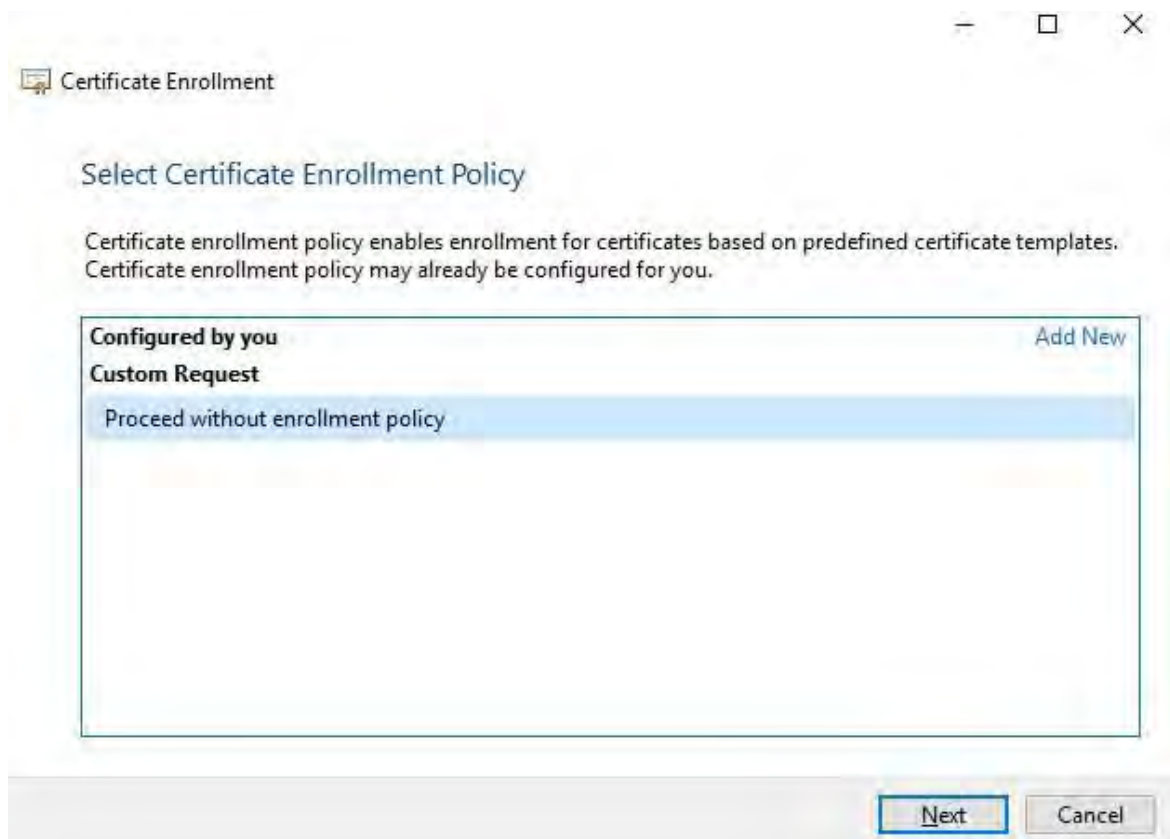
2. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf Hinzufügen.
3. Klicken Sie auf OK.



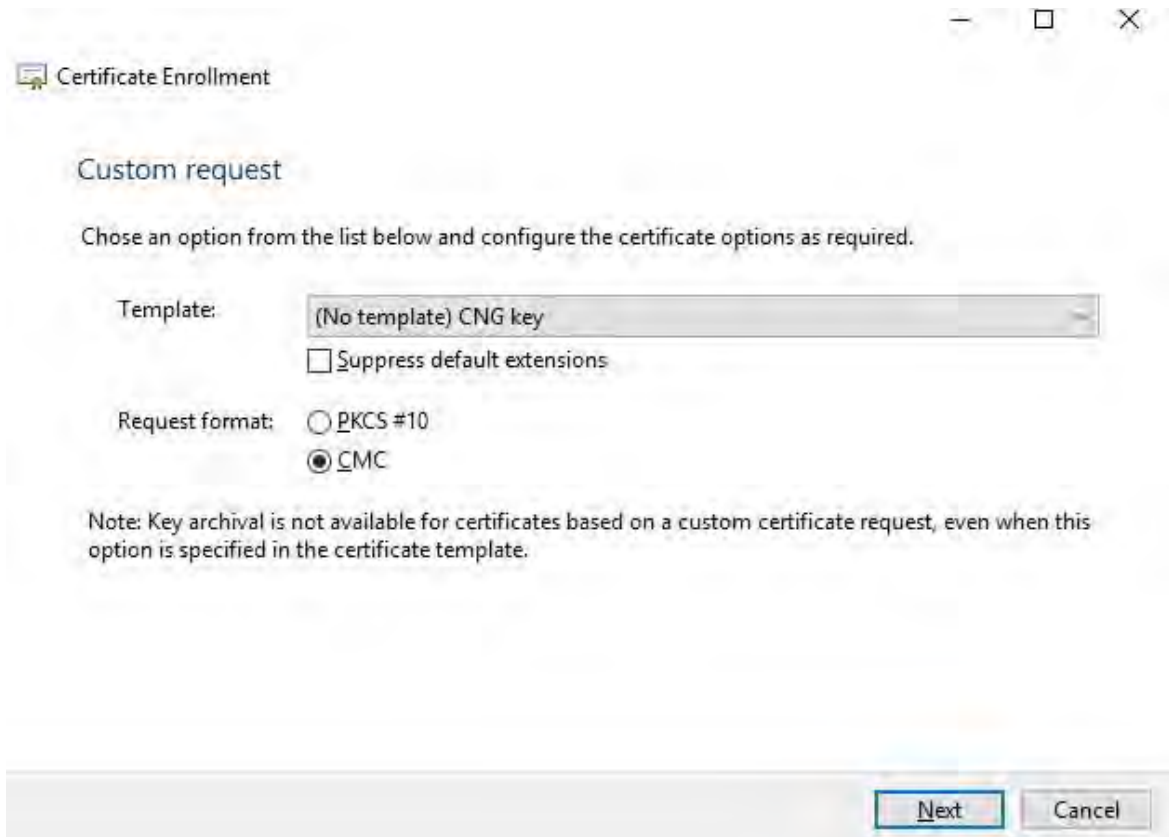
- Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner Persönlich und wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen.



- Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- Klicken Sie auf **Weiter**.



7. Wählen Sie die Vorlage **CNG-Schlüssel (keine Vorlage)** und das **CMC-Anforderungsformat** aus und

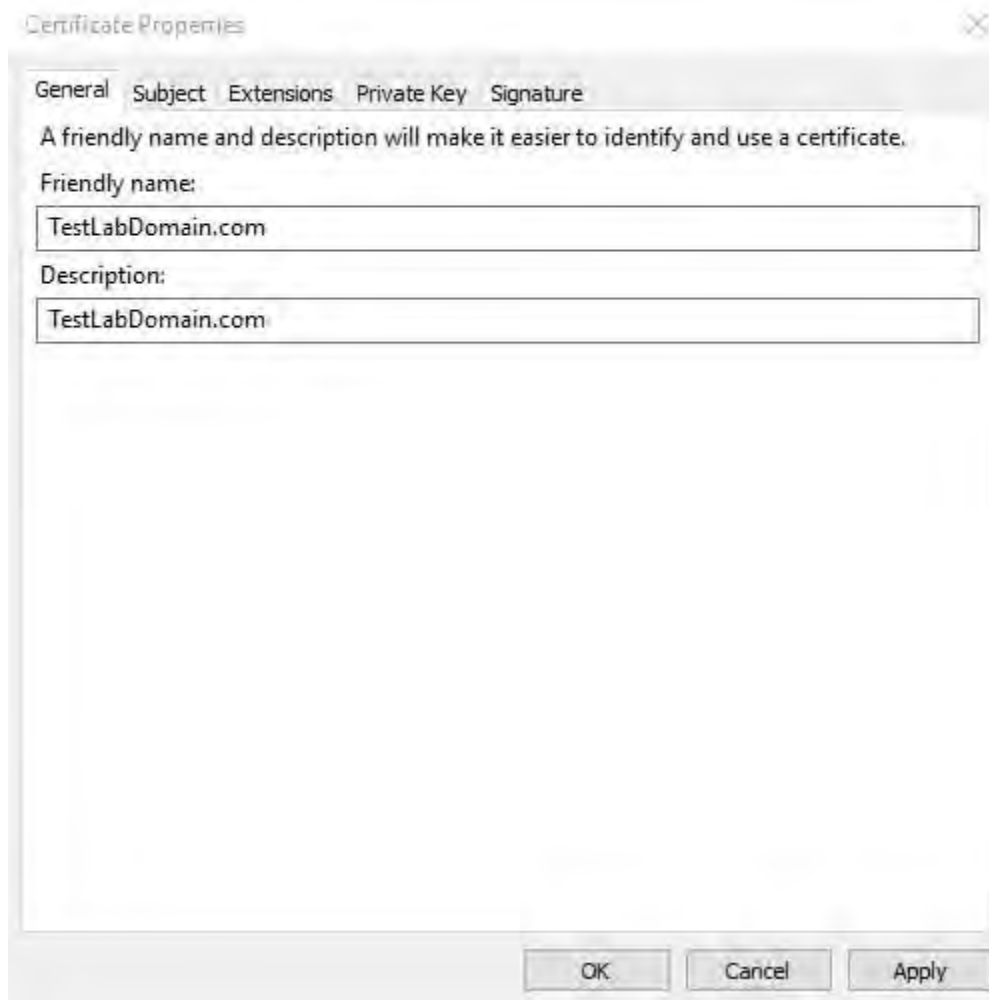


klicken Sie auf **Weiter**.

8. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf **Eigenschaften**.
9. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domännennamen aus, der bei der Zertifizierungsstelle registriert ist.



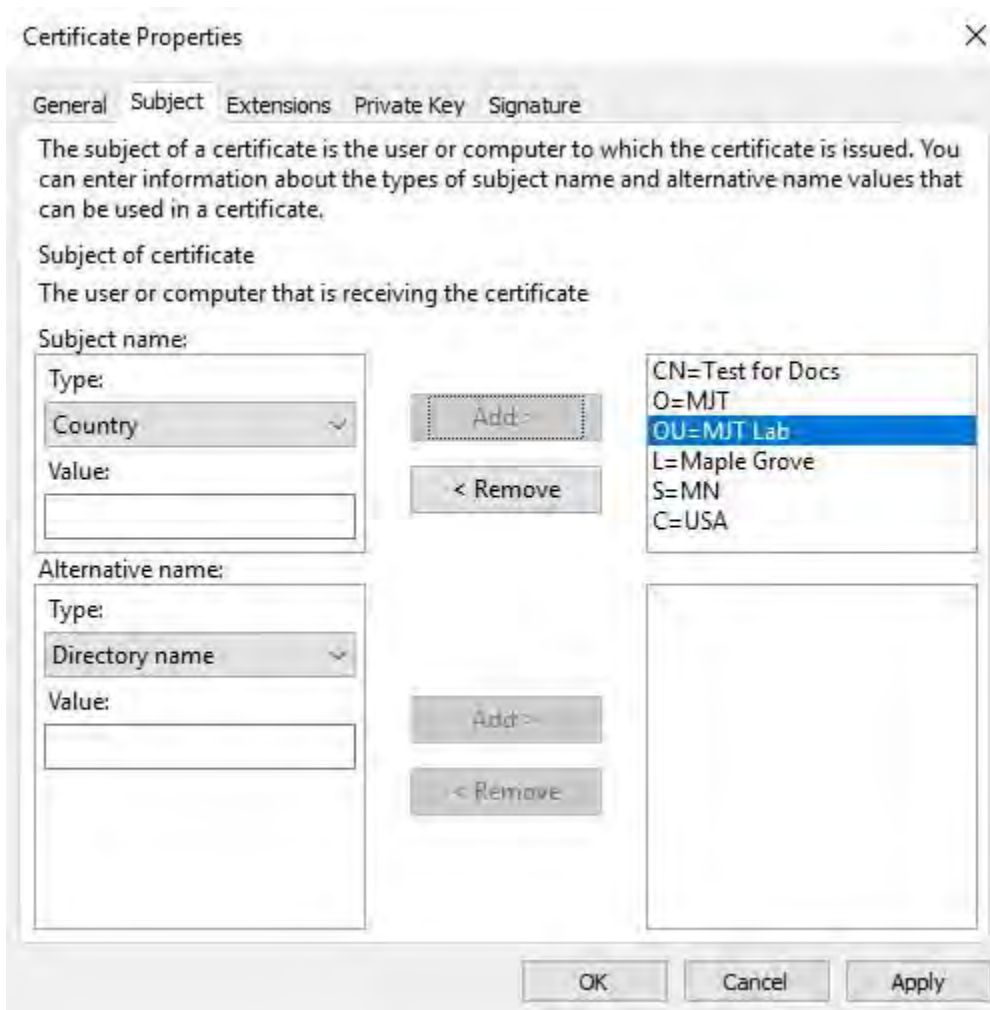
Das Anforderungsformat hängt von der Zertifizierungsstelle ab. Wenn das falsche Format ausgewählt wird, gibt die Zertifizierungsstelle einen Fehler aus, wenn die Zertifikatsignieranforderung (Certificate Signing Request, CSR) übermittelt wird. Wenden



10. Geben Sie auf der **Registerkarte Betreff** die Parameter ein, die für die jeweilige Zertifizierungsstelle erforderlich sind.

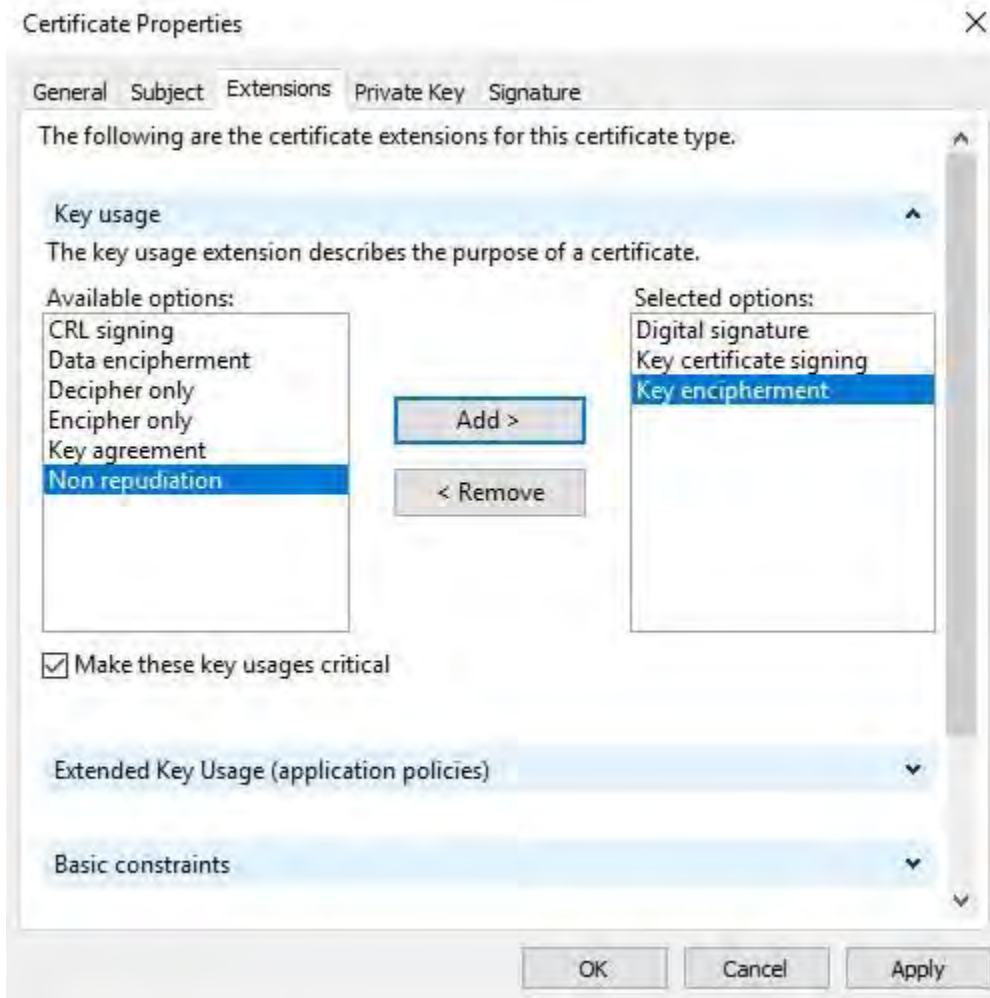
Beispielsweise sind der Antragstellername, der **Typ** und **der Wert** für jede Zertifizierungsstelle unterschiedlich. Ein Beispiel sind die folgenden erforderlichen Informationen:

- Trivialname:
- Organisation:
- Organisationseinheit :
- Stadt/Ort:
- Bundesland/Provinz:
- Land/Region:




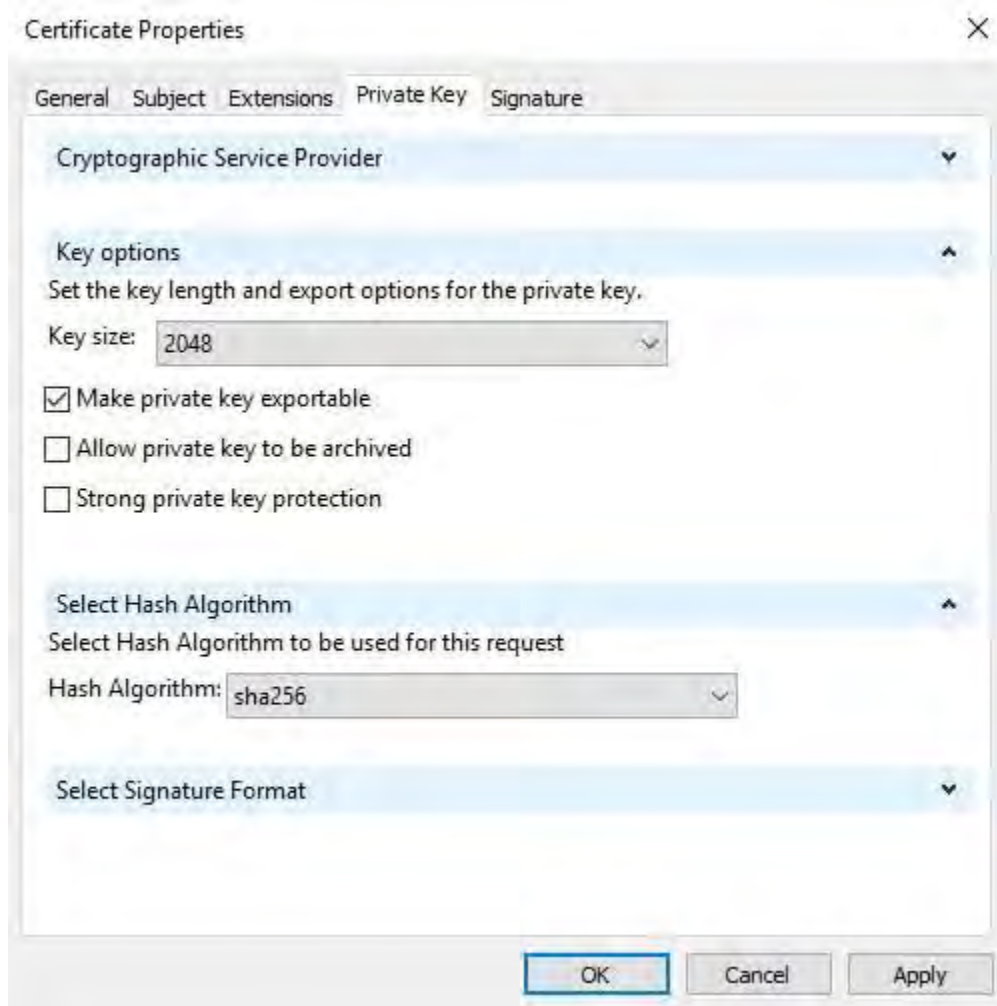
11. Für einige Zertifizierungsstellen sind keine Erweiterungen erforderlich. Wechseln Sie jedoch bei Bedarf zur **Registerkarte Erweiterungen**, und erweitern Sie das **Menü Schlüsselverwendung**. Fügen Sie der Liste Ausgewählte Optionen die erforderlichen Optionen aus der Liste **Verfügbare Optionen** hinzu .

12. Erweitern Sie **auf der Registerkarte Privater Schlüssel** das Menü **Schlüsselloptionen**.

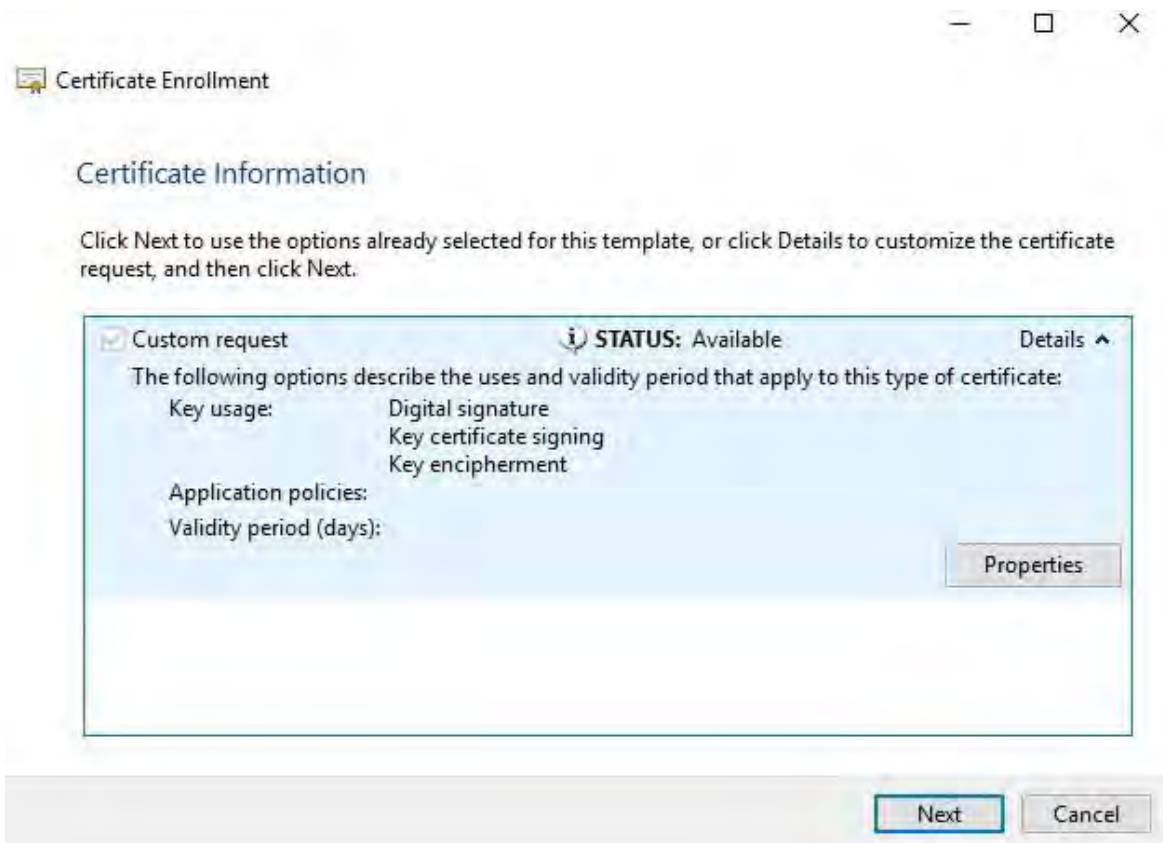


13. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen.

 Die Variable für die Schlüsselgröße wird von der Zertifizierungsstelle bestimmt, daher kann ein Schlüssel mit höherer Größe erforderlich sein. Möglicherweise sind auch andere Optionen, wie z. B. ein bestimmter Hash-Algorithmus (sha256), erforderlich. Passen Sie

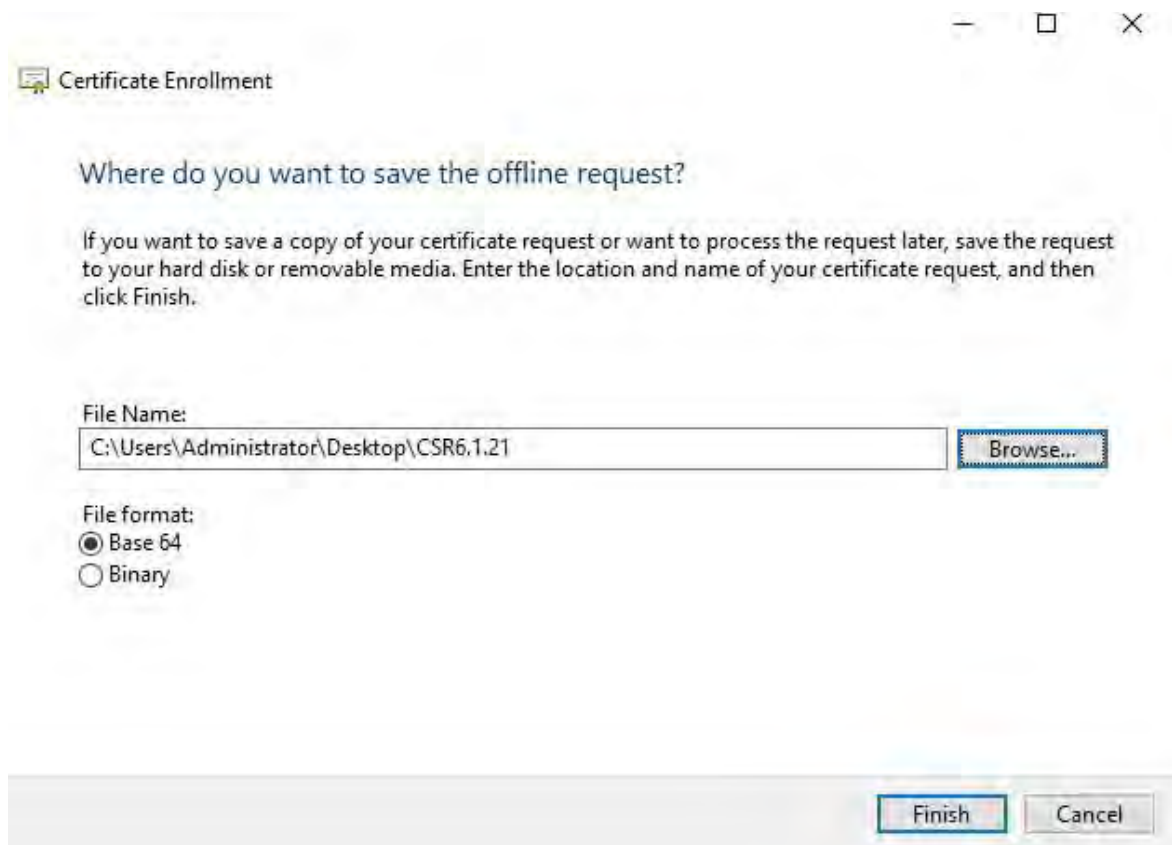


14. Sofern die Zertifizierungsstelle keine Signatur verlangt, besteht der nächste Schritt darin, auf **OK** zu klicken.
15. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **im Zertifikatregistrierungs-Assistenten** auf Weiter.



16. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist Basis 64, einige Zertifizierungsstellen erfordern jedoch das Binärformat.

17. Klicken Sie auf **Fertig stellen**.



Es wird eine **.req**-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

14.2 Laden Sie die **.req**-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.



Jede Zertifizierungsstelle hat einen anderen Prozess zum Hochladen von **.req**-Dateien, um im Gegenzug ein signiertes Zertifikat zu erhalten. In der Dokumentation Ihrer Zertifizierungsstelle finden Sie Informationen zum Abrufen eines signierten Zertifikats.

Bei der Arbeit mit dem Mobile Server wird empfohlen, eine Zertifizierungsstelle eines Drittanbieters zu verwenden. In den meisten Fällen ist es erforderlich, eine **.ZIP** Datei herunterzuladen und den Inhalt auf den Computer zu extrahieren, auf dem der Mobile Server gehostet wird.

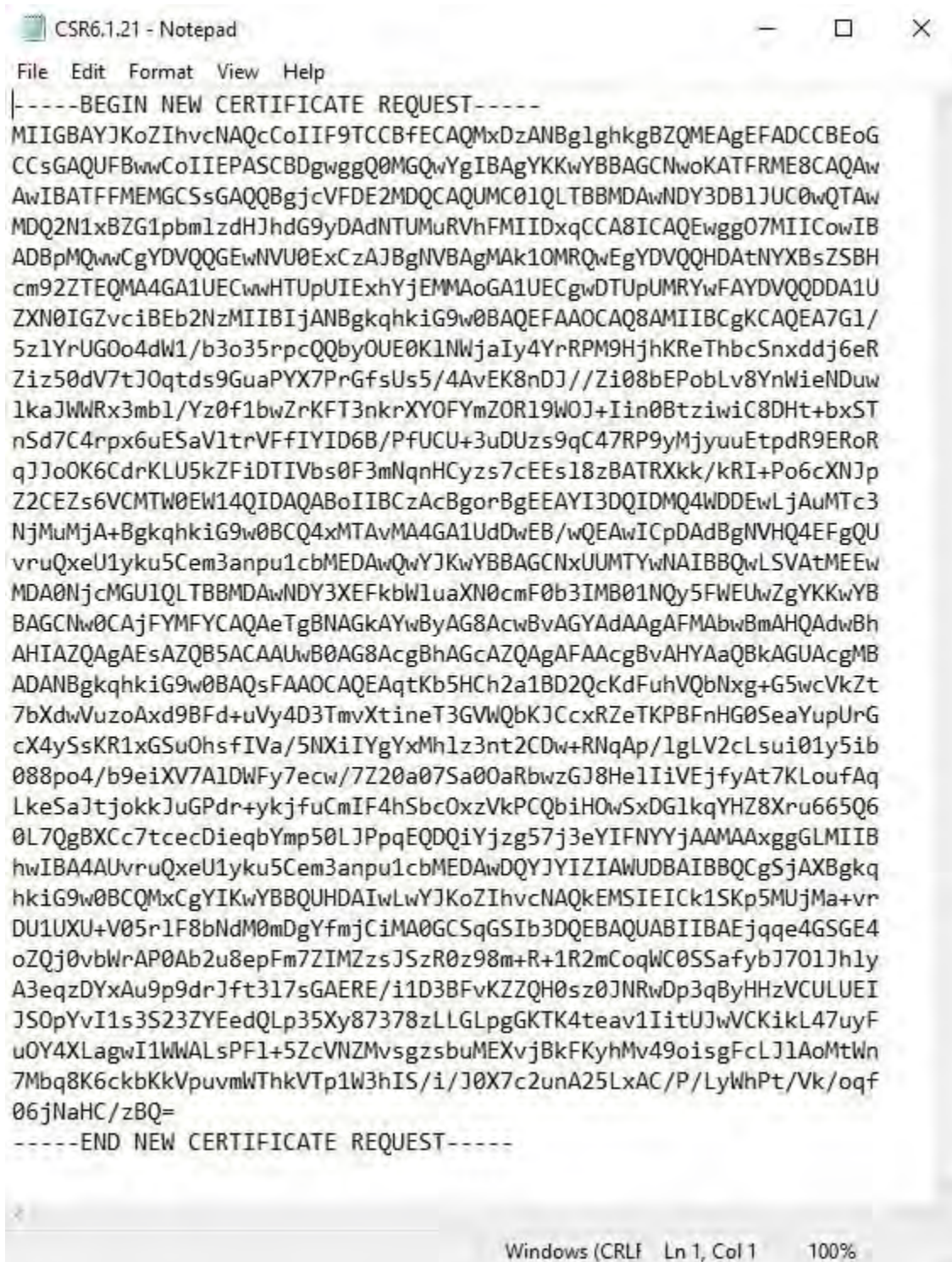
Es gibt mehrere Dateitypen, die in den extrahierten **.ZIP** Dateiinhalten enthalten sein können.

.CER oder **.CRT**-Dateien können auf ähnliche Weise installiert werden. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Zertifikat installieren aus** aus dem Kontextmenü.

In den folgenden Schritten wird eine **.CER**-Datei von einer internen Zertifizierungsstelle.

Ihre Zertifizierungsstelle benötigt den Inhalt der **REQ**-Datei. Sie werden aufgefordert, den gesamten Text der **REQ**-Datei, einschließlich der Anfangs- und Endzeilen, zu kopieren und den Text in ein Feld einzufügen, das in einem von der Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

1. Navigieren Sie zum Speicherort der REQ-Datei, öffnen Sie sie in Editor, und fügen Sie den Text in ein Feld ein, das in einem von Ihrer Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.



```
CSR6.1.21 - Notepad
File Edit Format View Help
|-----BEGIN NEW CERTIFICATE REQUEST-----
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBFECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG
CCsGAQUFBwwCoIIEPASCBDgwgGQ0MGQwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw
AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw
MDQ2N1xBZG1pbm1zdHJhdG9yDAANTUMuRVhFMIIDxqCCA8ICAQEwgG07MIICowIB
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAGMAk1OMRQwEgYDVQQHDA1NYXBsZSBH
cm92ZTEQMA4GA1UECwwHTUUpUIExhYjEMMAoGA1UECgwDTUUpUMRYwFAYDVQQDDA1U
ZXN0IGZvcjBEB2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/
5z1YrUG0o4dW1/b3o35rpcQQbyOUE0K1NwjaIy4YrRPM9HjhKReThbcSnxddj6eR
Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw
lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W0J+Iin0BtziwiC8DHT+bxST
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDuzs9qC47RP9yMjyuuEtpdR9ERoR
qJJ0oK6CdrKLU5kZFIDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDEwLjAuMtc3
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEW
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbl1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh
AHIAZQAgaEAsAZQB5ACAuUwB0AG8AcgBhAGcAZQAgaFAAcgBvAHYAaQBkAGUAcgMB
ADANBgkqhkiG9w0BAQsFAAOCAQEAAqtKb5HCh2a1BD2QcKdFuhVQbNxxg+G5wcVkJz
7bXdwWuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG
cX4ySsKR1xGSu0hsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2cLsuio1y5ib
088po4/b9eiXV7A1DWfY7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAq
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbc0xzVkJPCQbIH0wSxDG1kqYHZ8Xru665Q6
0L7QgBXCc7tcecDieqbYmp50LJppqEQDQIYjz57j3eYIFNYYjAAMAAxggGLMIIB
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEIck1SKp5MUjMa+vr
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jhly
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI
JS0pYvI1s3S23ZYEdQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF
u0Y4XLagwI1WWALsPF1+5ZcVNZMvszsbuMEXvjbkFKyhMv49oisgFcLJ1AoMtWn
7Mbq8K6ckbKkVpuvmlWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf
06jNaHC/zBQ=
-----END NEW CERTIFICATE REQUEST-----
```

2. Wenn Sie das Zertifikat von Ihrer Zertifizierungsstelle erhalten, navigieren Sie zum Ordner "Downloads" (oder an einem anderen Ort, an dem Sie den Ordner auf dem Computer speichern möchten), klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **"Zertifikat installieren"** aus.



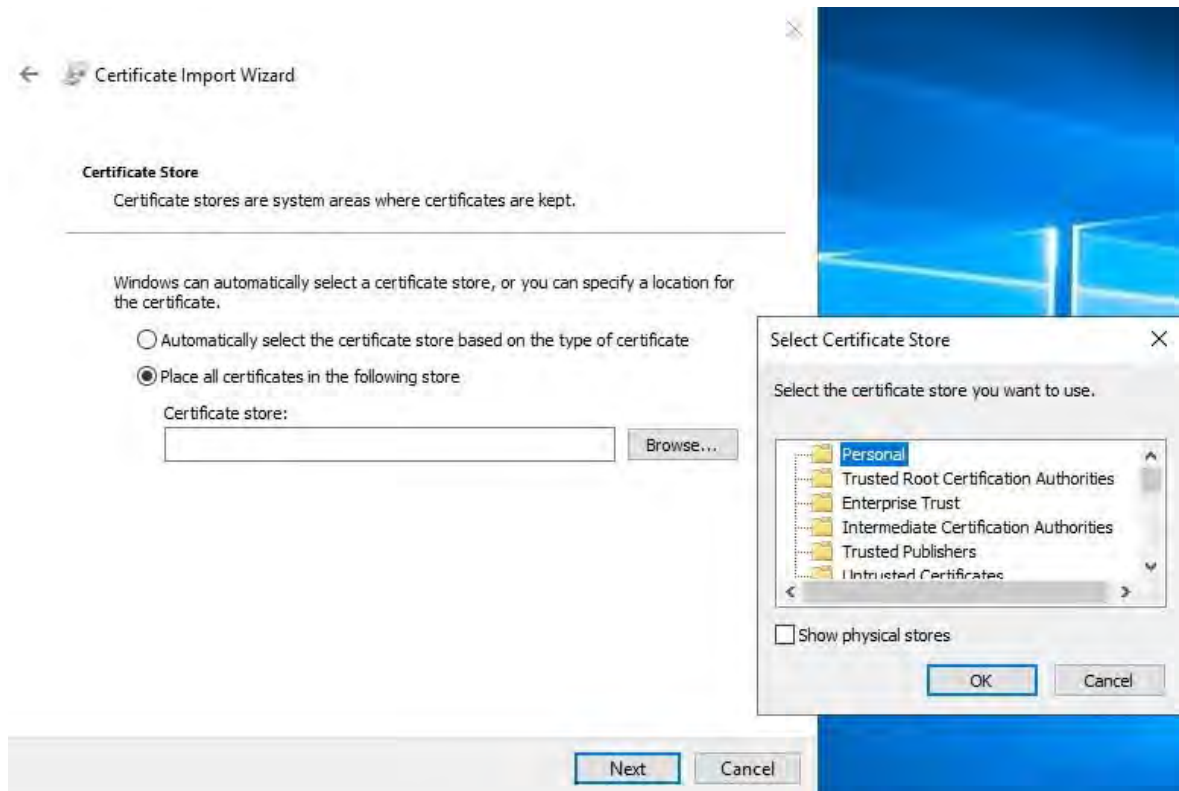
3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.

4. Wählen Sie diese Option aus, um das Zertifikat für den lokalen Computer zu installieren, und klicken Sie auf



Weiter.

5. Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf **Weiter**.



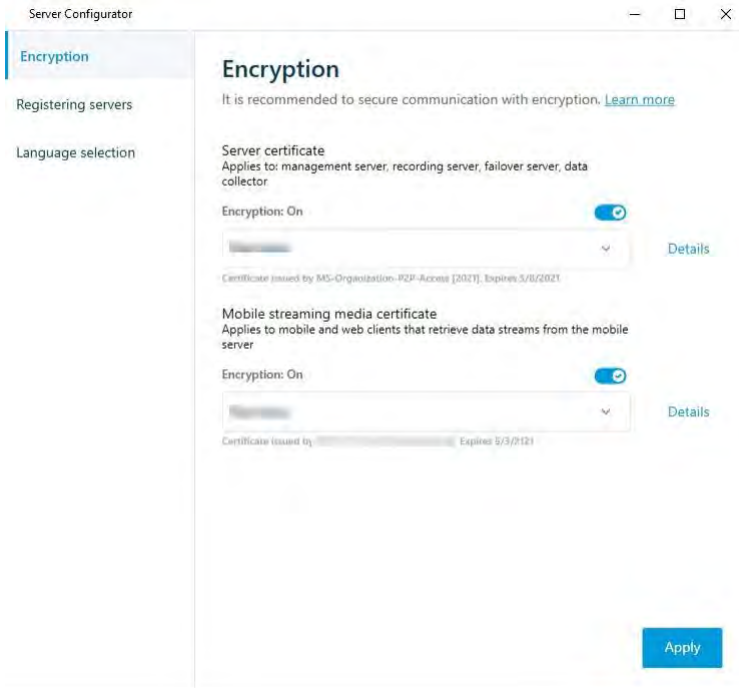
6. Beenden Sie den Assistenten zum Installieren von Zertifikaten.

14.3 Aktivieren der Verschlüsselung auf dem Mobile Server

Nachdem das Zertifikat auf dem Computer installiert wurde, auf dem der Mobile Server gehostet wird, gehen Sie wie folgt vor.

1. Öffnen Sie auf einem Computer, auf dem ein Mobile Server installiert ist, den **Server-Konfigurator** über:
 - Das Windows-Startmenü
oder
 - Den Mobile Server Manager, indem Sie mit der rechten Maustaste auf das Mobile Server Manager-Symbol in der Taskleiste des Computers klicken
2. Aktivieren Sie im Server-Konfigurator unter Mobiles Streaming-Media-Zertifikat die Option Encryption.
3. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
4. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem MOBOTIX HUB Mobile Client und dem MOBOTIX HUB Web Client mit dem Mobile Server zu verschlüsseln.

Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen. Dem Benutzer des Mobile Server-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.



5. Klicken Sie auf **Übernehmen**.



Wenn Sie Zertifikate anwenden, wird der Mobile Server-Dienst neu gestartet.

Weitere Informationen finden Sie unter:

Video zum Powershell-Prozess.

Whitepaper zu Zertifikaten mit dem Mobile Server.

15 Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder Recording Server

Management-Server und Aufzeichnungsserver benötigen keine vertrauenswürdigen Zertifikate von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Verschlüsselung, aber Sie können diese Zertifikate verwenden, wenn dies Teil Ihrer Sicherheitsrichtlinie ist, und sie werden automatisch von Client-Workstations und -Servern als vertrauenswürdig eingestuft.

Der Vorgang ist identisch mit der Installation des Mobile Server-Zertifikats.



Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert



Zertifikate, die von einer Zertifizierungsstelle (CA) ausgestellt wurden, verfügen über eine Kette von Zertifikaten, und im Stammverzeichnis dieser Kette befindet sich das Stammzertifikat der Zertifizierungsstelle. Wenn ein Gerät oder Browser dieses Zertifikat sieht, vergleicht es sein Stammzertifikat mit den auf dem Betriebssystem (Android, iOS, Windows usw.) vorinstallierten Zertifikaten. Wenn das Stammzertifikat in der Liste der vorinstallierten Zertifikate aufgeführt ist, stellt das Betriebssystem dem Benutzer sicher, dass

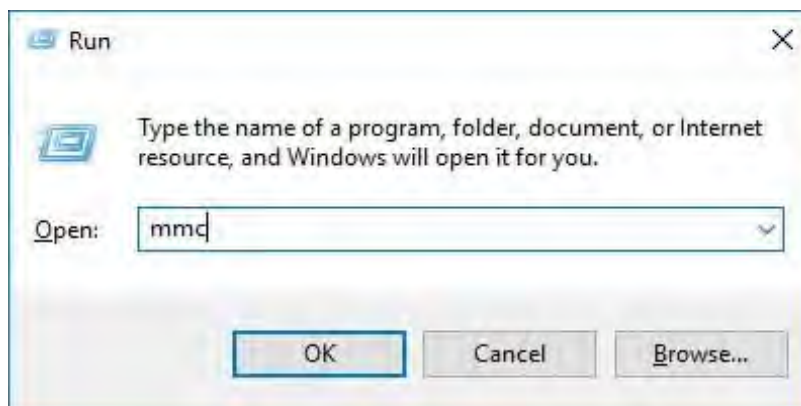
15.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

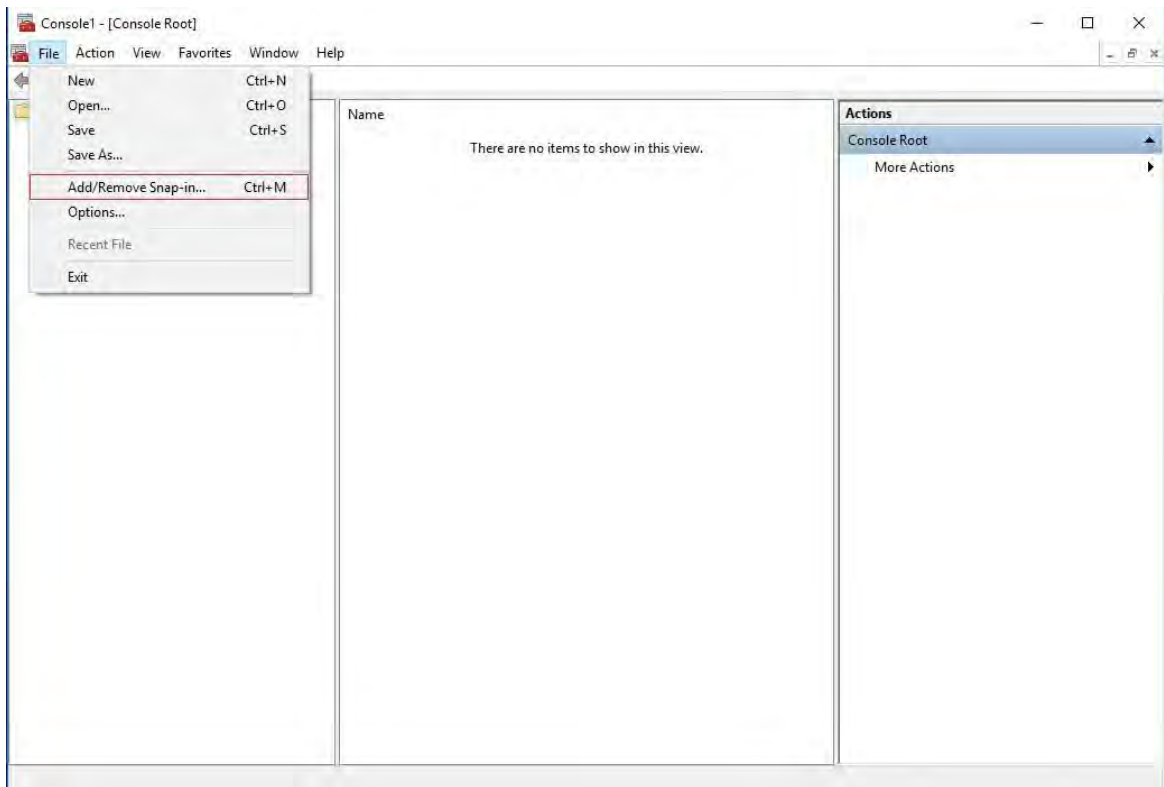
Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.



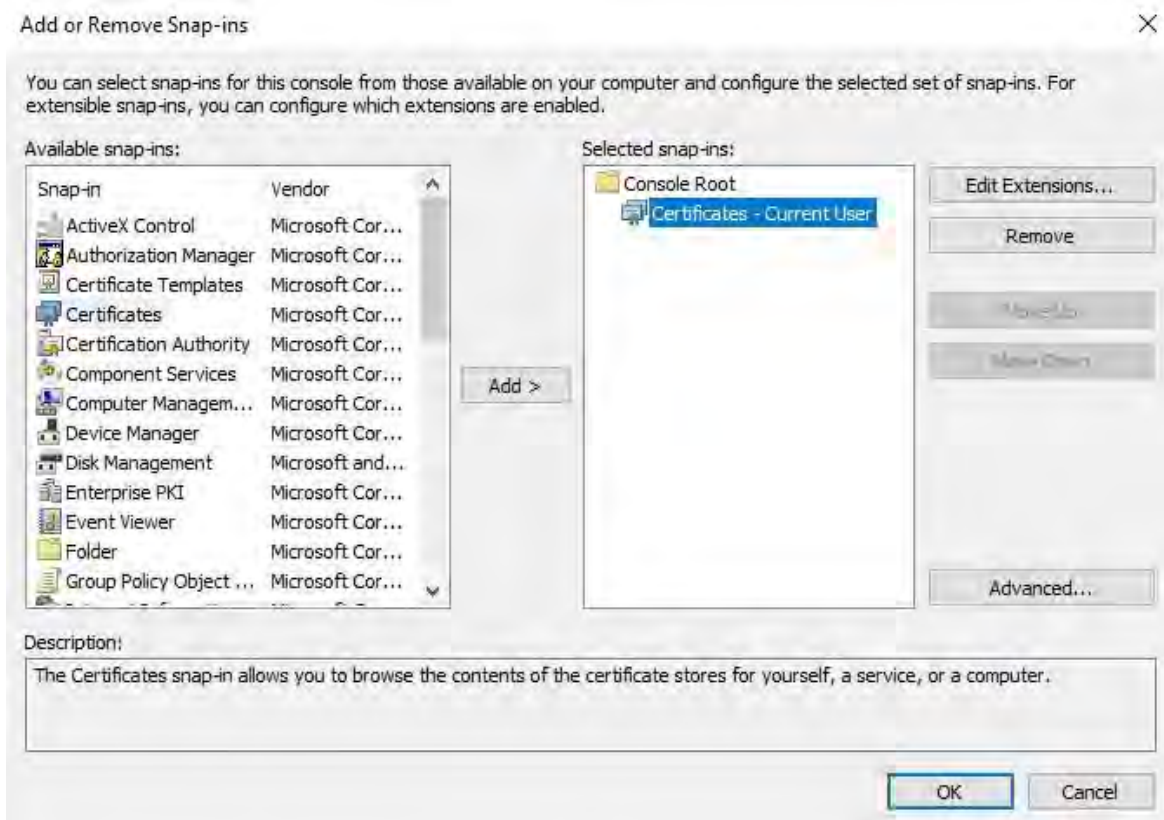
Bestimmte Parameter hängen von der Zertifizierungsstelle ab. Lesen Sie die Dokumentation Ihrer Zertifizierungsstelle, bevor Sie fortfahren.

1. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In hinzufügen/entfernen...**

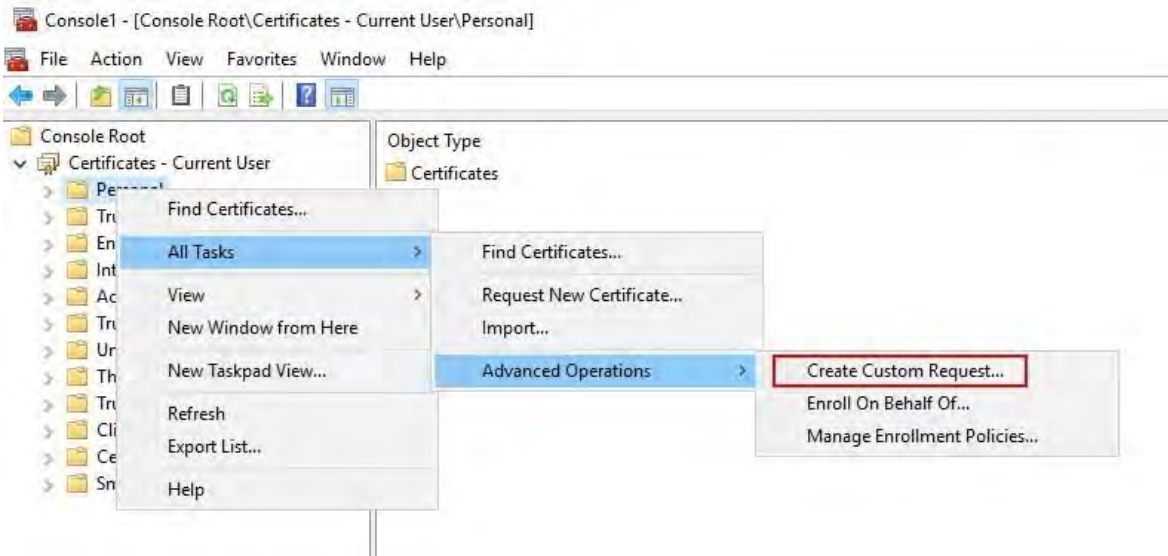




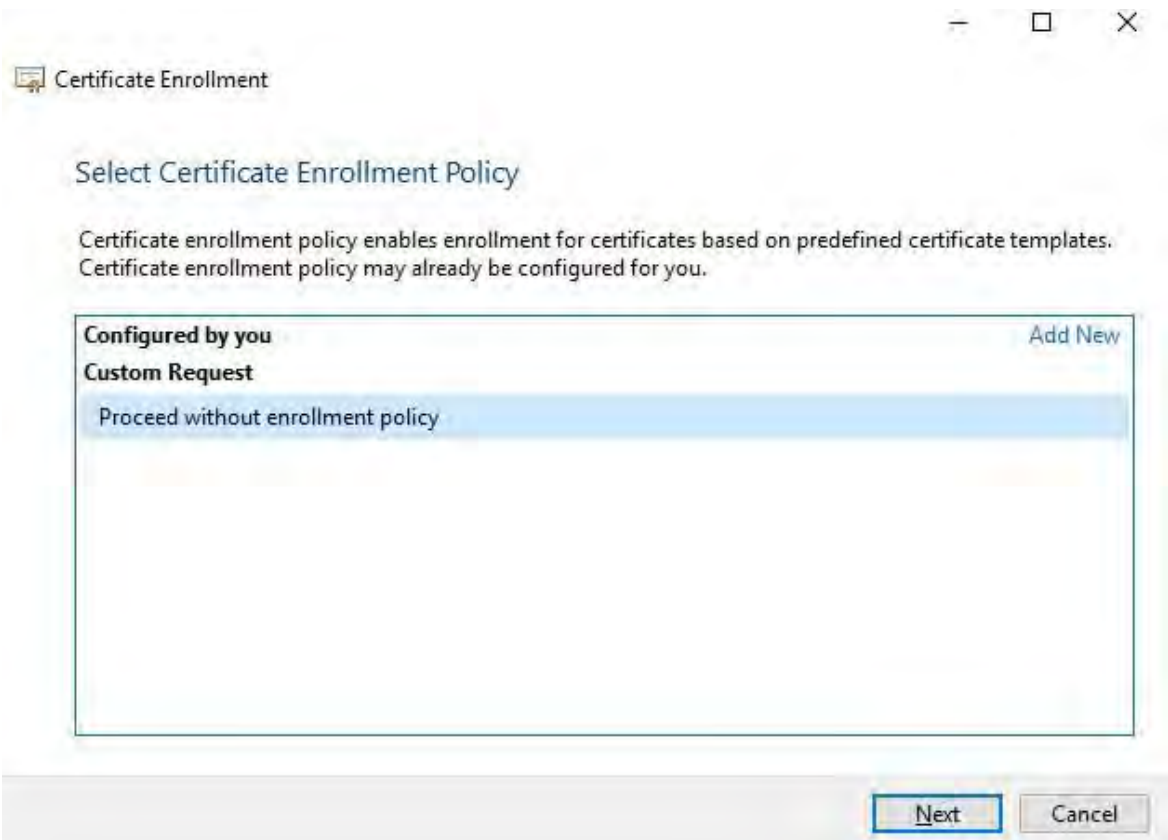
2. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **OK**.



- 4. Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den Ordner Persönlich und wählen Sie **Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen**.

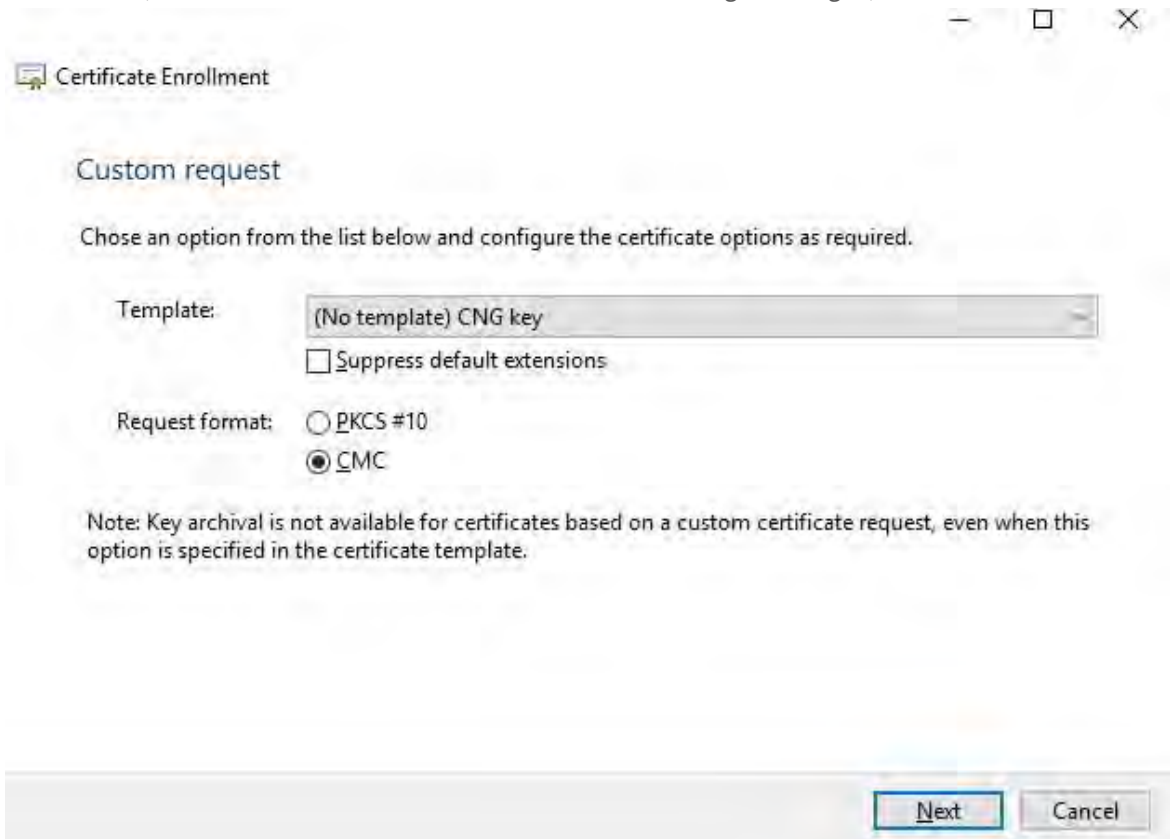


- 5. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- 6. Klicken Sie auf Weiter.




- 7. Wählen Sie die Vorlage **CNG-Schlüssel (keine Vorlage)** und das **CMC-Anforderungsformat** aus und klicken Sie auf **Weiter**.

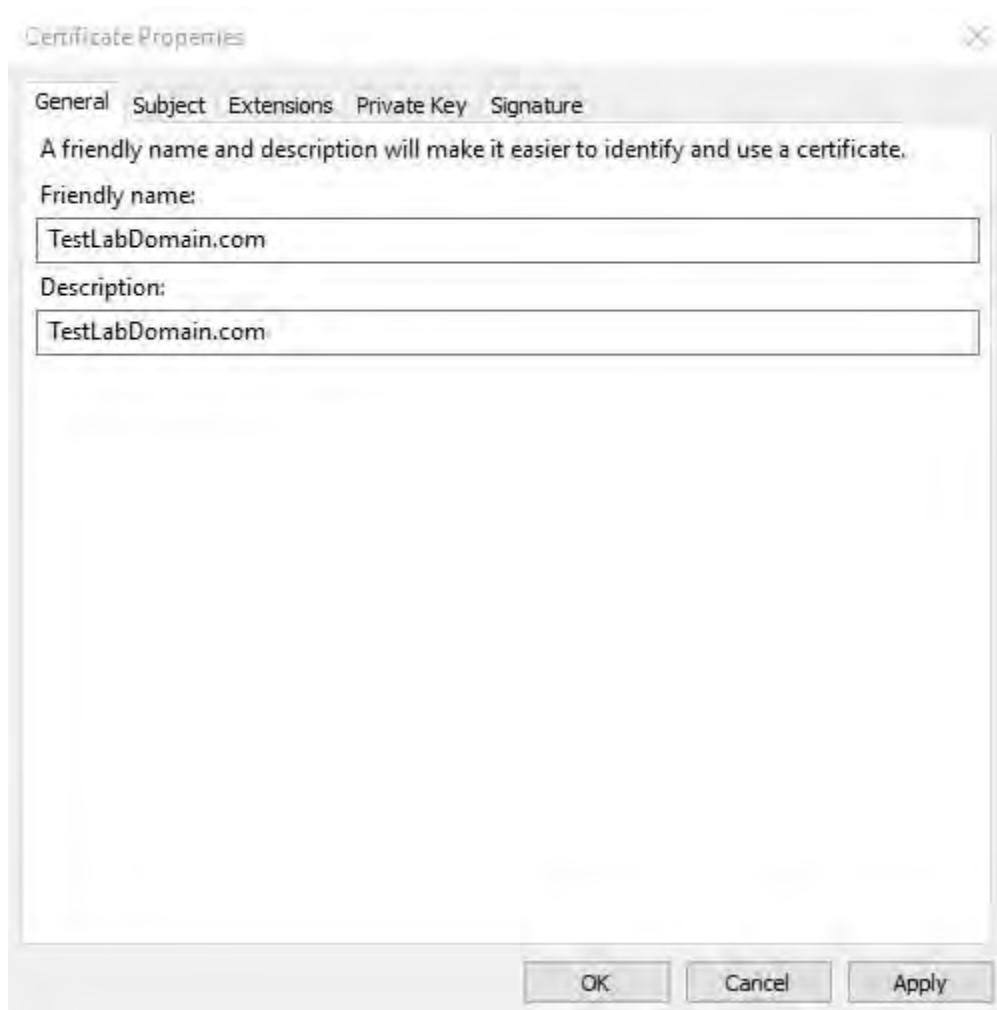
8. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf



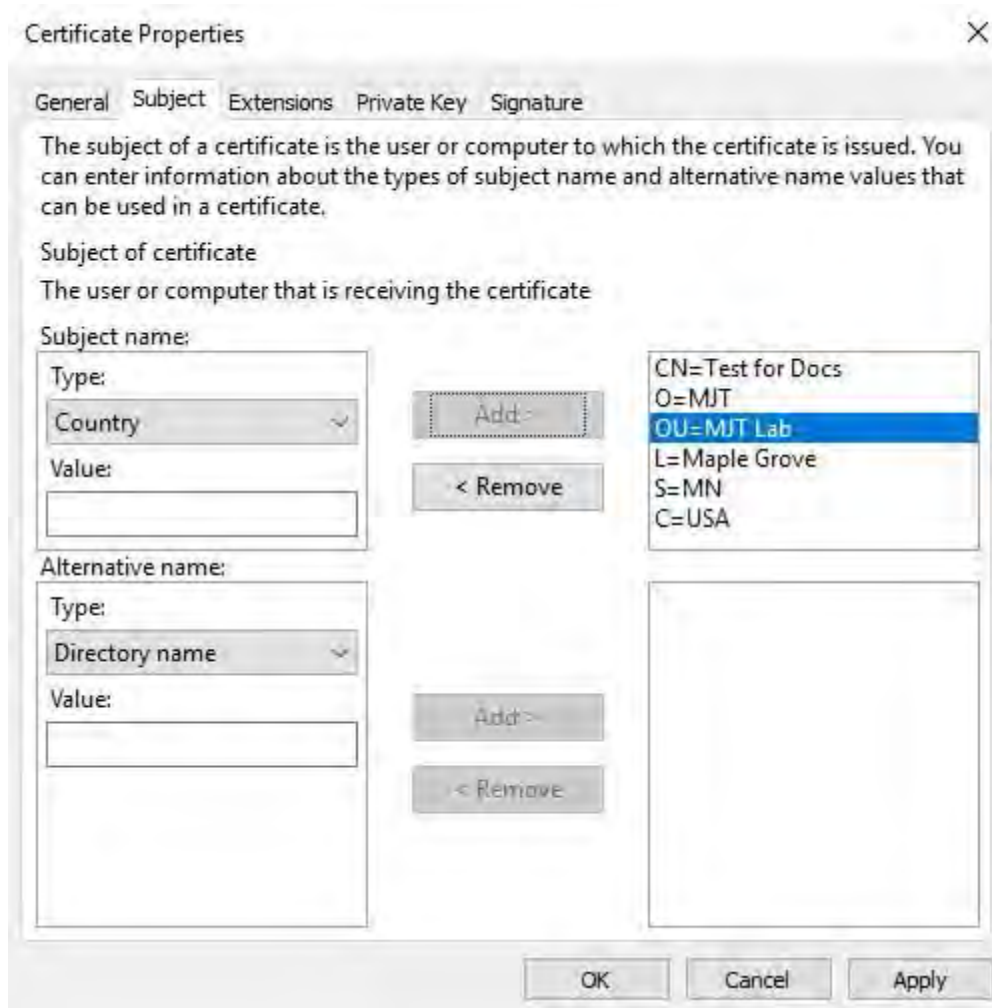
Eigenschaften.

 Das Anforderungsformat hängt von der Zertifizierungsstelle ab. Wenn das falsche Format ausgewählt wird, gibt die Zertifizierungsstelle einen Fehler aus, wenn die Zertifikatsignieranforderung (Certificate Signing Request, CSR) übermittelt wird. Wenden

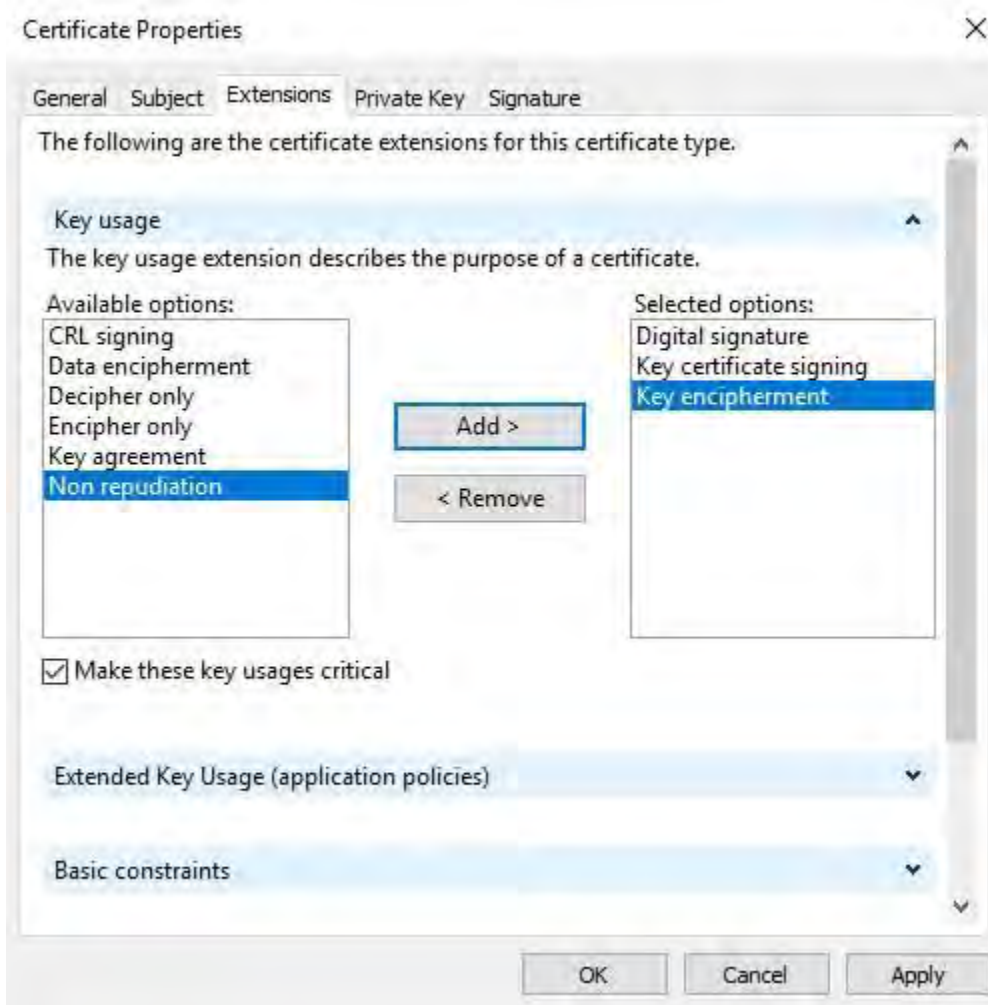
9. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domännennamen aus, der bei der Zertifizierungsstelle registriert ist.



10. Geben Sie auf der **Registerkarte Betreff** die Parameter ein, die für die jeweilige Zertifizierungsstelle erforderlich sind.
11. Beispielsweise sind der Antragstellername, der **Typ** und **der Wert** für jede Zertifizierungsstelle unterschiedlich. Ein Beispiel sind die folgenden erforderlichen Informationen:
- Trivialname:
 - Organisation:
 - Organisationseinheit :
 - Stadt/Ort:
 - Bundesland/Provinz:
 - Land/Region:



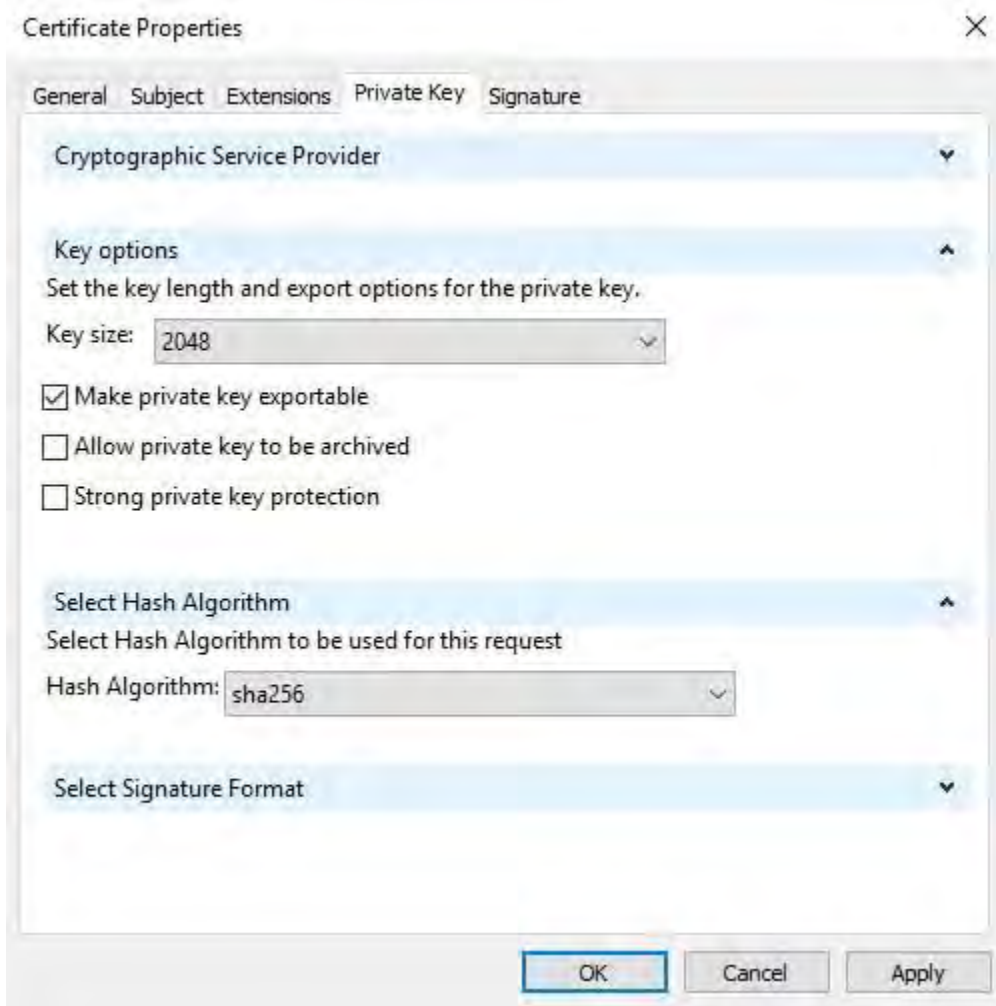
12. Für einige Zertifizierungsstellen sind keine Erweiterungen erforderlich. Wechseln Sie jedoch bei Bedarf zur **Registerkarte Erweiterungen**, und erweitern Sie das **Menü Schlüsselverwendung**. Fügen Sie der Liste Ausgewählte Optionen die erforderlichen Optionen aus der Liste **Verfügbare Optionen** hinzu .



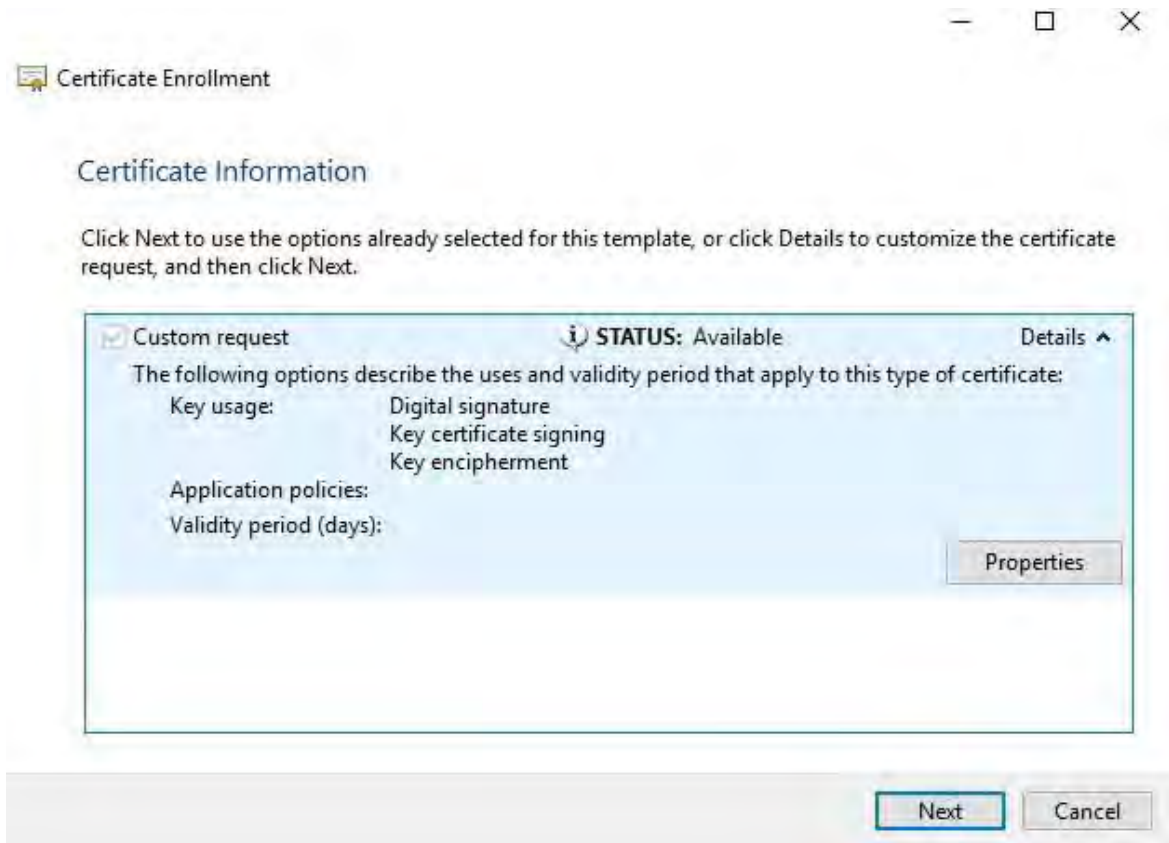
13. Erweitern Sie **auf der Registerkarte Privater Schlüssel** das Menü **Schlüsseloptionen**.
14. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen.



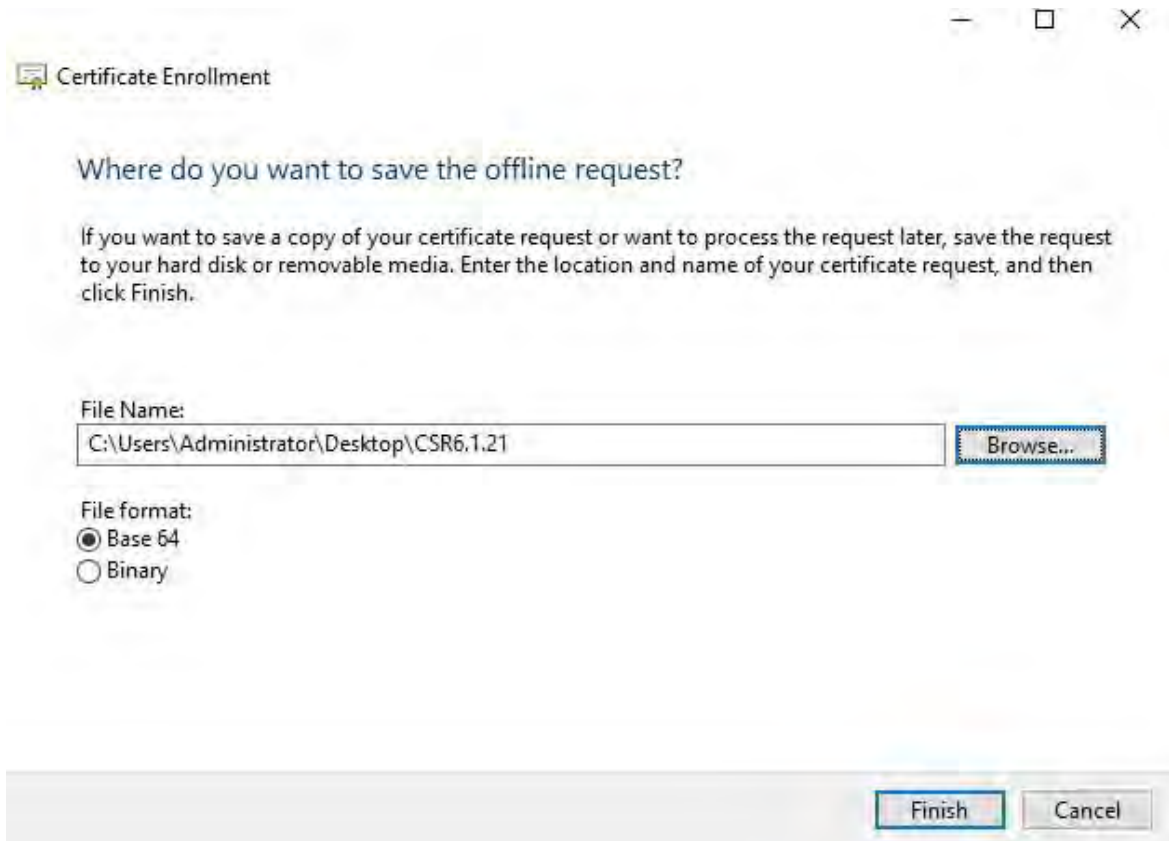
Die Variable für die Schlüsselgröße wird von der Zertifizierungsstelle bestimmt, daher kann ein Schlüssel mit höherer Größe erforderlich sein. Möglicherweise sind auch andere Optionen, wie z. B. ein bestimmter Hash-Algorithmus (sha256), erforderlich. Passen Sie



- 15. Sofern die Zertifizierungsstelle keine Signatur verlangt, besteht der nächste Schritt darin, auf **OK zu** klicken.
- 16. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter.



- 17. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist Basis 64, einige Zertifizierungsstellen erfordern jedoch das Binärformat.
- 18. Klicken Sie auf **Fertig stellen**.



Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

15.2 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.



Jede Zertifizierungsstelle hat einen anderen Prozess zum Hochladen von .req-Dateien, um im Gegenzug ein signiertes Zertifikat zu erhalten. In der Dokumentation Ihrer Zertifizierungsstelle finden Sie Informationen zum Abrufen eines signierten Zertifikats.

In den meisten Situationen mit Zertifizierungsstellen von Drittanbietern ist es erforderlich, eine .ZIP Datei herunterzuladen und den Inhalt auf den Computer zu extrahieren, auf dem der MOBOTIX HUB-Server gehostet wird.

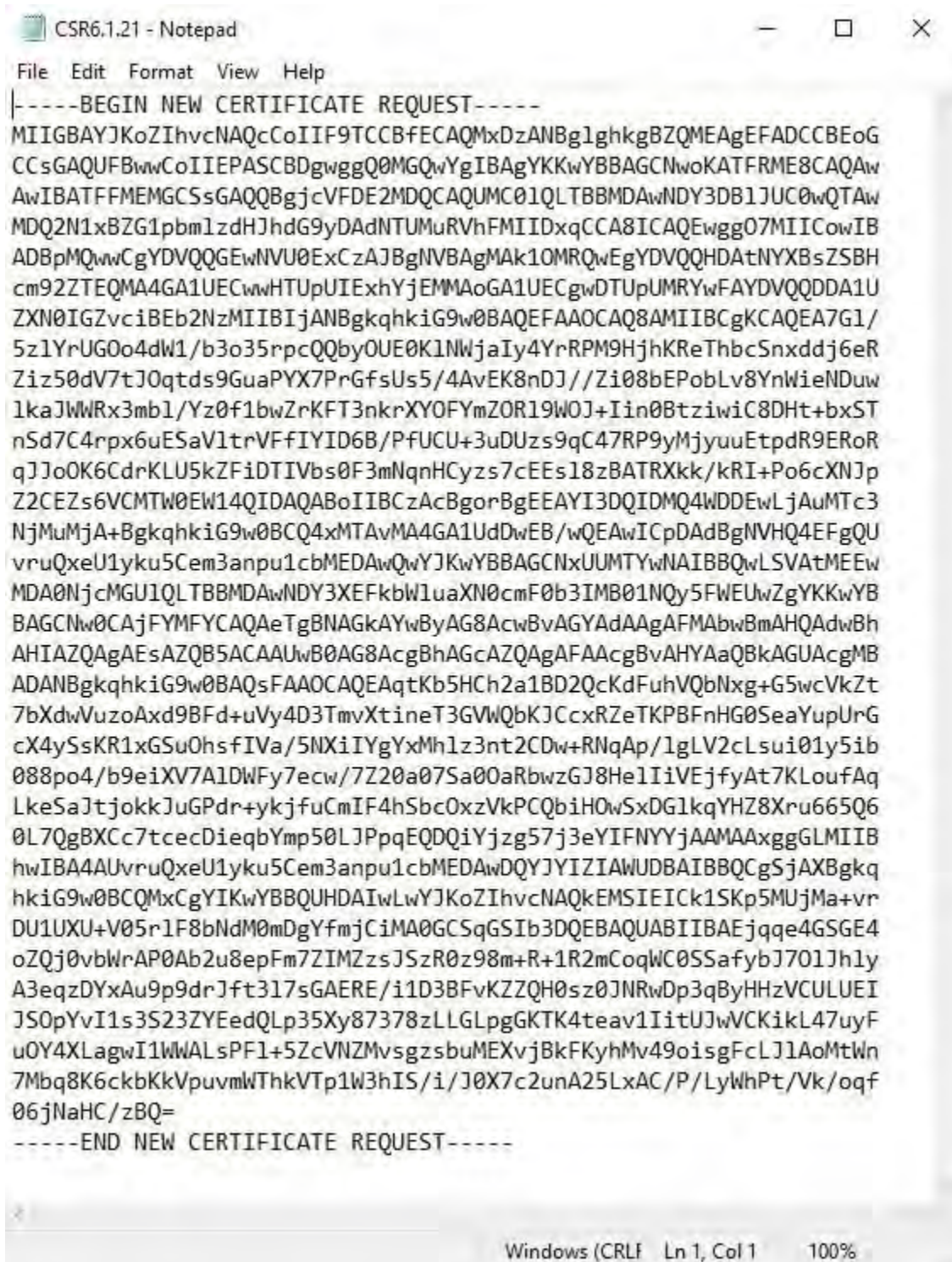
Es gibt mehrere Dateitypen, die in den extrahierten .ZIP Dateiinhalten enthalten sein können.

. CER oder . CRT-Dateien können auf ähnliche Weise installiert werden. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Zertifikat installieren aus.** aus dem Kontextmenü.

In den folgenden Schritten wird eine . CER-Datei von einer internen Zertifizierungsstelle.

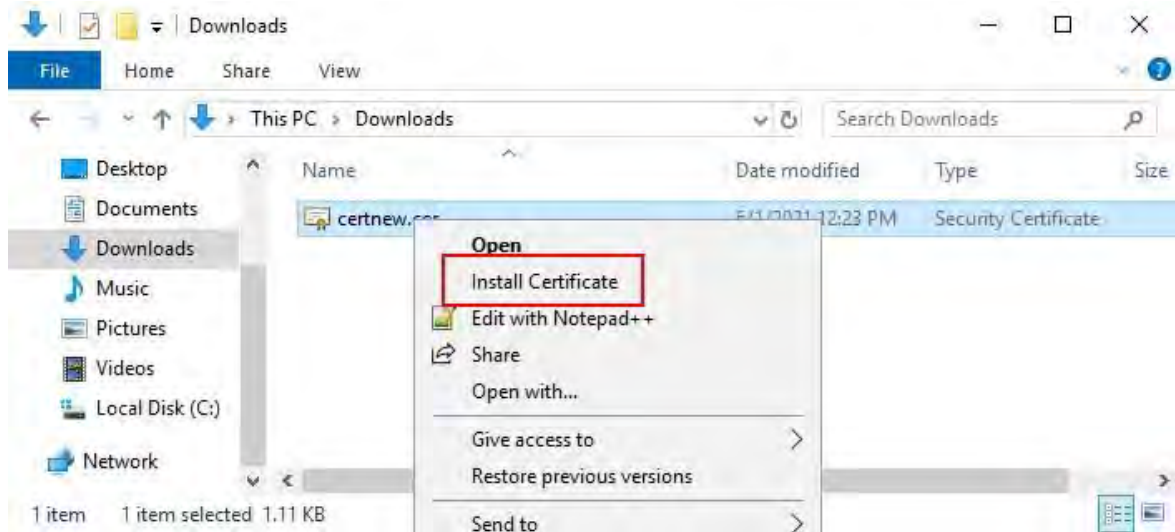
Ihre Zertifizierungsstelle benötigt den Inhalt der REQ-Datei. Sie werden aufgefordert, den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, zu kopieren und den Text in ein Feld einzufügen, das in einem von der Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.

1. Navigieren Sie zum Speicherort der REQ-Datei, öffnen Sie sie in Editor, und fügen Sie den Text in ein Feld ein, das in einem von Ihrer Zertifizierungsstelle verwalteten Portal zur Verfügung gestellt wird.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIGBAYJKoZIhvcNAQcCoIIF9TCCBFECAQMxDzANBg1ghkgBZQMEAgEFADCCBEoG
CCsGAQUFBwwCoIIEPASCBDgwgGQ0MQGwYgIBAgYKKwYBBAGCNwoKATFRME8CAQAw
AwIBATFFMEMGCSsGAQQBgjcVFDE2MDQCAQUMC01QLTBBMDAwNDY3DB1JUC0wQTAw
MDQ2N1xBZG1pbm1zdHJhdG9yDAANTUMuRvhFMIIDxqCCA8ICAQEwgG07MIICowIB
ADBpMQwwCgYDVQQGEwNVU0ExCzAJBgNVBAGMAk1OMRQwEgYDVQQHDA1NYXBsZSBH
cm92ZTEQMA4GA1UECwwHTUUpUIExhYjEMMAoGA1UECgwDTUUpUMRYwFAYDVQQDDA1U
ZXN0IGZvcjBEB2NzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7G1/
5z1YrUG0o4dW1/b3o35rpcQQbyOUE0K1NwjaIy4YrRPM9HjhKReThbcSnxddj6eR
Ziz50dV7tJ0qtds9GuaPYX7PrGfsUs5/4AvEK8nDJ//Zi08bEPobLv8YnWieNDuw
lkaJWWRx3mb1/Yz0f1bwZrKFT3nkrXY0FYmZOR19W0J+Iin0BtziwiC8DHT+bxST
nSd7C4rpx6uESaV1trVFfIYID6B/PfUCU+3uDuzs9qc47RP9yMjyuuEtpdR9ERoR
qJJ0K6CdrKLU5kZFIDTIVbs0F3mNqnHCyzs7cEEs18zBATRXkk/kRI+Po6cXNJp
Z2CEZs6VCMTW0EW14QIDAQABoIIBCzAcBgorBgEEAYI3DQIDMQ4WDEwLjAuMtc3
NjMuMjA+BgkqhkiG9w0BCQ4xMTAvMA4GA1UdDwEB/wQEAwICpDAdBgNVHQ4EFgQU
vruQxeU1yku5Cem3anpu1cbMEDAwQwYJKwYBBAGCNxUUMTYwNAIBBQwLSVAtMEEW
MDA0NjcMGU1QLTBBMDAwNDY3XEFkbw1uaXN0cmF0b3IMB01NQy5FWEUwZgYKKwYB
BAGCNw0CAjFYMFYCAQAeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAbwBmAHQAdwBh
AHIAZQAgaEAsAZQB5ACAuUwB0AG8AcgBhAGcAZQAgaFAAcgBvAHYAaQBkAGUAcgMB
ADANBgkqhkiG9w0BAQsFAAOCAQEAAqtKb5HCh2a1BD2QcKdFuhVQbNxxg+G5wcVkJz
7bXdwWuzoAxd9BFd+uVy4D3TmvXtineT3GVWQbKJCcxRZeTKPBFnHG0SeaYupUrG
cX4ySsKR1xGSu0hsfIVa/5NXiIYgYxMh1z3nt2CDw+RNqAp/1gLV2cLsuio1y5ib
088po4/b9eiXV7A1DWFy7ecw/7Z20a07Sa00aRbwzGJ8He1IiVEjfyAt7KLoufAq
LkeSaJtjokkJuGPdr+ykjfuCmIF4hSbc0xzVkJPCQbIH0wSxDG1kqYHZ8Xru665Q6
0L7QgBXCc7tcecDieqbYmp50LJppqEQDQiyjz57j3eYIFNYYjAAMAAxggGLMIIB
hwIBA4AUvruQxeU1yku5Cem3anpu1cbMEDAwDQYJYIZIAWUDBAIBBQCgSjAXBgkq
hkiG9w0BCQMxCgYIKwYBBQUHDAIwLwYJKoZIhvcNAQkEMSIEIck1SKp5MUjMa+vr
DU1UXU+V05r1F8bNdM0mDgYfmjCiMA0GCSqGSIb3DQEBAQUABIIBAEjqqe4GSGE4
oZQj0vbWrAP0Ab2u8epFm7ZIMZzsJSzR0z98m+R+1R2mCoqWC0SSafybJ701Jhly
A3eqzDYxAu9p9drJft317sGAERE/i1D3BFvKZZQH0sz0JNRwDp3qByHHzVCULUEI
JS0pYvI1s3S23ZYEdQLp35Xy87378zLLGLpgGKTK4teav1IitUJwVCKikL47uyF
u0Y4XLagwI1WWALsPF1+5ZcVNZMvszsbuMEXvjbkFKyhMv49oisgFcLJ1AoMtWn
7Mbq8K6ckbKkVpuvmlWThkVTp1W3hIS/i/J0X7c2unA25LxAC/P/LyWhPt/Vk/oqf
06jNaHC/zBQ=
-----END NEW CERTIFICATE REQUEST-----
```

2. Wenn Sie das Zertifikat von Ihrer Zertifizierungsstelle erhalten, navigieren Sie zum Ordner "Downloads" (oder an einem anderen Ort, an dem Sie den Ordner auf dem Computer speichern möchten), klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **"Zertifikat installieren"** aus.



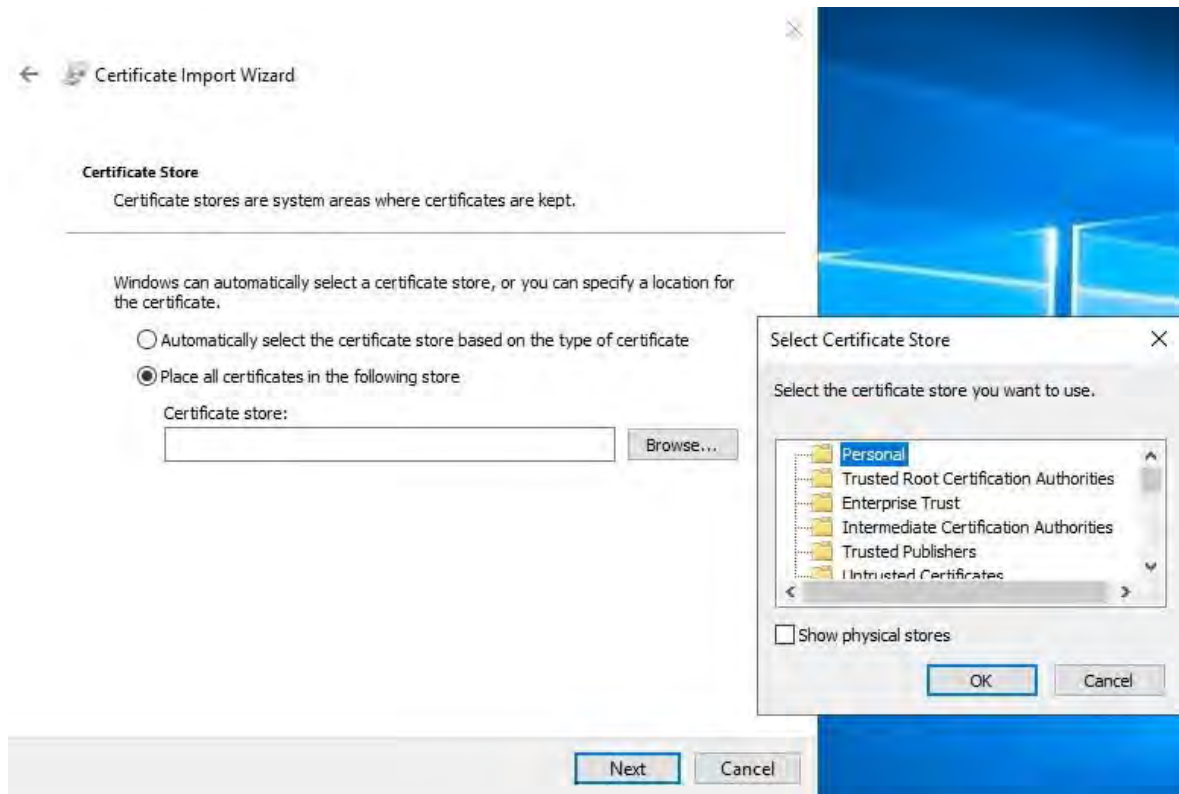
3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.

4. Wählen Sie diese Option aus, um das Zertifikat für den lokalen Computer zu installieren, und klicken Sie auf



Weiter.

5. Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf **Weiter**.



6. Beenden Sie den Assistenten zum Installieren von Zertifikaten.

15.3 Aktivieren der Verschlüsselung zum und vom Management-Server

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem zugehörigen Datensammler verschlüsseln, wenn Sie über einen Remoteserver des folgenden Typs verfügen:

- Aufzeichnungsserver
- Ereignisserver
- Protokollserver
- LPR-Server
- Mobiler Server

Wenn Ihr System über mehrere Aufzeichnungsserver oder Remote-Server verfügt, müssen Sie die Verschlüsselung auf allen Servern aktivieren.

15.3.1 Voraussetzungen:

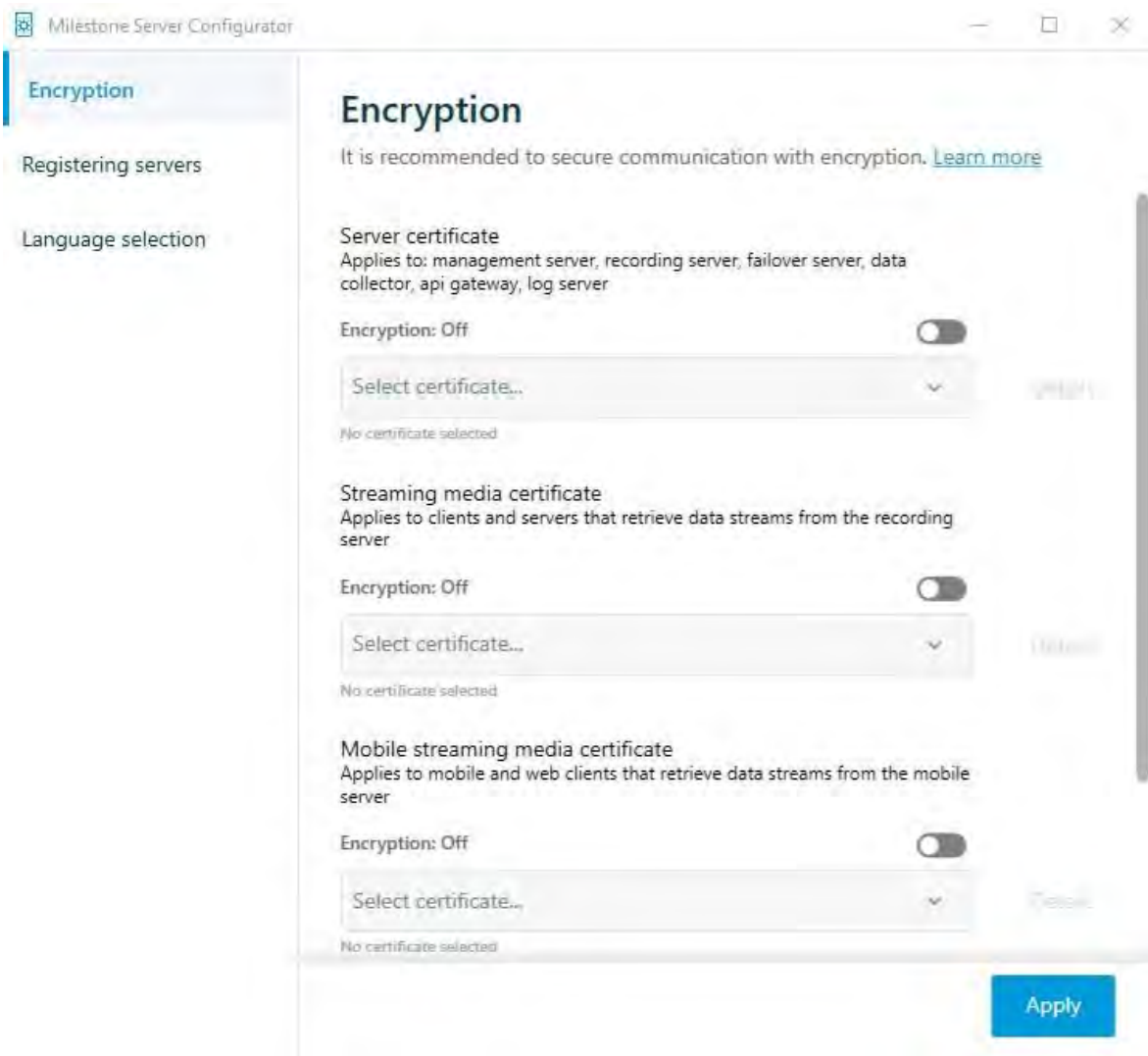


Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

Auf dem Computer, auf dem der Verwaltungsserver gehostet wird, ist ein Serverauthentifizierungszertifikat vertrauenswürdig. Aktivieren Sie zunächst die Verschlüsselung auf dem Verwaltungsserver.

Schritte:

7. Öffnen Sie auf einem Computer, auf dem ein Management-Server installiert ist, den **Server-Konfigurator** über:
 - Das Windows-Startmenü
oder
 - Den Management-Server-Manager, indem Sie mit der rechten Maustaste auf das Symbol Management-Server-Manager in der Taskleiste des Computers klicken.
1. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
2. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
3. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
4. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.



5. Klicken Sie auf Übernehmen.

Um die Aktivierung der Verschlüsselung abzuschließen, besteht der nächste Schritt darin, die Verschlüsselungseinstellungen auf jedem Aufzeichnungsserver und jedem Server mit einem Datensammler (Ereignisserver, Protokollserver, LPR-Server und mobiler Server) zu aktualisieren. Installieren von Active Directory-Zertifikatdiensten

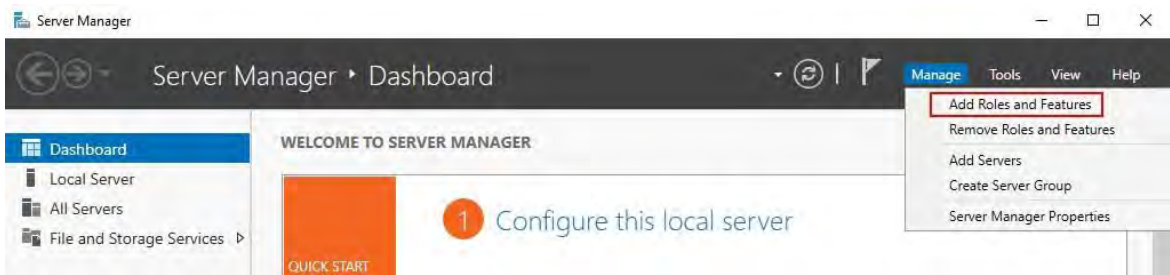
Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) sind ein Microsoft-Produkt, das PKI-Funktionen (Public Key Infrastructure) ausführt. Es fungiert als Serverrolle, die es Ihnen ermöglicht, eine Public Key-Infrastruktur (PKI) zu erstellen und Open-Key-Kryptografie, computergestützte Authentifizierung und erweiterte Markierungsfunktionen für Ihre Zuordnung bereitzustellen.

In diesem Dokument wird AD CS beim Installieren von Zertifikaten verwendet:

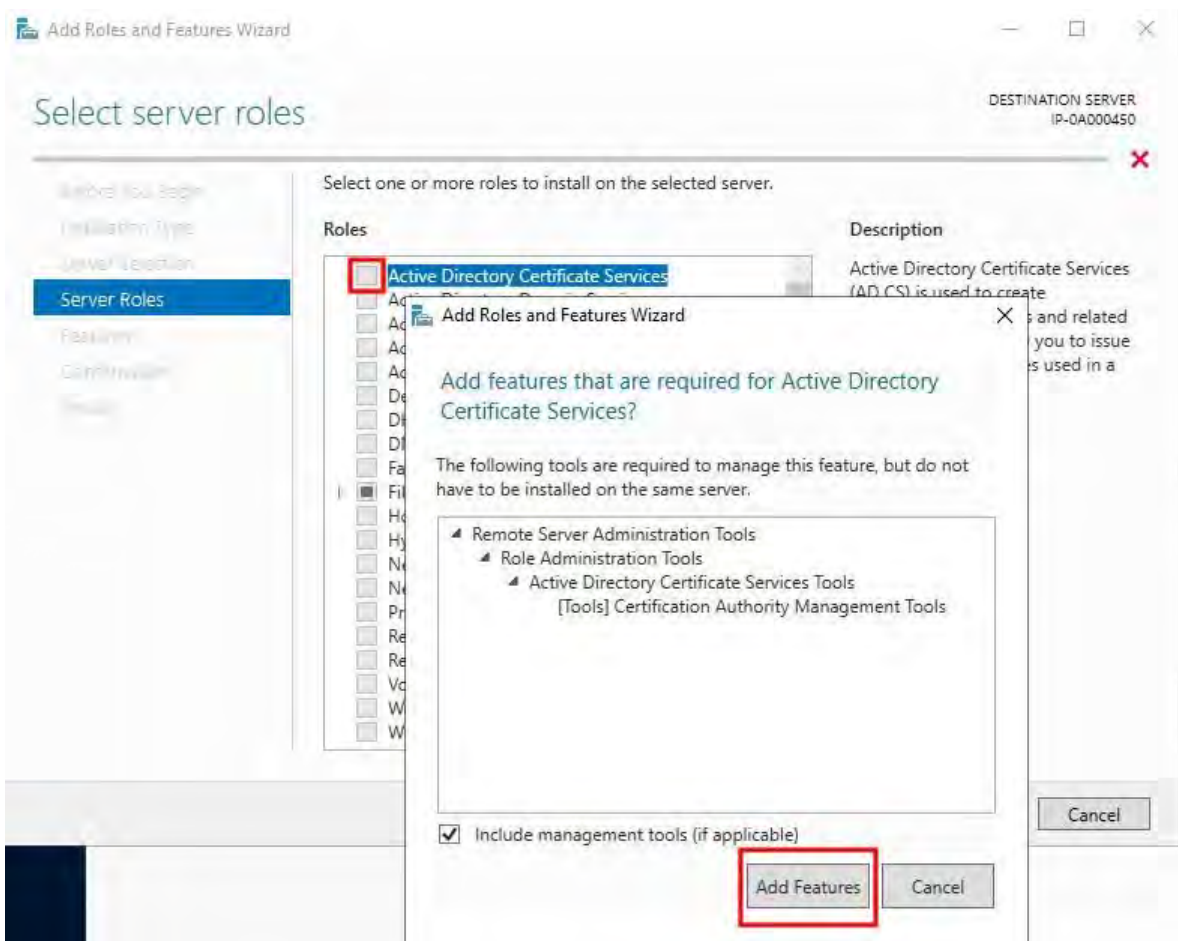
- In einer Domänenumgebung (siehe Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86)
- In einer Arbeitsgruppenumgebung (siehe Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104)

15.3.2 So installieren Sie AD CS:

1. Wählen Sie in der Server-Manager-Anwendung Verwalten > Rollen und Funktionen hinzufügen aus.



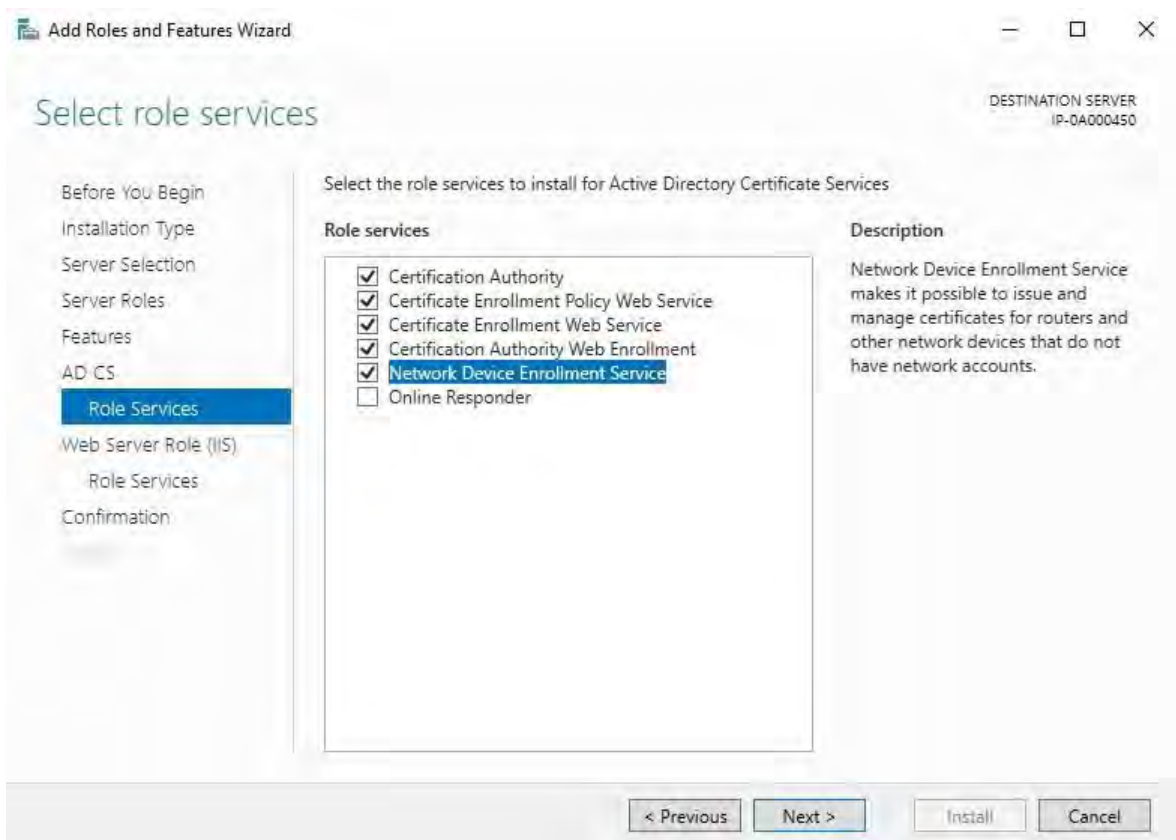
2. Klicken Sie unter Bevor Sie beginnen auf Weiter.
3. Wählen Sie unter Installationstyp die Option Rollenbasierte oder featurebasierte Installation aus, und klicken Sie auf Weiter.
4. Wählen Sie in der Serverauswahl den lokalen Server als Ziel für die Installation aus, und klicken Sie auf Weiter.
5. Wählen Sie unter Serverrollen die Rolle Active Directory-Zertifikatdienste aus. Überprüfen Sie die Liste der zu installierenden Funktionen, und klicken Sie auf Funktionen hinzufügen.



6. Klicken Sie auf **Weiter**.

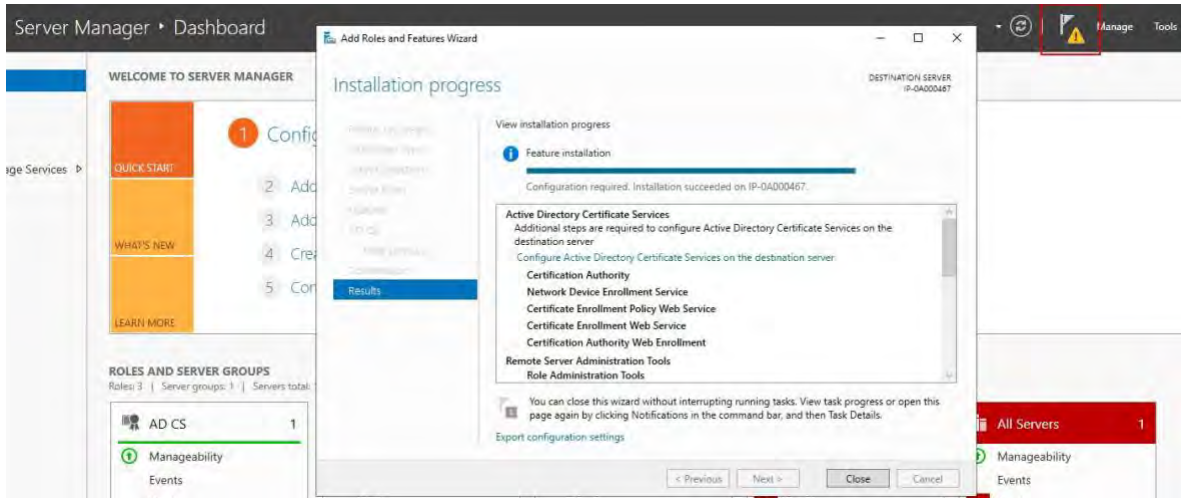
7. Klicken Sie **unter** Features auf **Weiter**. Alle erforderlichen Funktionen werden für die Installation ausgewählt.
8. Lesen Sie in **AD CS** die Beschreibung der Active Directory-Zertifikatdienste, und klicken Sie auf **Weiter**.
9. Wählen Sie unter Rollendienste Folgendes aus:
 - Zertifizierungsstelle
 - Webdienst für die Zertifizierungsregistrierungsrichtlinie
 - Webdienst für die Zertifizierungsregistrierung
 - Webregistrierung der Zertifizierungsstelle
 - Registrierungsdienst für Netzwerkgeräte

Fügen Sie bei der Auswahl der einzelnen Rollendienste die erforderlichen Features hinzu, um die Installation der einzelnen Dienste zu unterstützen .

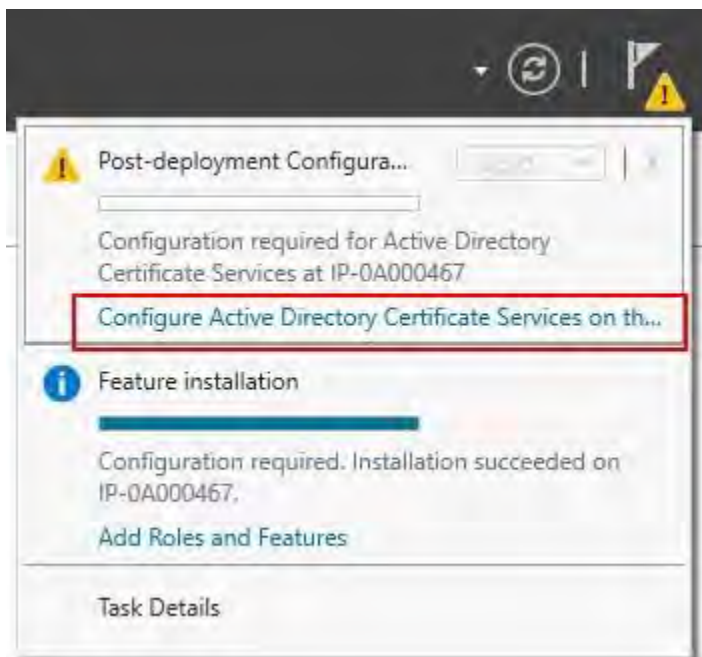


10. Klicken Sie auf **Weiter**.
11. Wählen Sie unter **Bestätigung** die Option **Zielservers bei Bedarf automatisch neu starten aus**, und klicken Sie auf **Installieren**.

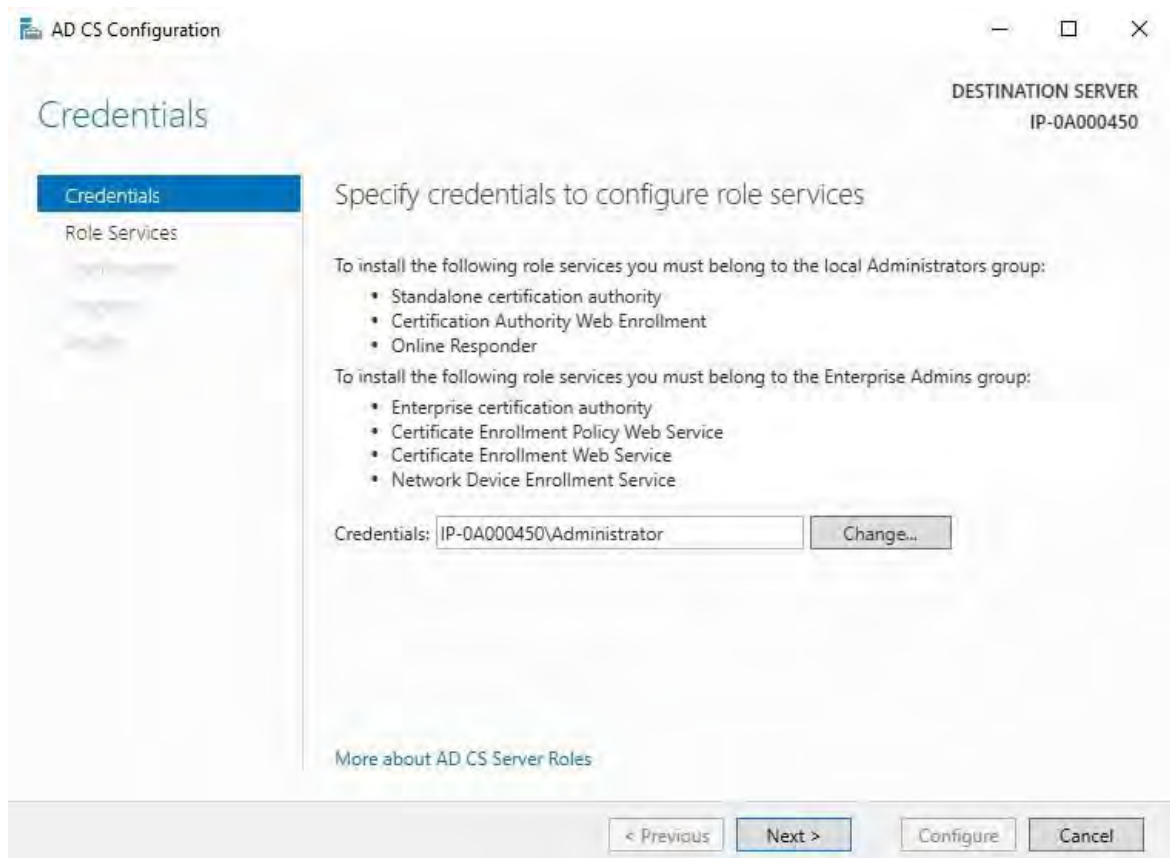
12. Wenn die Installation abgeschlossen ist, klicken Sie auf die **Schaltfläche Schließen**.
13. Wählen Sie das Benachrichtigungsflag in der Server-Manager-Anwendung aus.



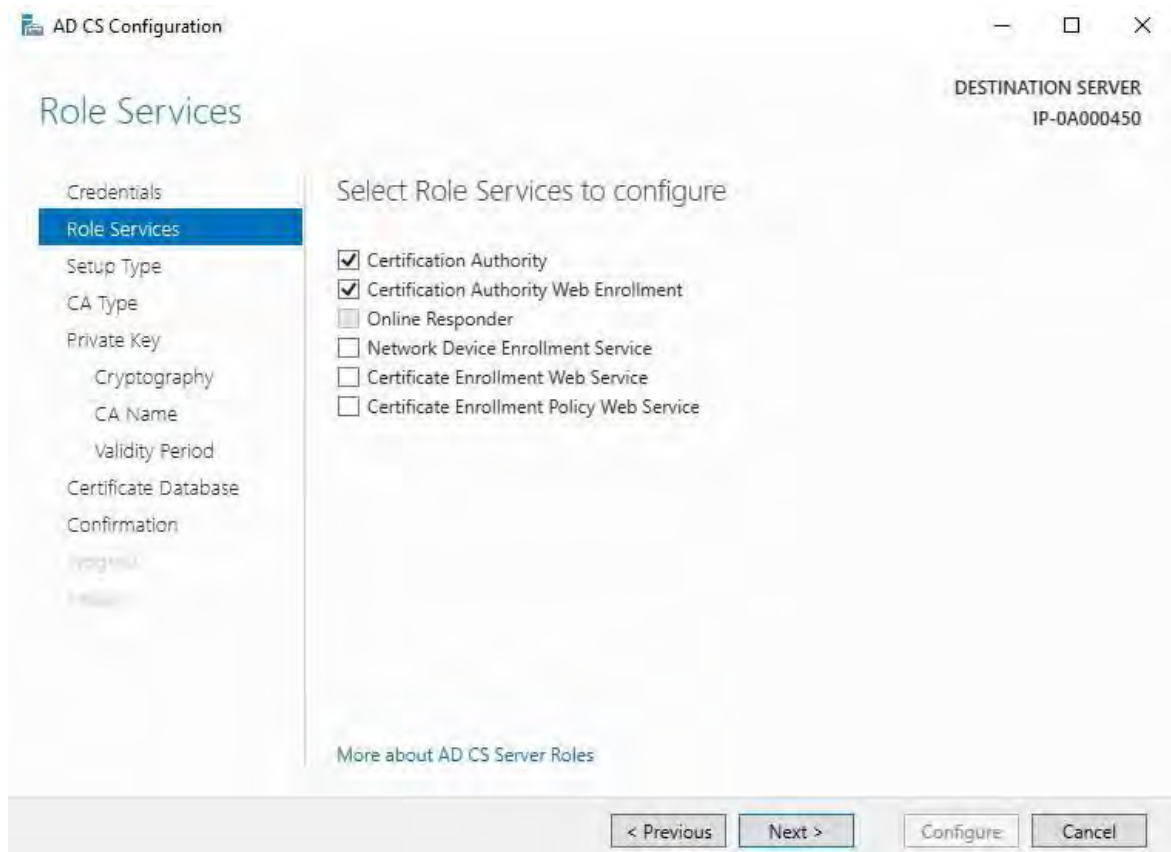
14. Eine Meldung, dass die Konfiguration nach der Bereitstellung gestartet werden soll, wird unter dem **Benachrichtigungsflag** aufgeführt.
15. Klicken Sie auf den Link, um mit der Konfiguration der installierten Dienste zu beginnen.



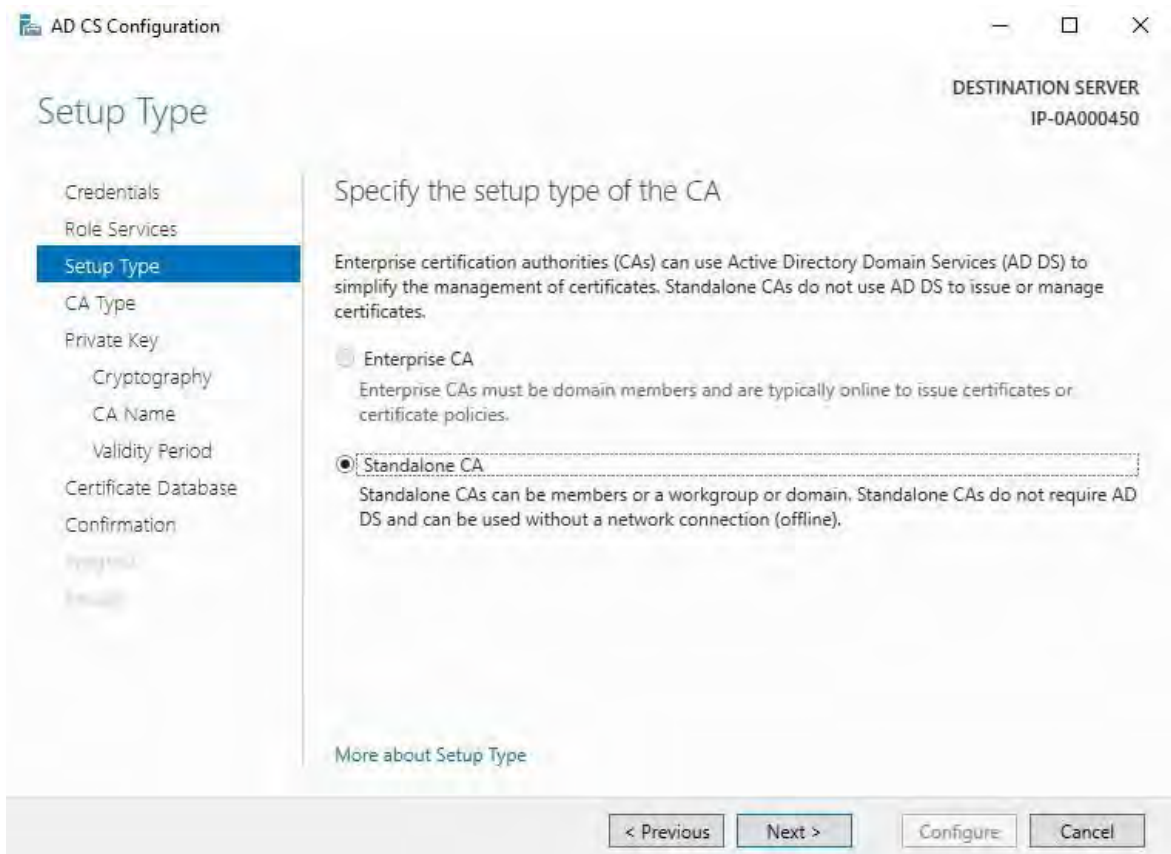
16. Der Konfigurationsassistent für Active Directory-Zertifikatdienste wird gestartet.
17. Wählen Sie unter **Anmeldeinformationen** das Benutzerkonto aus, das zum Ausführen der installierten Dienste erforderlich ist. Wie im Text angegeben, ist die Mitgliedschaft in den Gruppen "Lokaler Administrator" und "Unternehmensadministrator" erforderlich.
18. Geben Sie die erforderlichen Kontoinformationen ein und klicken Sie auf **Weiter**.



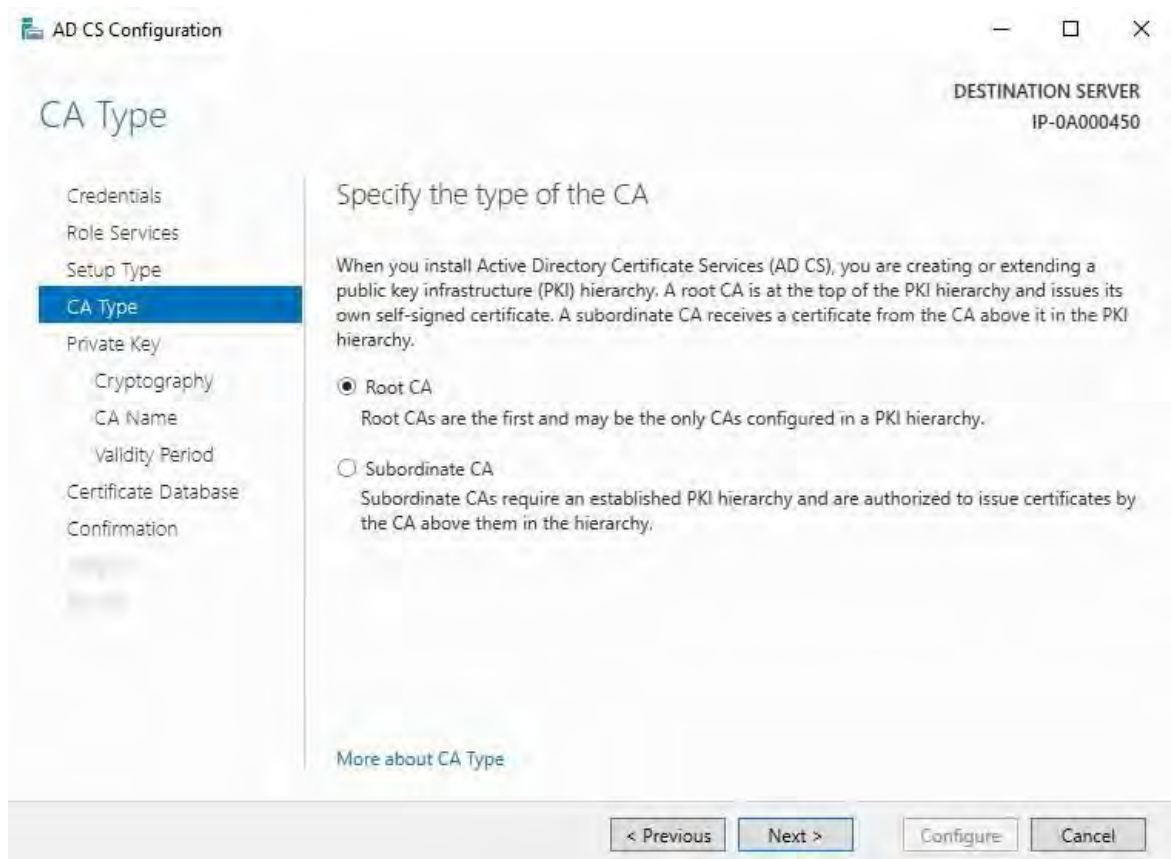
19. **Wählen Sie** unter Rollendienste die folgenden Dienste aus:
 - Zertifizierungsstelle
 - **Webregistrierung der Zertifizierungsstelle**
20. Klicken Sie auf **Weiter**.



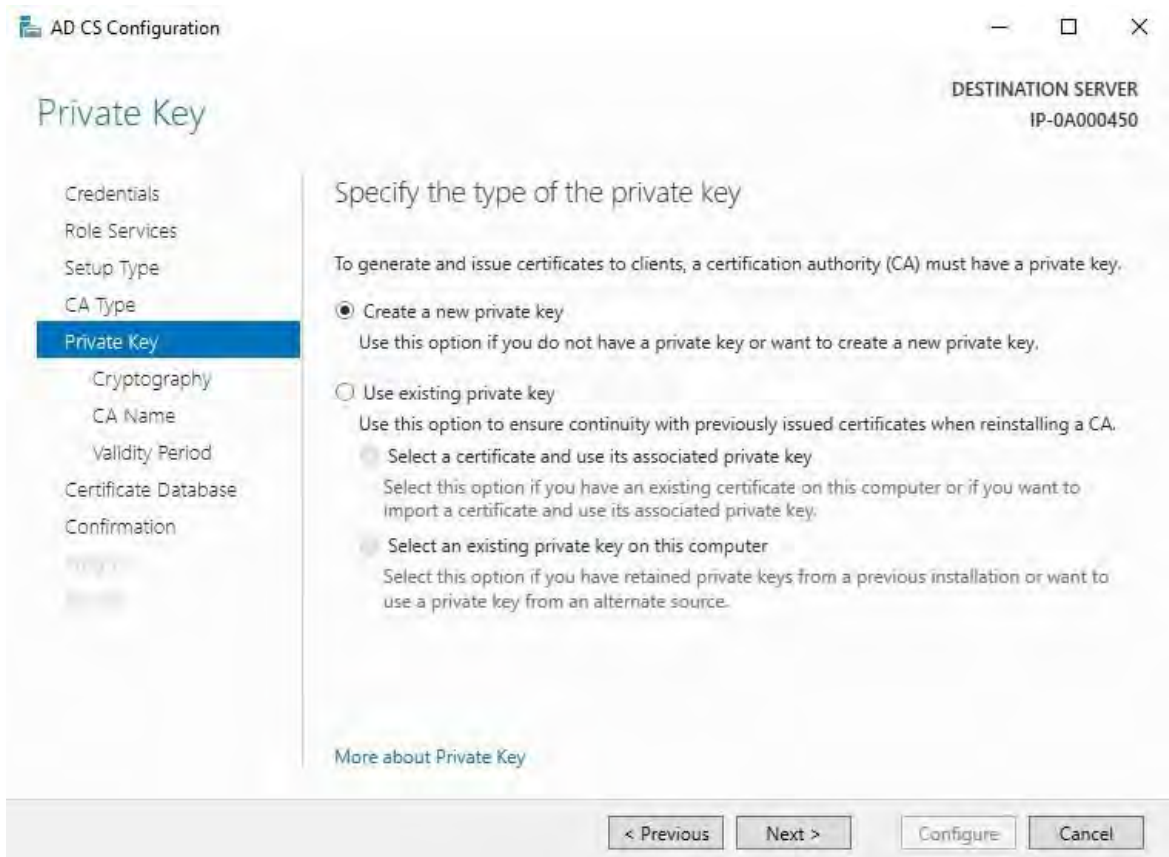
21. Wählen Sie **unter** Setup-Typ die Option **Eigenständige Zertifizierungsstelle** aus und klicken Sie auf **Weiter**.



22. Wählen Sie unter **CA-Typ** die Option zum Installieren einer **Root-CA aus**, und klicken Sie auf **Weiter**.

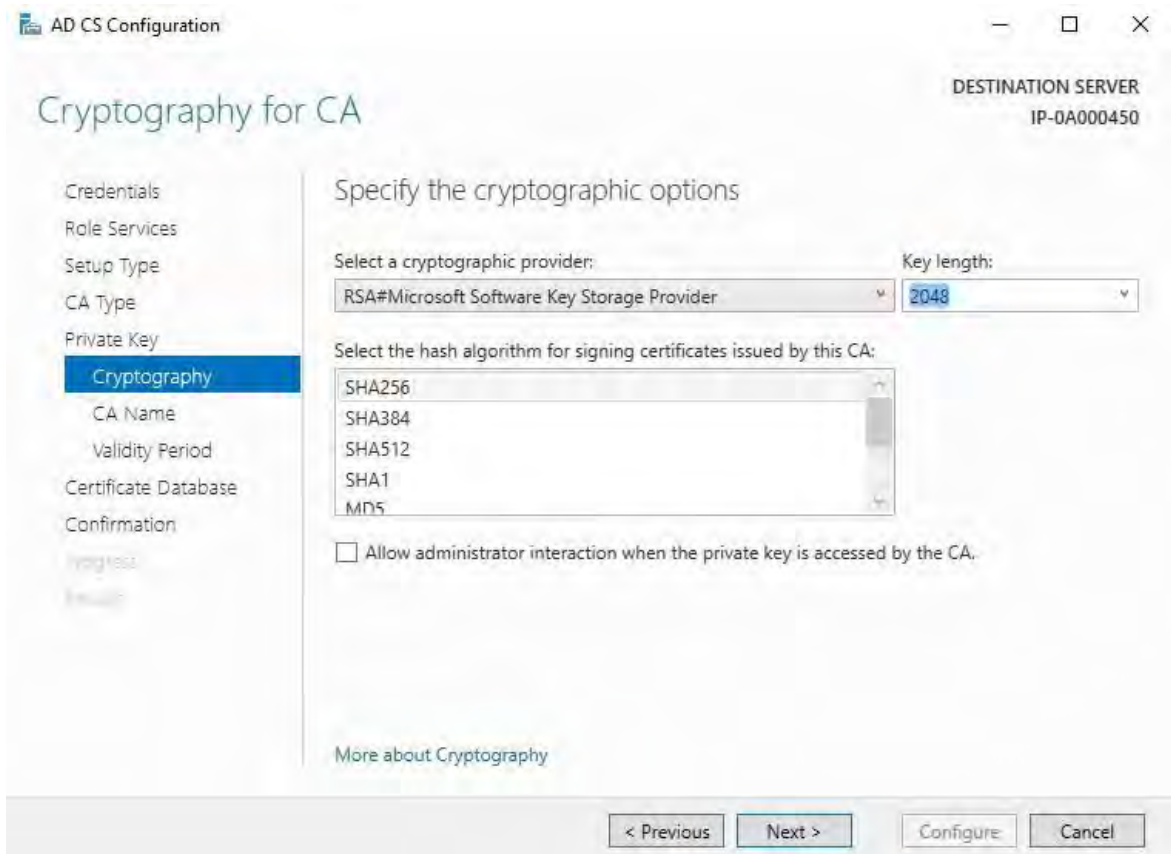


23. In **Privater Schlüssel**, wählen Sie die Option zum Erstellen eines neuen privaten Schlüssels aus, und klicken Sie auf **Weiter**.



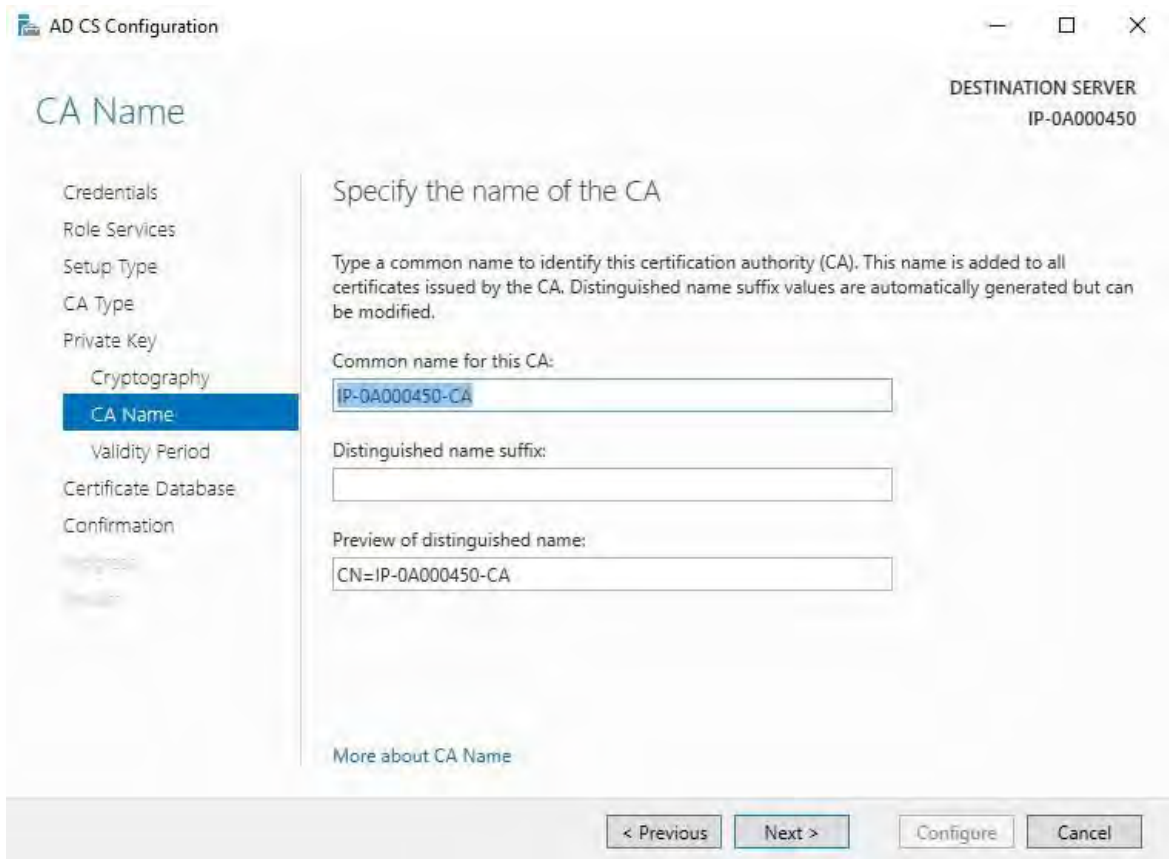
24. Wählen Sie unter **Kryptografie** die Option **RSA#Microsoft Software Key Storage Provider** für die Option Kryptografieanbieter mit einer **Schlüssellänge** von 2048 und einem Hashalgorithmus von SHA256 aus.

Klicken Sie auf **Weiter**.

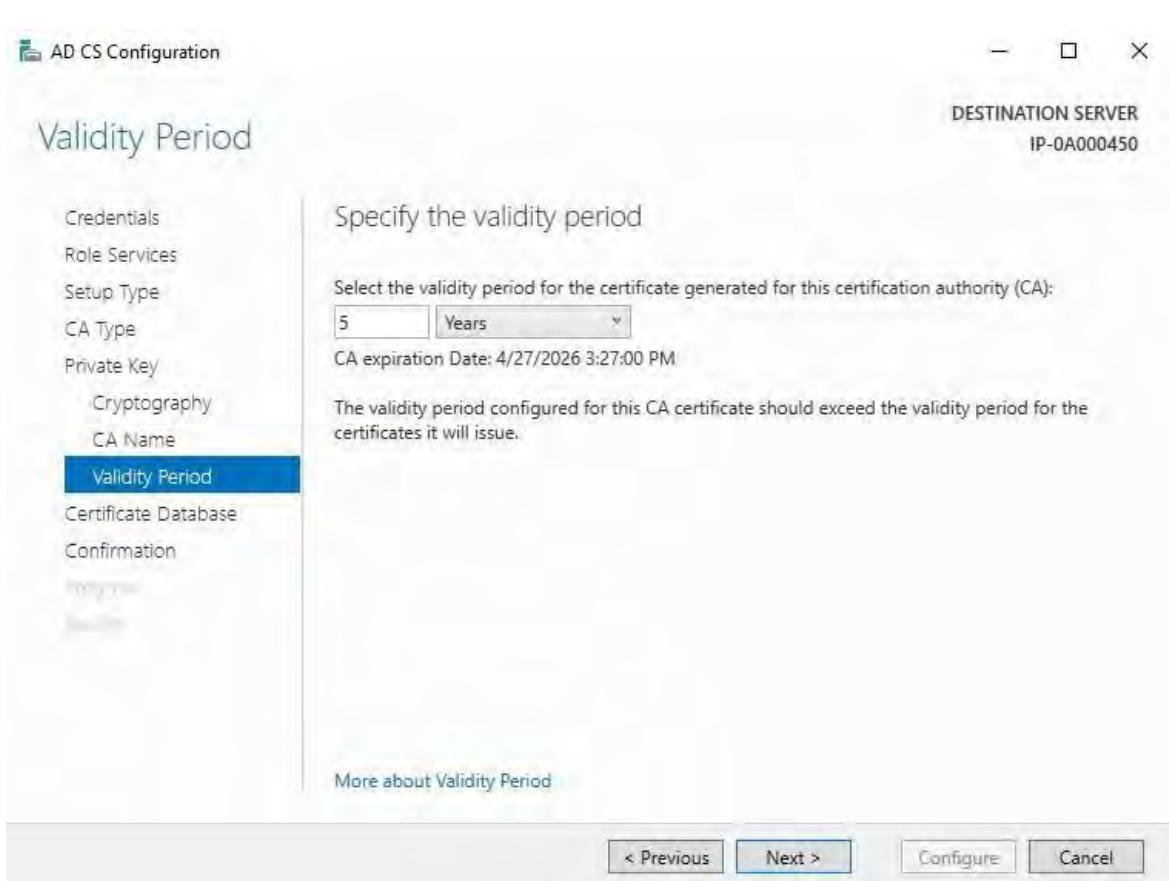


25. Geben Sie unter **Name** der Zertifizierungsstelle den Namen für die Zertifizierungsstelle ein, und klicken Sie auf **Weiter**.

Standardmäßig lautet der Name "localhost-CA" - unter der Annahme, dass der Computername des lokalen Servers "localhost" lautet.



26. Wählen Sie unter **Gültigkeitszeitraum** die Standardgültigkeitsdauer von 5 Jahren aus und klicken Sie auf **Weiter**.



27. Geben Sie unter **Zertifikatdatenbank** die Speicherorte der Datenbank und der Protokolldatenbank ein.
Die Standarddatenbankspeicherorte für den Zertifikatspeicher sind: C:\Windows\system32\CertLog
28. Klicken Sie auf **Weiter**.
29. **Überprüfen Sie unter Bestätigung die ausgewählten Konfigurationsoptionen und klicken Sie auf Konfigurieren, um den Konfigurationsprozess zu starten.**
30. Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Schließen**.
31. Wenn Sie aufgefordert werden, zusätzliche Rollendienste zu konfigurieren, klicken Sie auf **Nein**.
32. Starten Sie den lokalen Server neu, um sicherzustellen, dass er bereit ist, als Active Directory-Zertifikatsserver zu dienen.

15.4 Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver

Wenn Client- und Serverendpunkte alle in einer Domänenumgebung ausgeführt werden, ist es nicht erforderlich, CA-Zertifikate an Client-Arbeitsstationen zu verteilen. Die Gruppenrichtlinie innerhalb der Domäne verarbeitet die automatische Verteilung aller Zertifikate der vertrauenswürdigen Zertifizierungsstelle an alle Benutzer und Computer in der Domäne.

Dies liegt daran, dass bei der Installation einer Unternehmensstammzertifizierungsstelle Gruppenrichtlinien verwendet werden, um das Zertifikat für alle Benutzer und Computer in der Domäne an den Zertifikatspeicher der vertrauenswürdigen Stammzertifizierungsstellen weiterzugeben.

Sie müssen ein Domänenadministrator oder ein Administrator mit Schreibzugriff auf Active Directory sein, um eine Unternehmensstammzertifizierungsstelle installieren zu können.

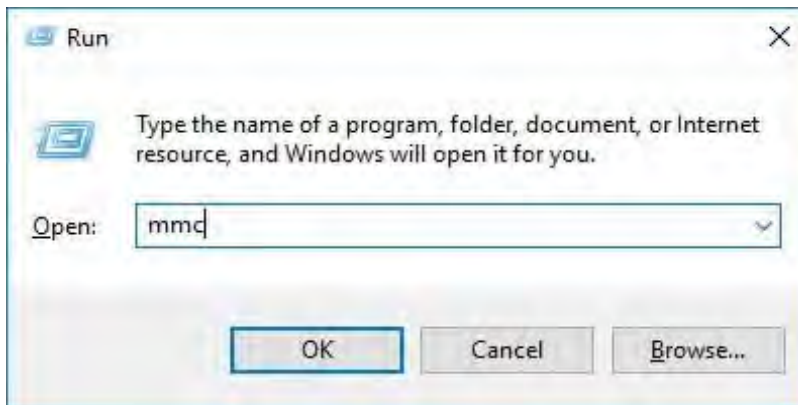


Microsoft stellt eine umfangreiche Dokumentation für Windows Server-Betriebssysteme bereit, die Vorlagen für Serverzertifikate, die Installation der Zertifizierungsstelle und die Zertifikatbereitstellung enthält, die in der Übersicht über die Bereitstellung von

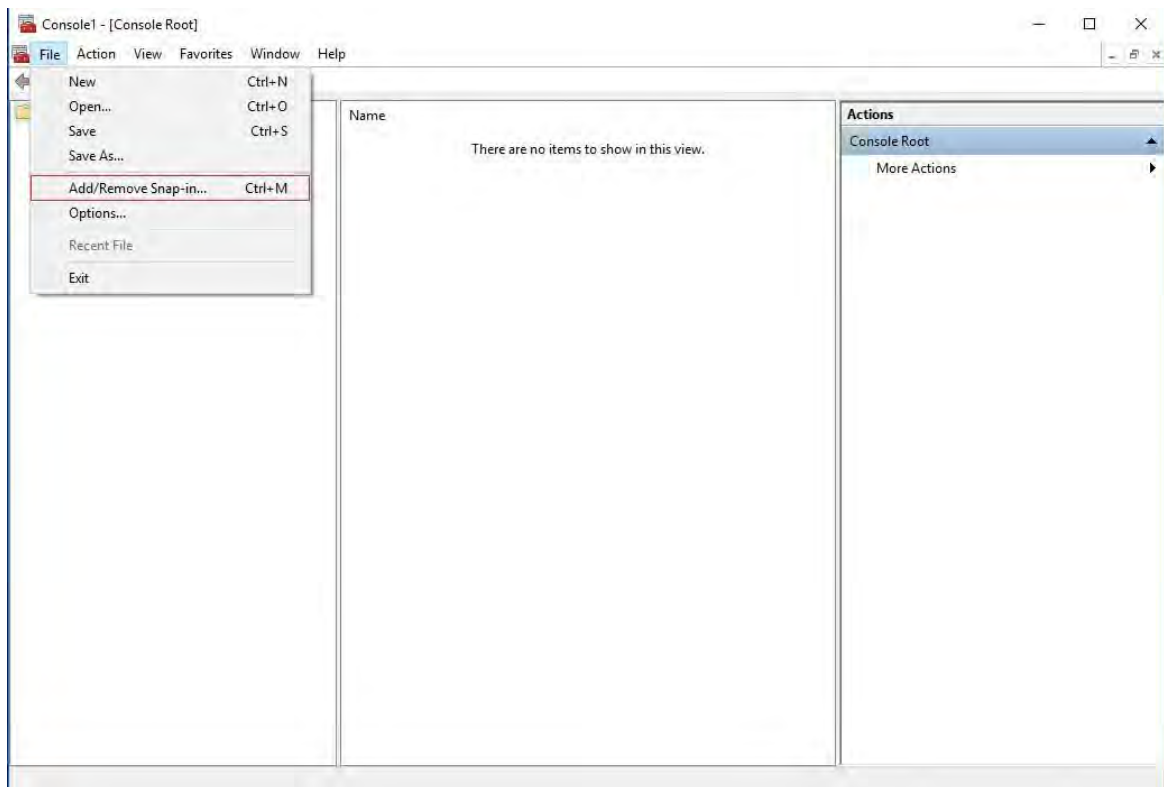
15.4.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen.

1. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.

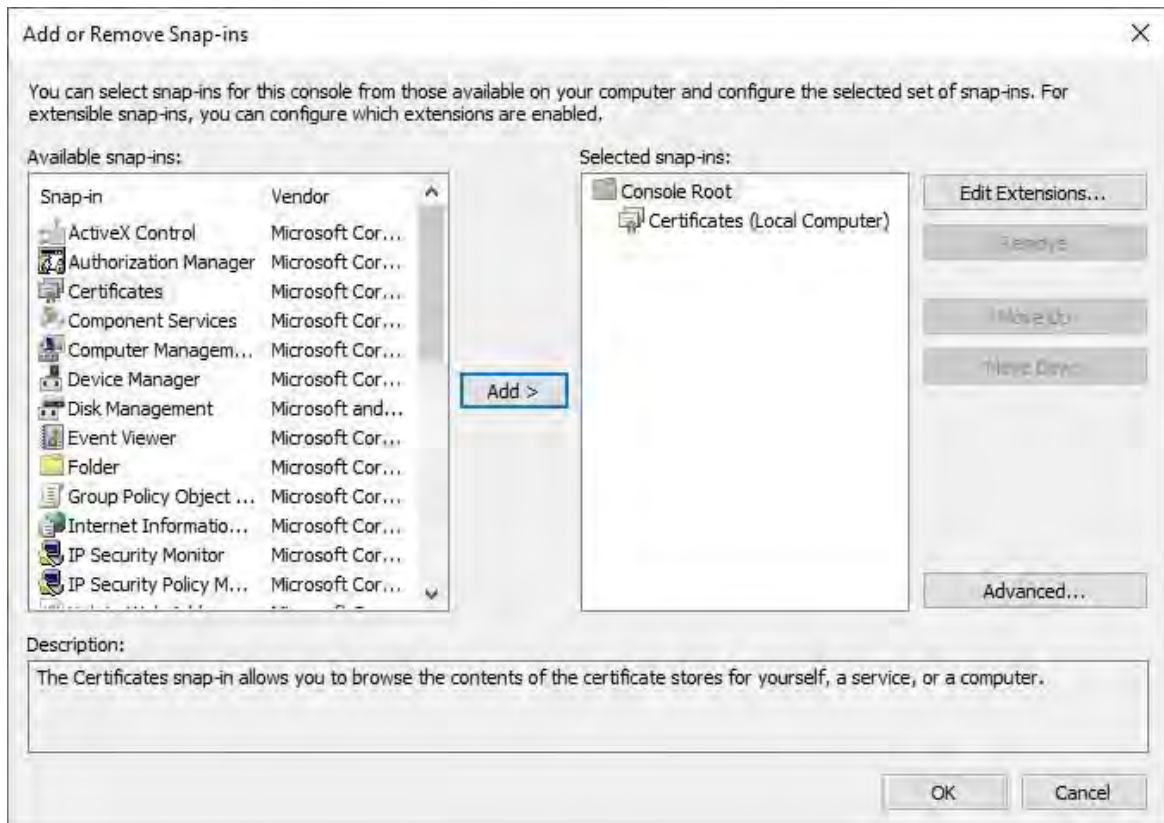


2. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In**

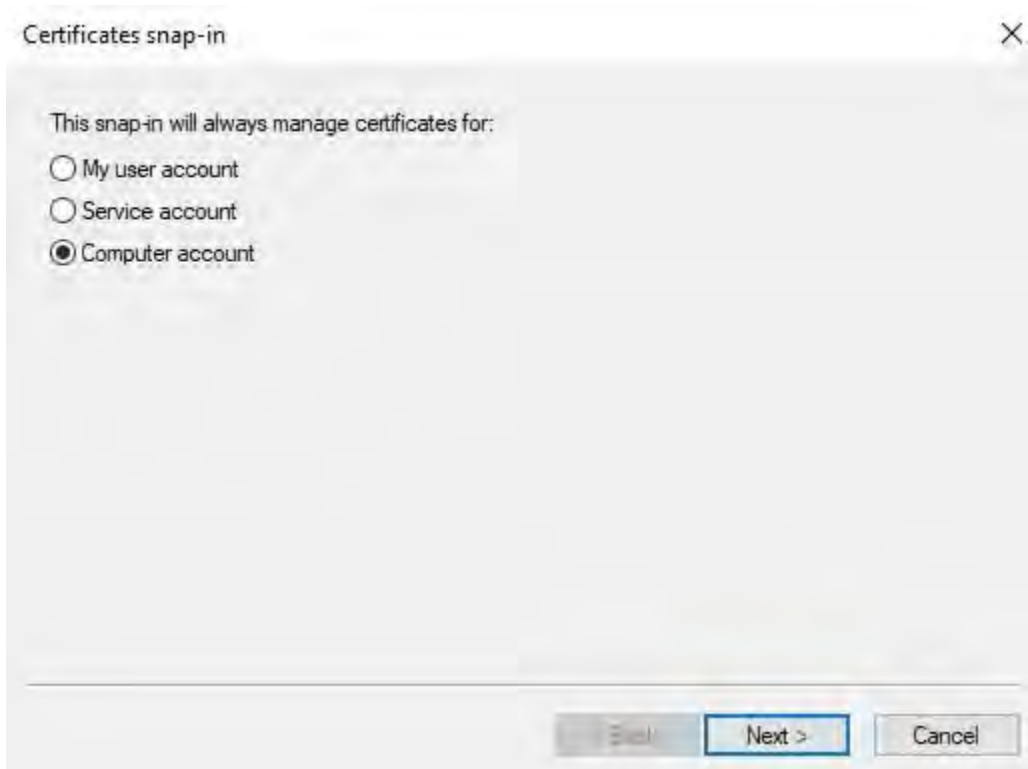


hinzufügen/entfernen....

3. Wählen Sie das Zertifikat-Snap-In aus, klicken Sie auf Zertifikat-Snap-In hinzufügen, und wählen Sie

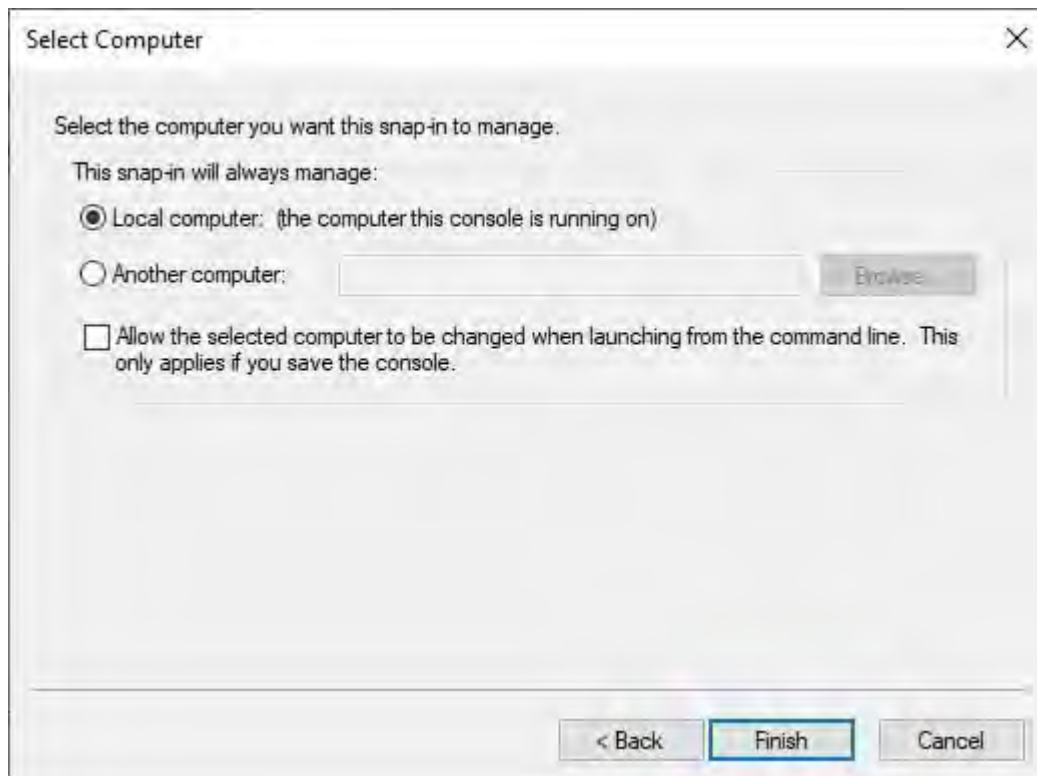


Computerkonto aus.




4. Wählen Sie unter Computer auswählen die Option Lokaler Computer aus.

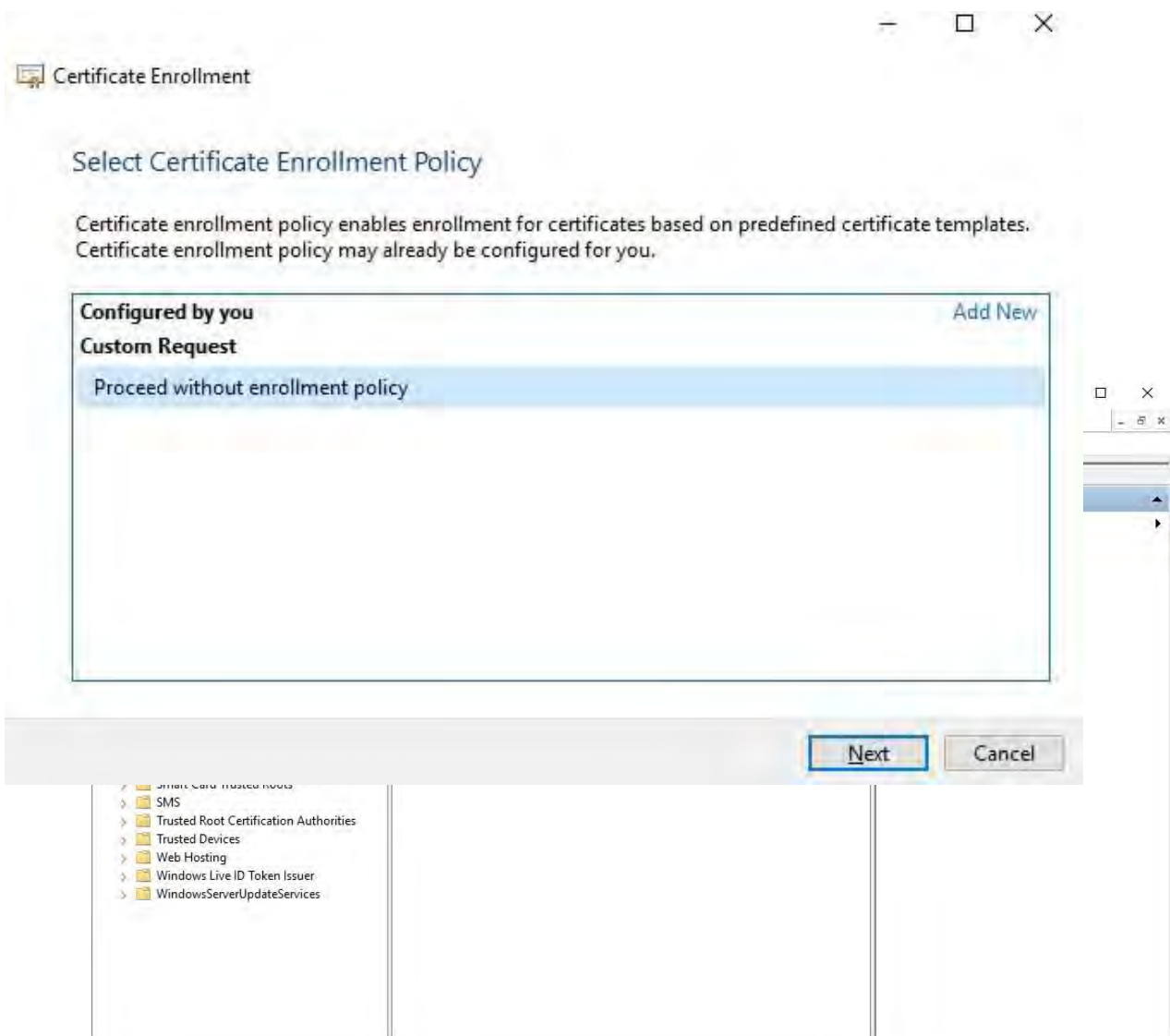
5. Wählen Sie **Fertig stellen** und dann **OK aus**.



- Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den **Ordner Persönlich** und wählen Sie **Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen**.
- Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.

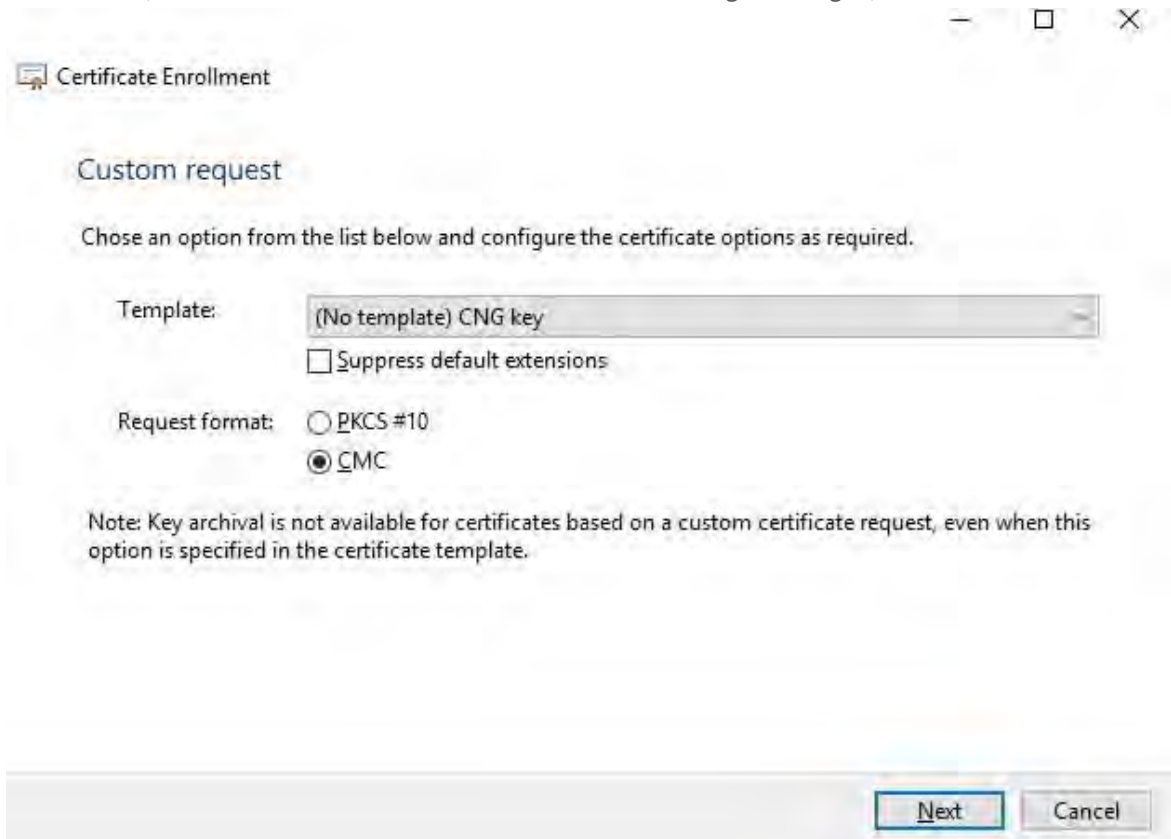
 Wenn Ihre Gruppenrichtlinie bereits eine Zertifikatregistrierungsrichtlinie enthält, sollten Sie den Rest dieses Vorgangs mit Ihrem Domänenverwaltungsteam bestätigen, bevor Sie fortfahren.

- Klicken Sie auf **Weiter**.
- Wählen Sie die Vorlage **CNG-Schlüssel (keine Vorlage)** und das **CMC-Anforderungsformat** aus und



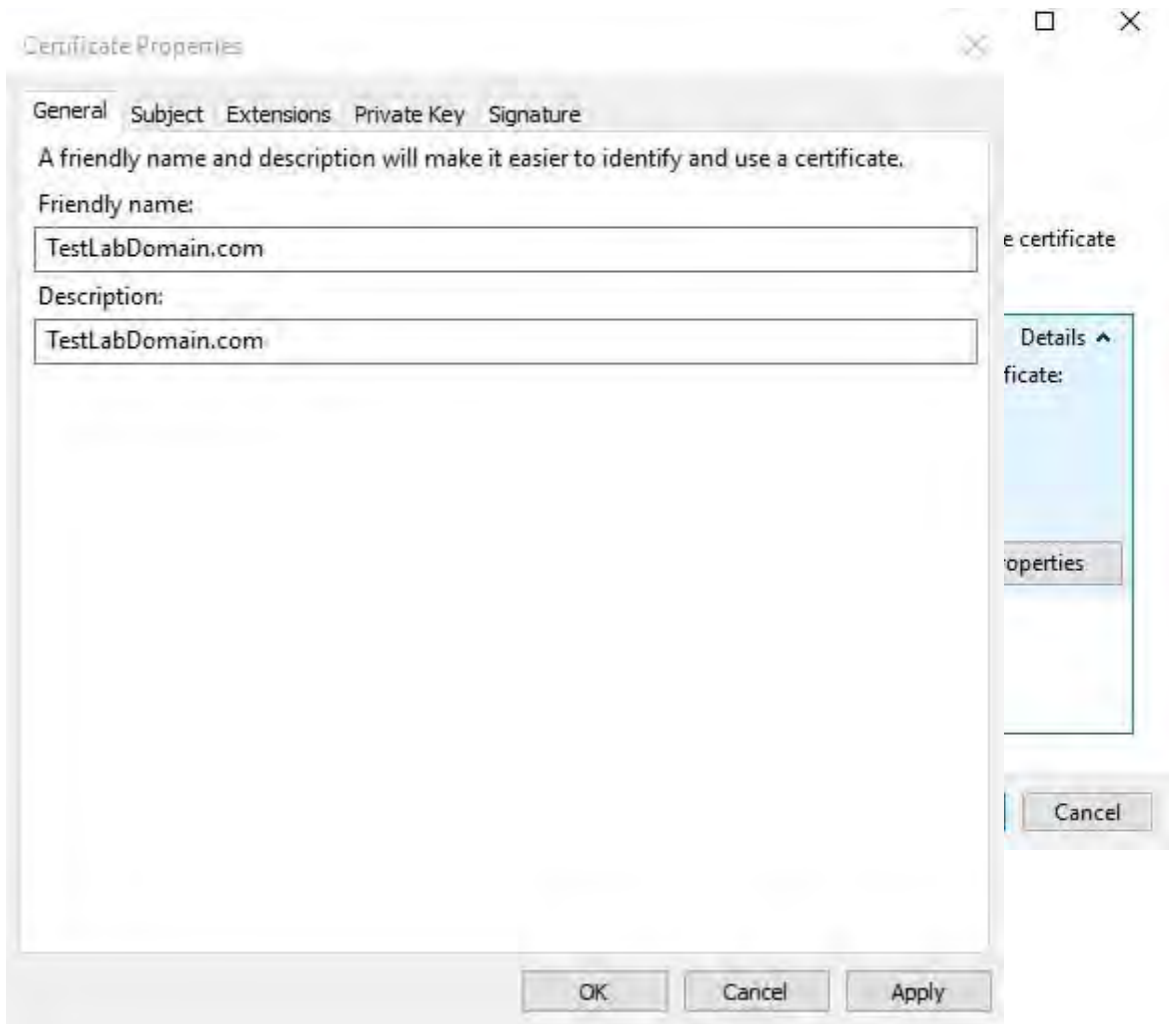
klicken Sie auf **Weiter**.

10. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf



Eigenschaften.

- 11. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domännennamen, dem Computernamen oder der Organisation aus.

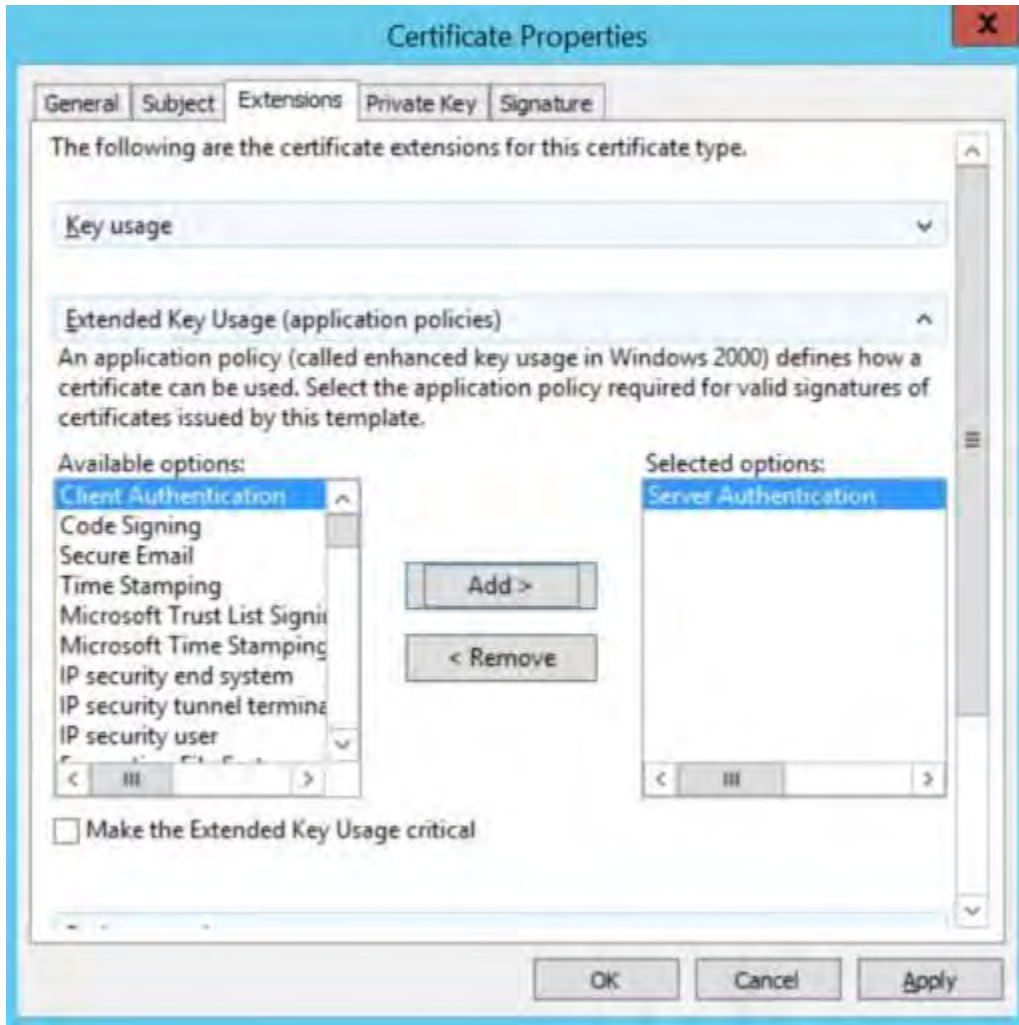


- 12. Geben Sie auf der **Registerkarte Betreff** die erforderlichen Parameter für den Antragstellernamen ein. Geben Sie unter **Antragstellername Typ** unter **Allgemeiner Name** den Hostnamen des Computers ein, auf dem das Zertifikat installiert werden soll.

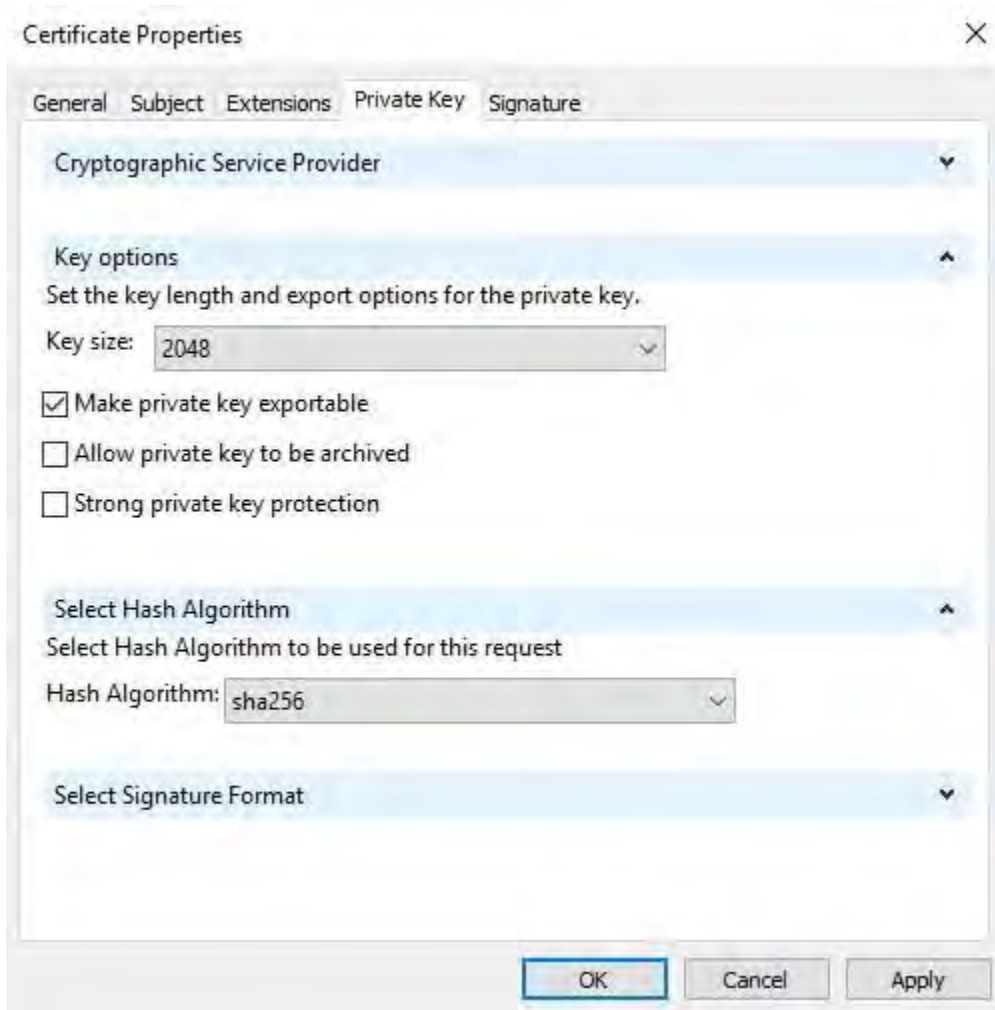
- 13. Erweitern Sie auf der Registerkarte Erweiterungen das Menü Erweiterte Schlüsselverwendung (Anwendungsrichtlinien). Fügen Sie die Serverauthentifizierung aus der Liste der verfügbaren Optionen



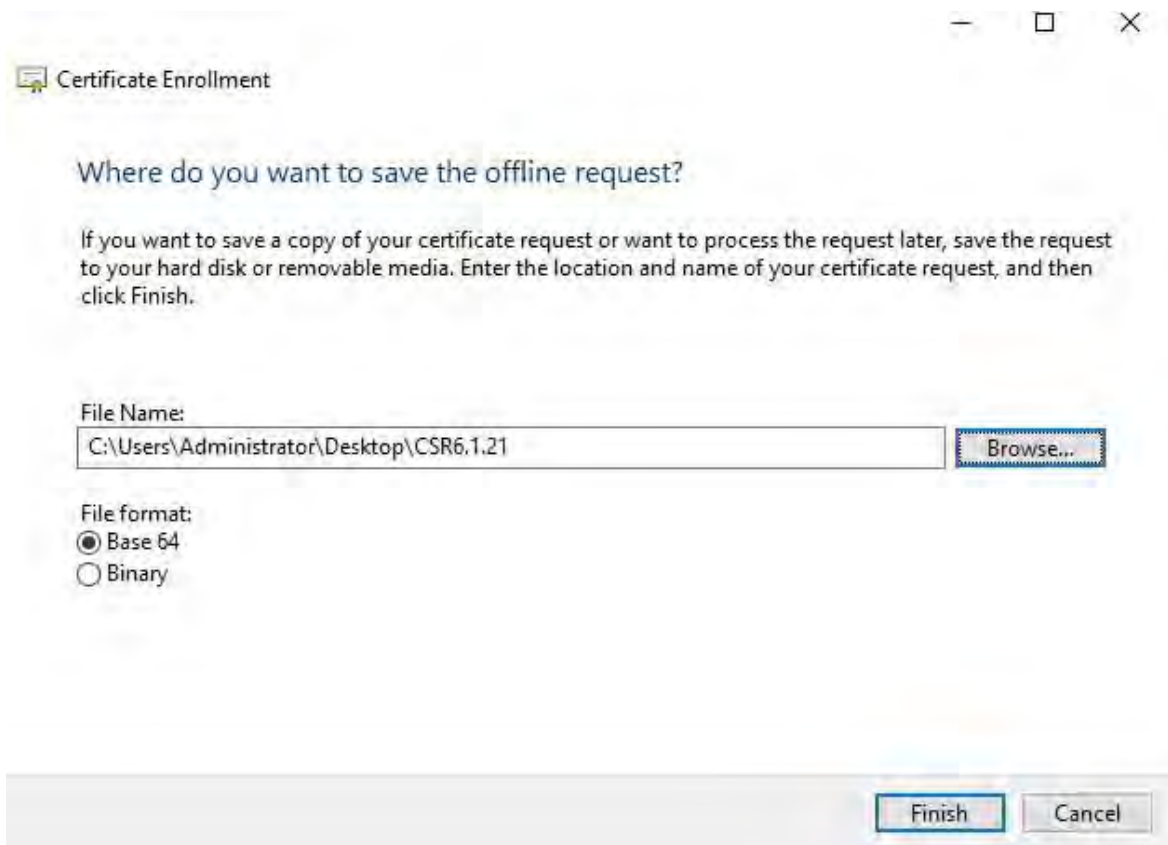
hinzu.



14. Erweitern Sie **auf der Registerkarte Privater Schlüssel** das Menü **Schlüsseloptionen**.
15. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen. Klicken Sie auf **OK**.



16. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **im Zertifikatregistrierungs-Assistenten** auf Weiter.
17. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist die Basis 64.
18. Klicken Sie auf **Fertig stellen**.



Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

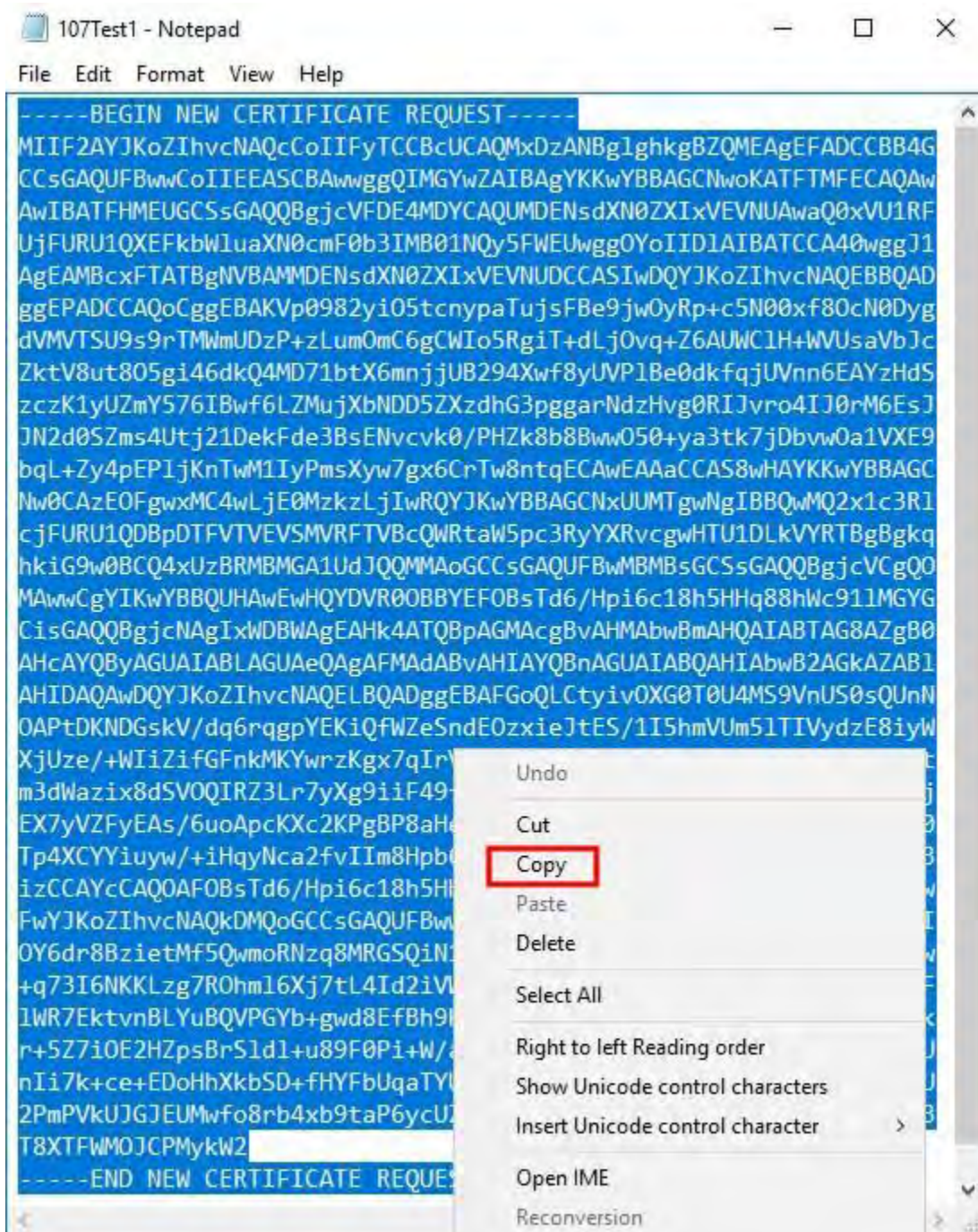
15.4.2 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Sie müssen den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, kopieren und den Text in die interne Zertifizierungsstelle der Active Directory-Zertifikatdienste im Netzwerk einfügen. Weitere Informationen finden Sie unter [Installieren von Active Directory-Zertifikatdiensten auf Seite 74](#).

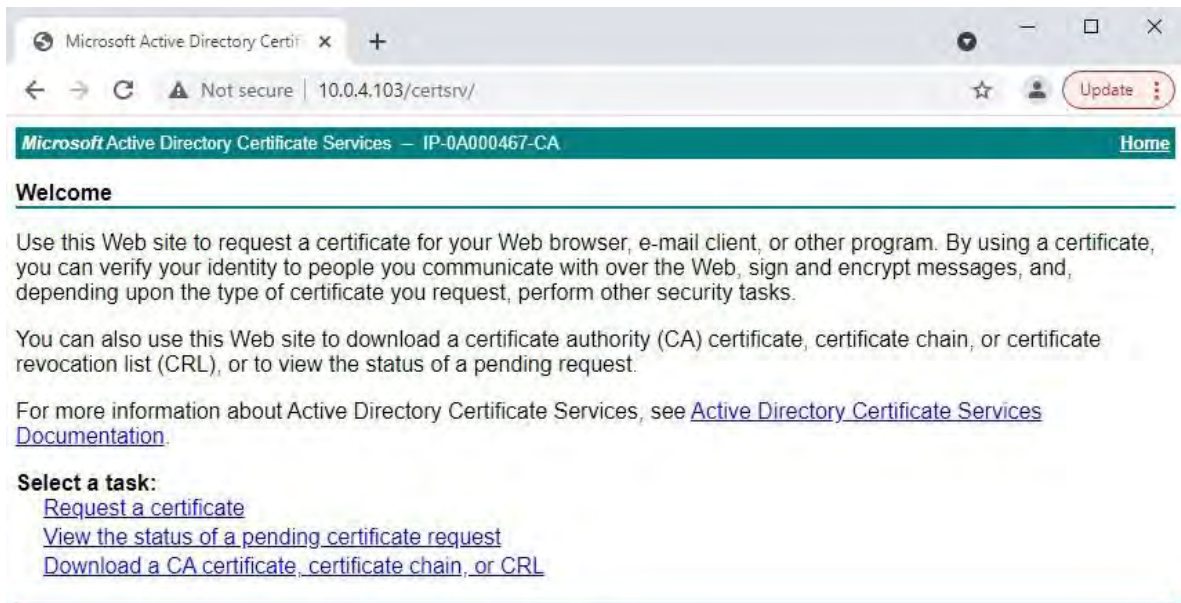


Sofern in Ihrer Domäne die Active Directory-Zertifikatdienste nicht erst kürzlich installiert wurden oder nur zu diesem Zweck installiert wurde, müssen Sie diese Anforderung nach einem separaten Verfahren senden, das von Ihrem Domänenverwaltungsteam konfiguriert wurde. Bitte bestätigen Sie diesen Vorgang mit ihnen, bevor Sie fortfahren.

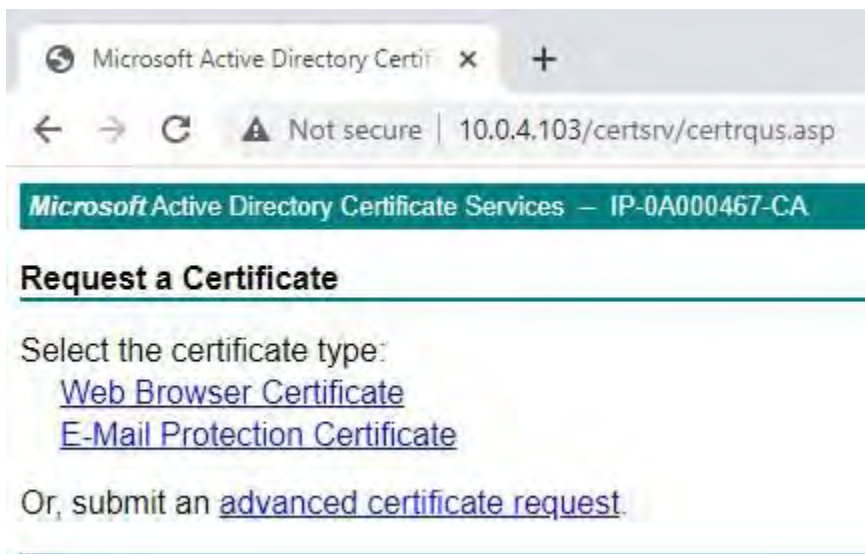
1. Navigieren Sie zum Speicherort der REQ-Datei, und öffnen Sie sie im Editor.



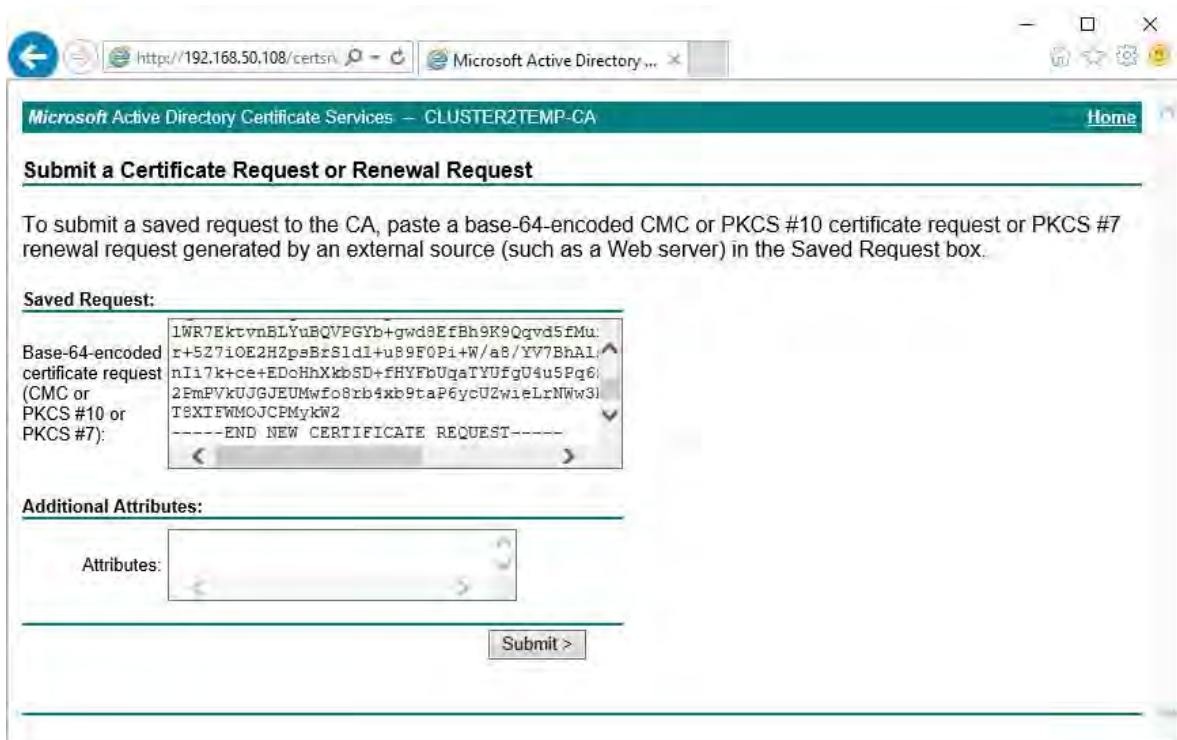
2. Kopieren Sie den gesamten Inhalt der Datei. Dazu gehören auch die gestrichelten Linien, die den Anfang und das Ende der Zertifikatsanforderung markieren.
3. Öffnen Sie einen Webbrowser und geben Sie die Adresse der Domänenzertifizierungsstelle ein.



- 4. Klicken Sie auf den Link Zertifikat anfordern.
- 5. Klicken Sie auf den Link für die Anforderung eines erweiterten Zertifikats.



- 6. Fügen Sie den Inhalt der .req-Datei in das Formular ein. Wenn es erforderlich ist, eine Zertifikatvorlage auszuwählen, wählen Sie **Webserver** aus der Liste Zertifikatvorlage.



7. Klicken Sie auf **Senden**.

Auf der Website wird eine Meldung angezeigt, dass das Zertifikat in einigen Tagen ausgestellt wird.

Ihr Domänenverwaltungsteam wird das Zertifikat wahrscheinlich für Sie verteilen und installieren. Wenn Ihnen das Zertifikat jedoch zugestellt wird, können Sie es manuell installieren.

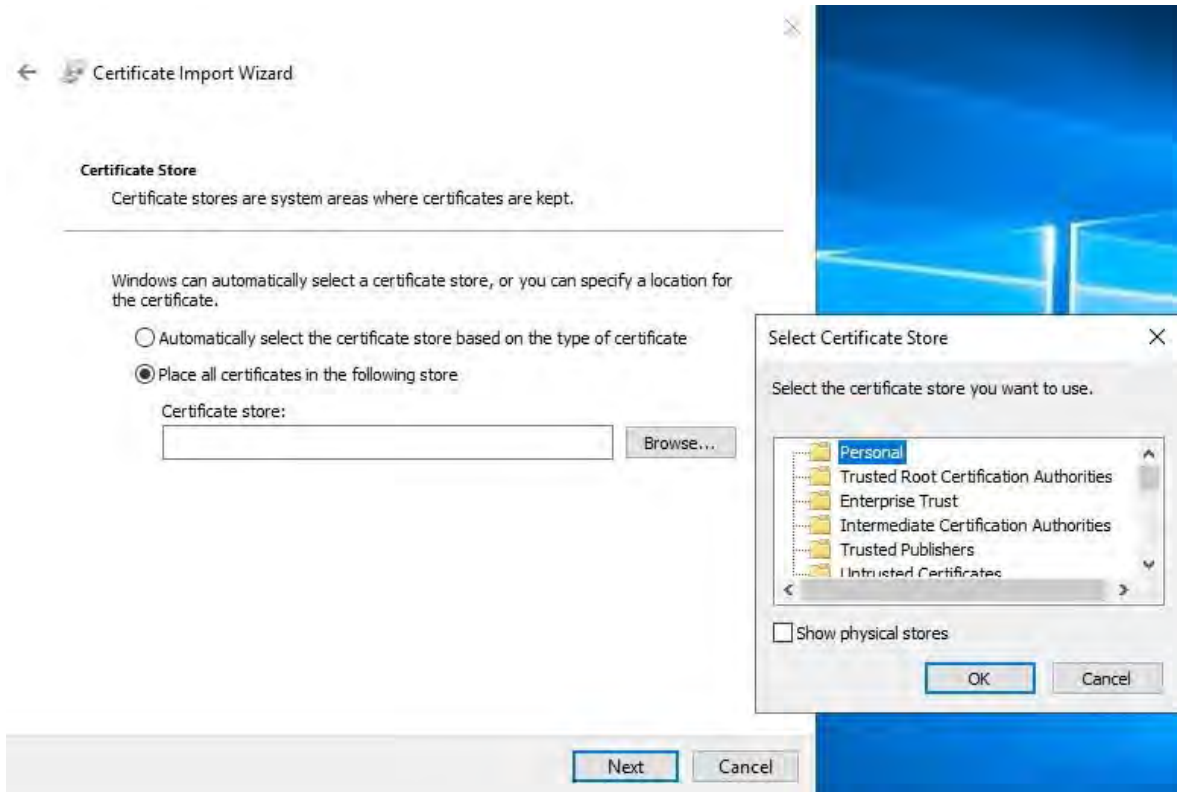
15.5 Manuelles Installieren des Zertifikats

Wenn Ihnen das Zertifikat zugestellt wird, können Sie es manuell installieren.

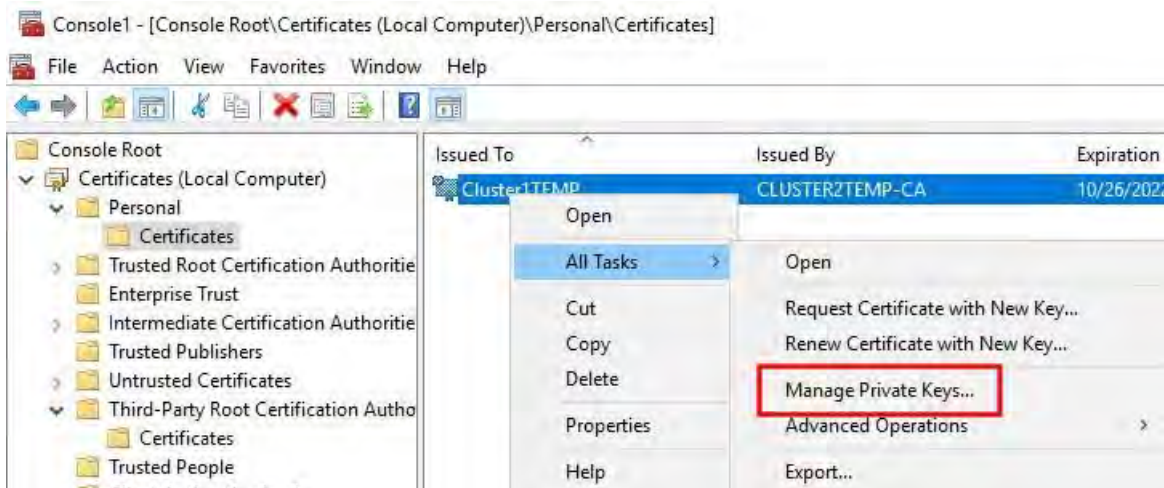
1. Suchen Sie die Zertifikatsdatei auf dem Computer, auf dem der Management-Server oder der Aufzeichnungsserver gehostet wird.
2. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie Zertifikat installieren aus.
3. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.
4. Wählen Sie aus, um das Zertifikat für den aktuellen Benutzer zu installieren, und klicken Sie auf Weiter.

Wählen Sie einen Speicherort aus, navigieren Sie zum Speicher für persönliche Zertifikate, und klicken Sie auf **Weiter**.





5. Beenden Sie den Assistenten zum Installieren von Zertifikaten.
6. Wechseln Sie zum Zertifikat-Snap-In der Microsoft Management Console (MMC).
7. Navigieren Sie in der Konsole zum persönlichen Speicher, in dem das Zertifikat installiert ist. Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie Alle Aufgaben > Private Schlüssel verwalten.



8. Stellen Sie sicher, dass das Konto, auf dem die MOBOTIX HUB Management Server-, Recording Server- oder Mobile Server-Software ausgeführt wird, in der Liste der Benutzer mit der Berechtigung zur Verwendung des Zertifikats enthalten ist.
9. Stellen Sie sicher, dass für den Benutzer sowohl die Berechtigung Vollzugriff als auch die Leseberechtigung aktiviert sind.



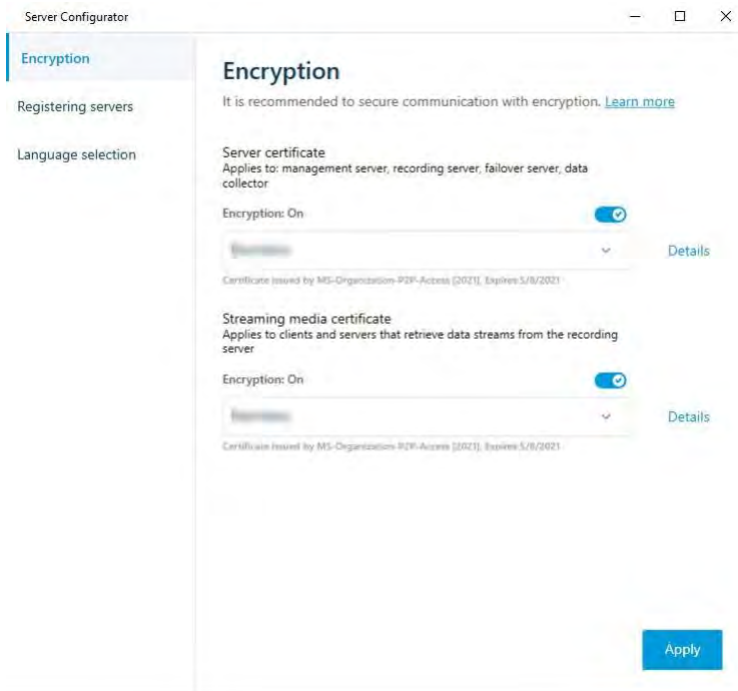
Standardmäßig verwendet die MOBOTIX HUB-Software das NETWORK SERVICE-Konto. In einer Domänenumgebung werden Dienstkonto häufig zum Installieren und Ausführen von MOBOTIX HUB-Diensten verwendet. Sie müssen dies mit Ihrem Domänenverwaltungsteam besprechen und den Dienstkonto die richtigen Berechtigungen hinzufügen, wenn sie noch nicht ordnungsgemäß konfiguriert

15.5.1 Aktivieren der Serververschlüsselung für Management-Server und Aufzeichnungsserver

Nachdem das Zertifikat mit den richtigen Eigenschaften und Berechtigungen installiert wurde, gehen Sie wie folgt vor.

10. Öffnen Sie auf einem Computer, auf dem ein Management-Server oder Aufzeichnungsserver installiert ist, den Server-Konfigurator über:
 - Das Windows-Startmenü
oder
 - Der Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken
11. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
12. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
13. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
14. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Dem Benutzer des Aufzeichnungsserver-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.



15. Klicken Sie auf **Übernehmen**.



Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver gestoppt und neu gestartet. Das Beenden des Aufzeichnungsserver-Dienstes bedeutet, dass Sie keine Live-Videos aufzeichnen und anzeigen können, während Sie die Grundkonfiguration des Aufzeichnungsservers

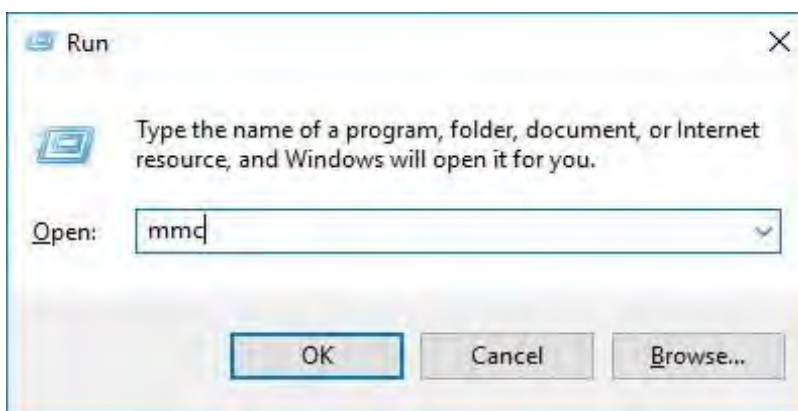
16 Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver

Beim Betrieb in einer Workgroup-Umgebung wird davon ausgegangen, dass keine Infrastruktur für Zertifizierungsstellen vorhanden ist. Zum Verteilen von Zertifikaten ist es erforderlich, eine Zertifizierungsstelleninfrastruktur zu erstellen. Es ist auch erforderlich, die Zertifikatsschlüssel an Client-Workstations zu verteilen. Abgesehen von diesen Anforderungen ähnelt der Prozess des Anforderns und Installierens eines Zertifikats auf einem Server sowohl dem Domänenszenario als auch dem Szenario einer kommerziellen Zertifizierungsstelle.

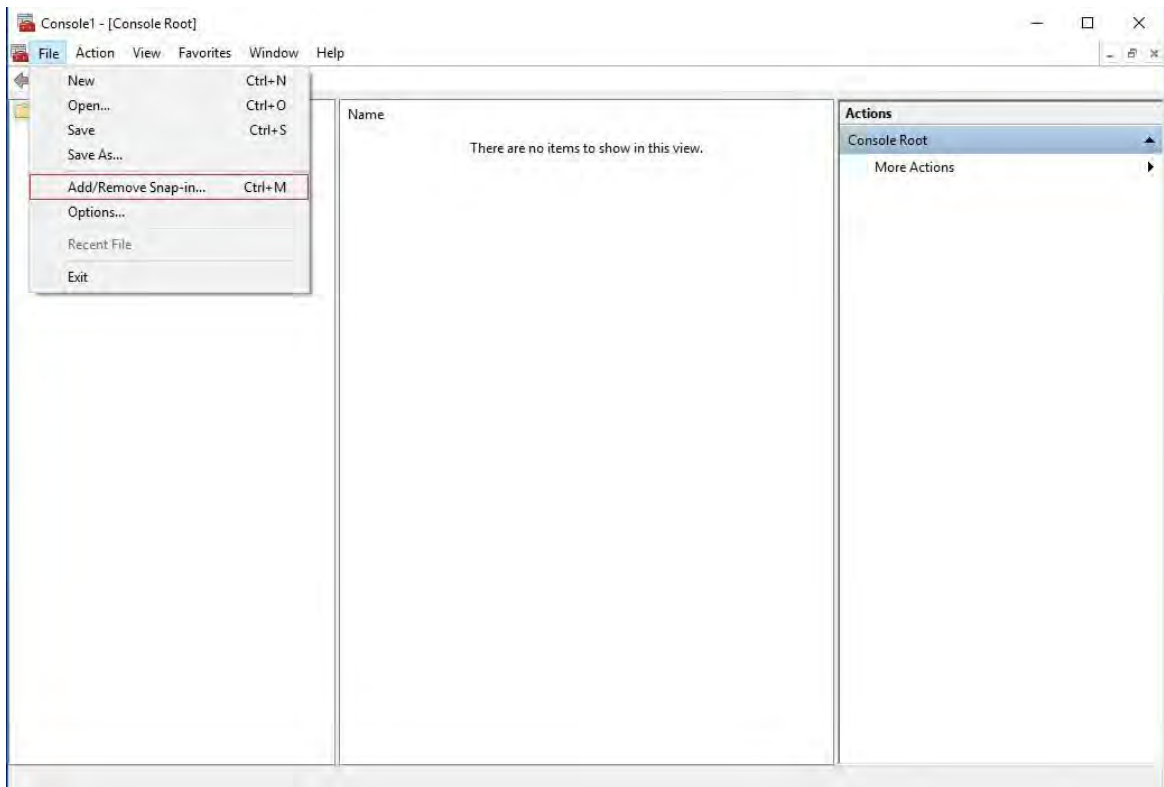
16.1 Hinzufügen eines Zertifizierungsstellenzertifikats zum Server

Fügen Sie dem Server das Zertifizierungsstellenzertifikat hinzu, indem Sie wie folgt vorgehen.

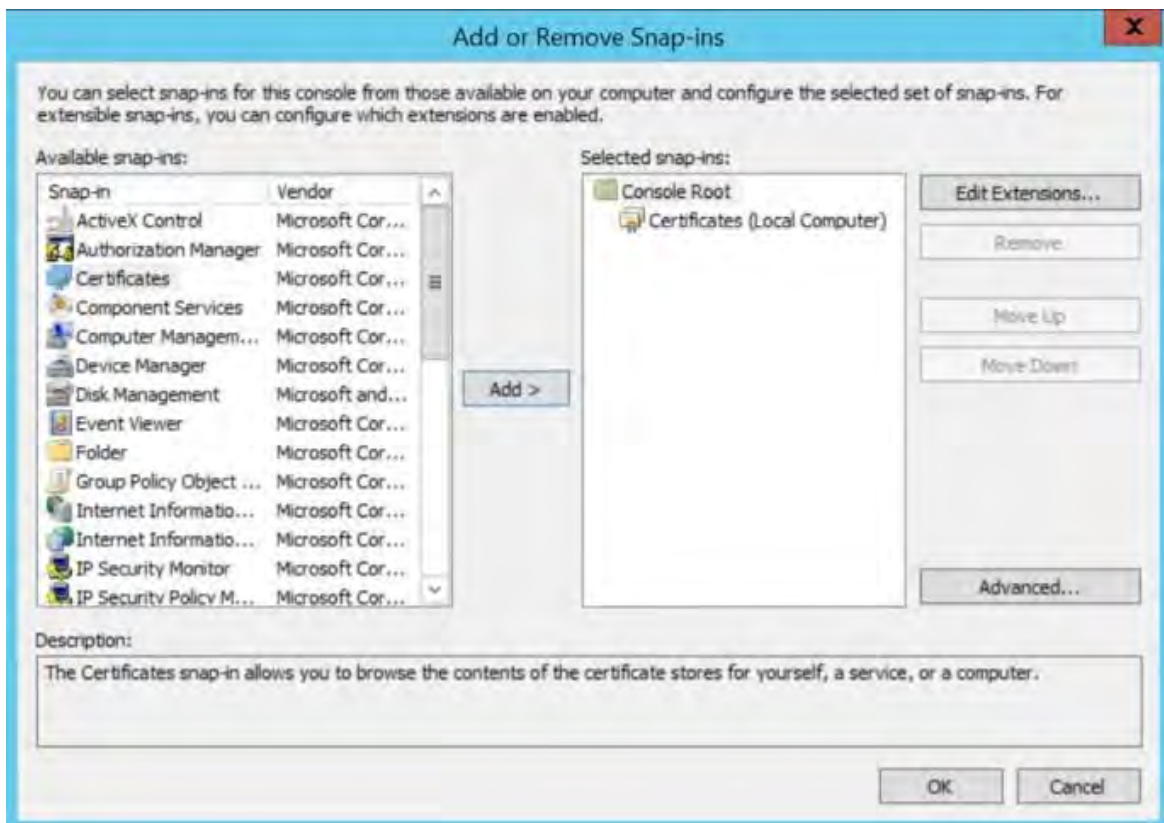
16. Öffnen Sie auf dem Computer, auf dem der MOBOTIX HUB-Server gehostet wird, die Microsoft Management Console.



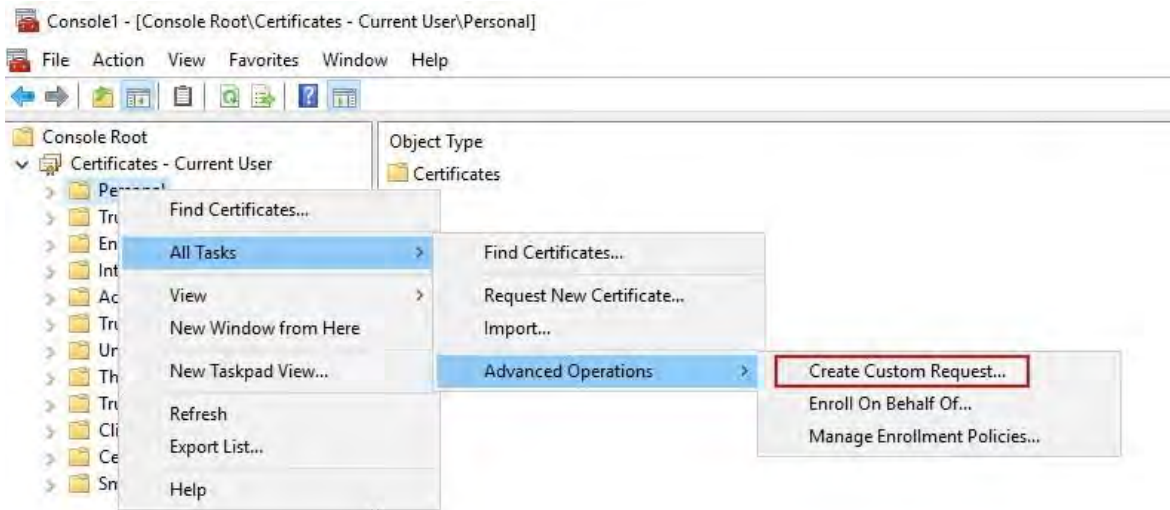
17. Wählen Sie in der Microsoft Management Console im **Menü Datei** die Option **Snap-In hinzufügen/entfernen....**



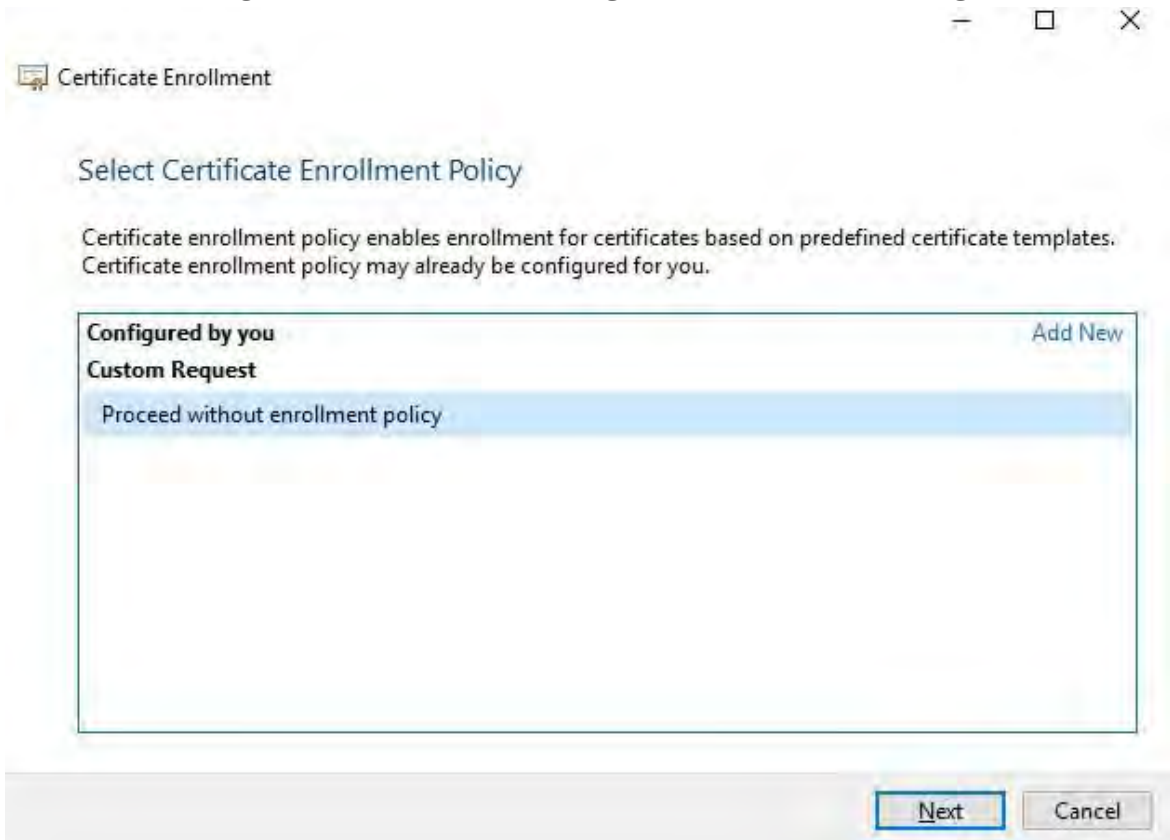
- 18. Wählen Sie das Snap-In Zertifikate aus, und klicken Sie auf **Hinzufügen**.
- 19. Klicken Sie auf **OK**.



- 20. Erweitern Sie das Objekt Zertifikate. Klicken Sie mit der rechten Maustaste auf den **Ordner Persönlich** und wählen Sie **Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen**.

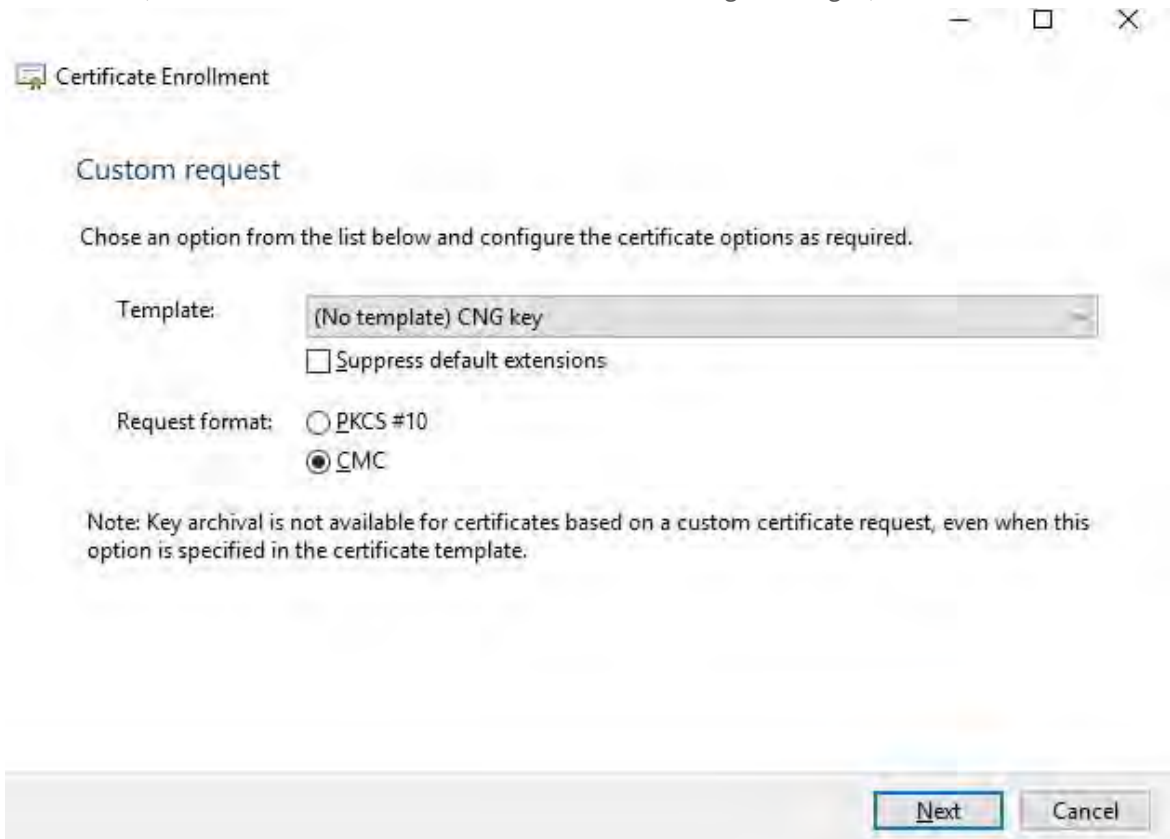


- 21. Klicken Sie im Zertifikatregistrierungs-Assistenten auf Weiter, und wählen Sie Ohne Registrierungsrichtlinie fortfahren aus.
- 22. Klicken Sie auf Weiter.
- 23. Wählen Sie die Vorlage **CNG-Schlüssel (keine Vorlage)** und das **CMC-Anforderungsformat** aus und

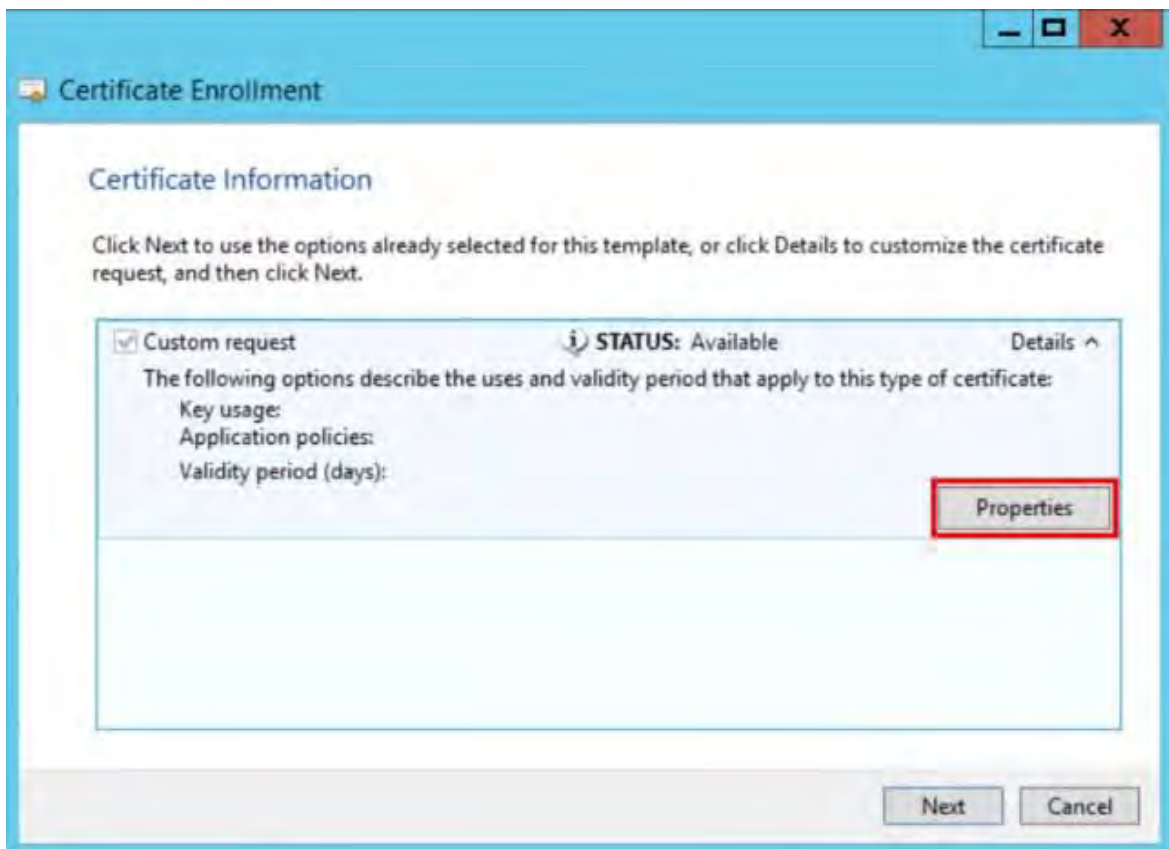


klicken Sie auf **Weiter**.

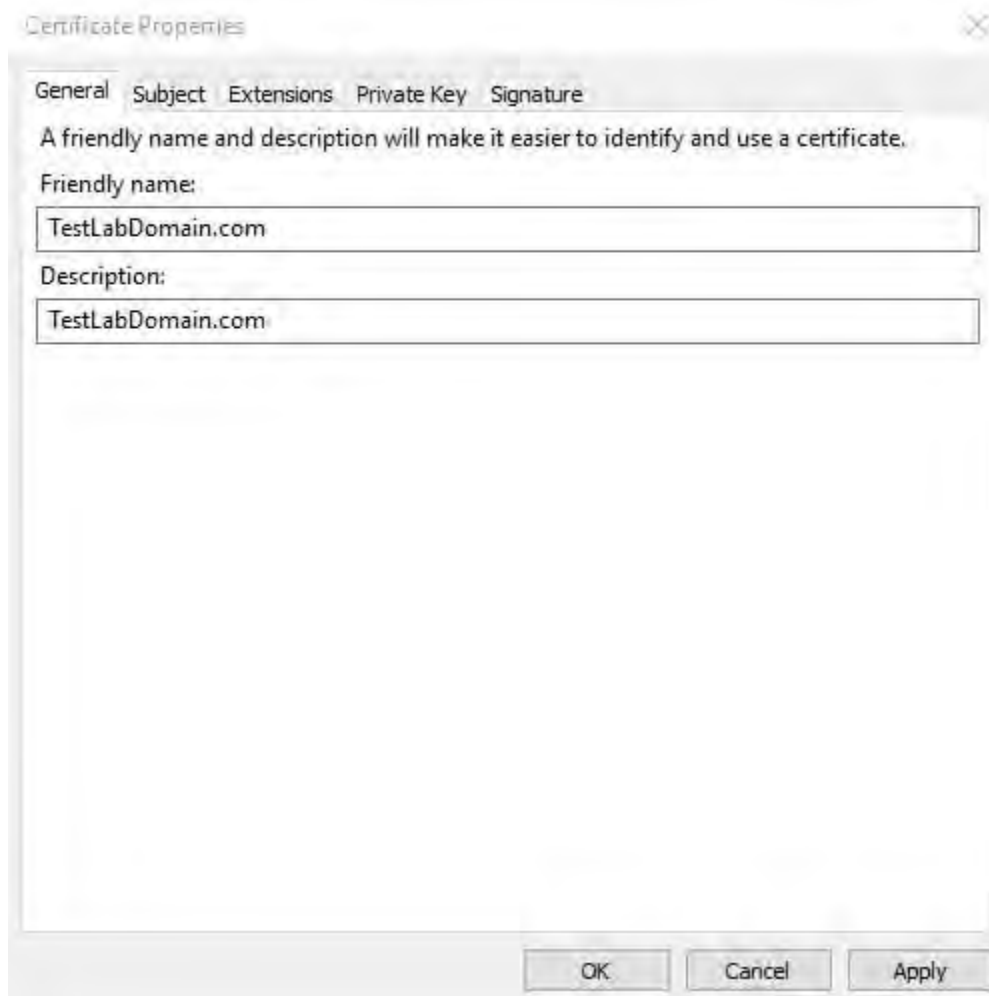
24. Erweitern Sie, um die **Details** der benutzerdefinierten Anforderung anzuzeigen, und klicken Sie auf



Eigenschaften.



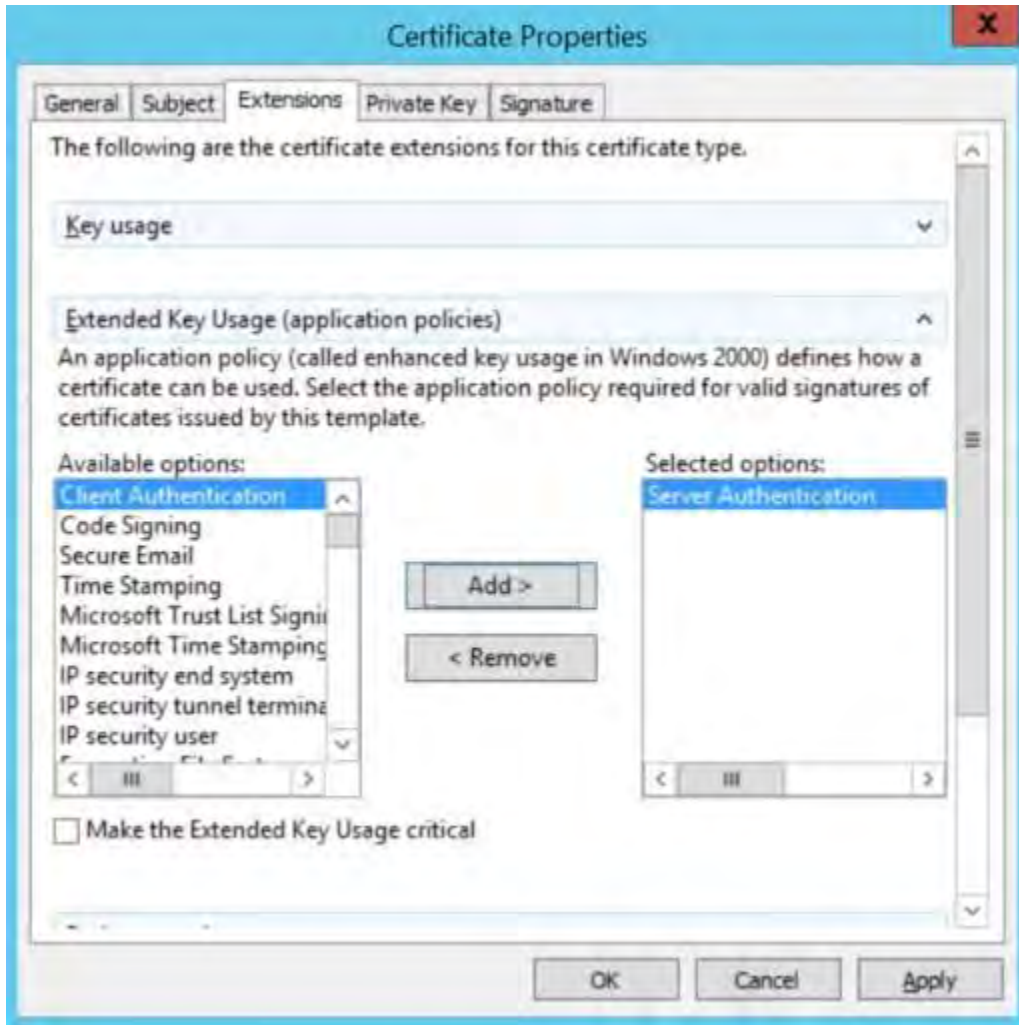
25. Füllen Sie auf der **Registerkarte Allgemein** die Felder **Anzeigename** und **Beschreibung** mit dem Domännennamen, dem Computernamen oder der Organisation aus.



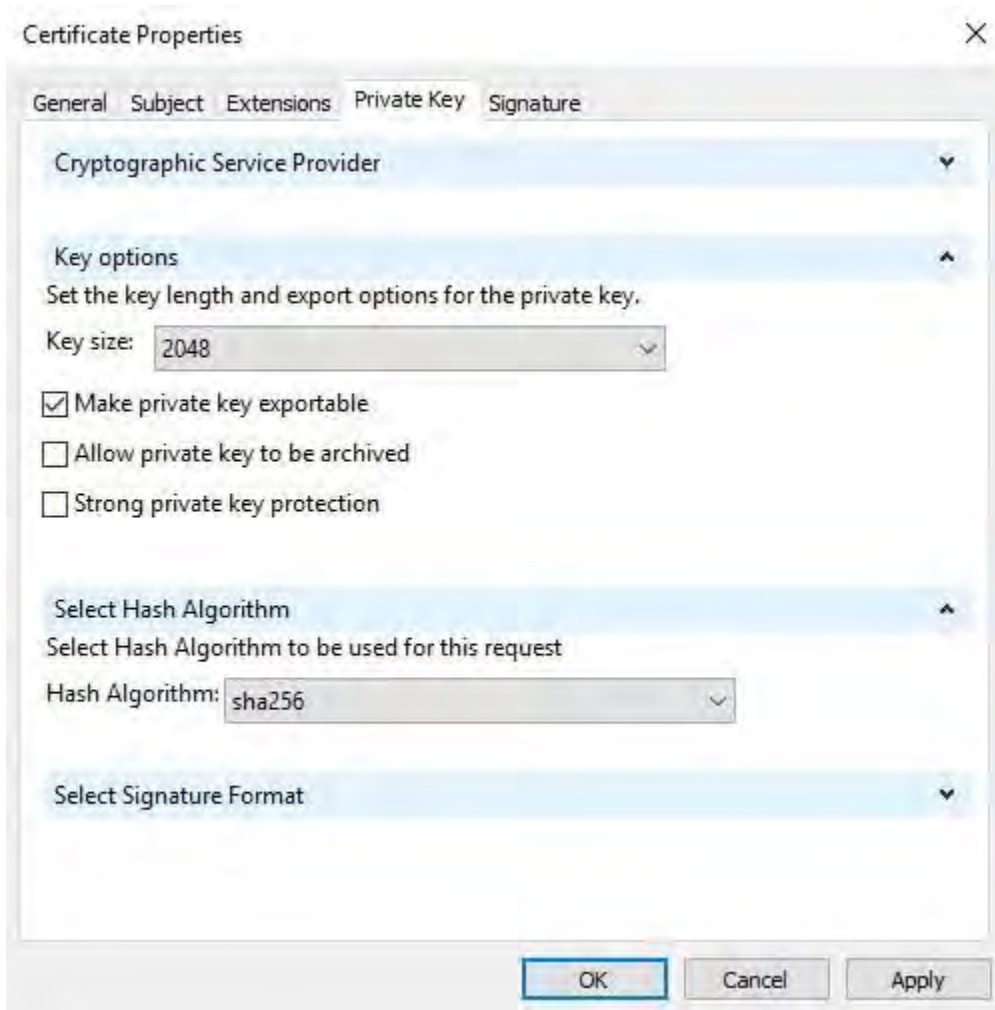
26. Geben Sie auf der **Registerkarte Betreff** die erforderlichen Parameter für den Antragstellernamen ein.
27. Geben Sie unter Antragstellername **Typ** unter **Allgemeiner Name** den Hostnamen des Computers ein, auf dem das Zertifikat installiert werden soll.



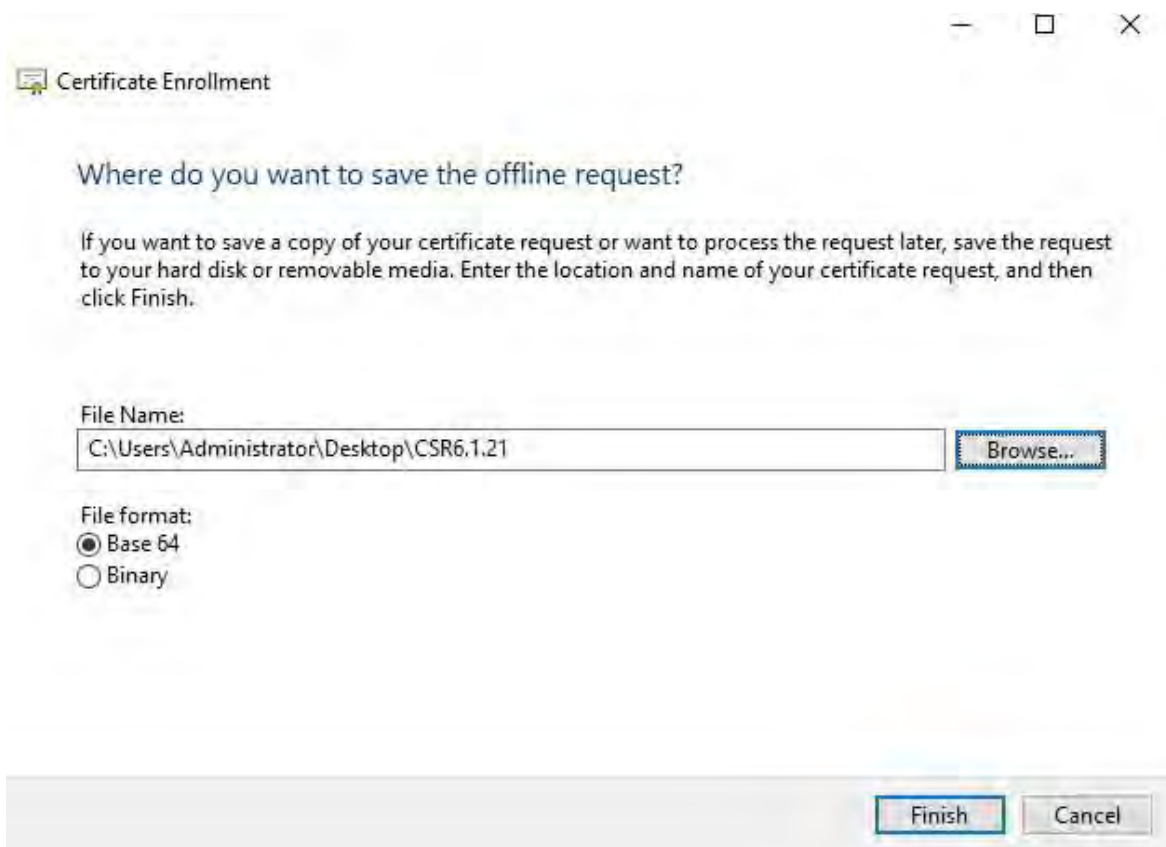
28. Erweitern Sie auf der Registerkarte Erweiterungen das Menü Erweiterte Schlüsselerwendung (Anwendungsrichtlinien). Fügen Sie die Serverauthentifizierung aus der Liste der verfügbaren Optionen hinzu.



- 29. Erweitern Sie **auf der Registerkarte Privater Schlüssel** das Menü **Schlüsseloptionen**.
- 30. Legen Sie die Schlüsselgröße auf 2048 fest, und wählen Sie die Option aus, um den privaten Schlüssel exportierbar zu machen. Klicken Sie auf **OK**.



31. Wenn alle Zertifikateigenschaften definiert wurden, klicken Sie **in der Zertifikatregistrierung** auf **Weiter**
32. Zauberer.
33. Wählen Sie einen Speicherort für die Zertifikatanforderung und ein Format aus. Navigieren Sie zu diesem Speicherort, und geben Sie einen Namen für die REQ-Datei an. Das Standardformat ist die Basis 64.
34. Klicken Sie auf **Fertig stellen**.



Es wird eine .req-Datei generiert, die Sie zum Anfordern eines signierten Zertifikats verwenden müssen.

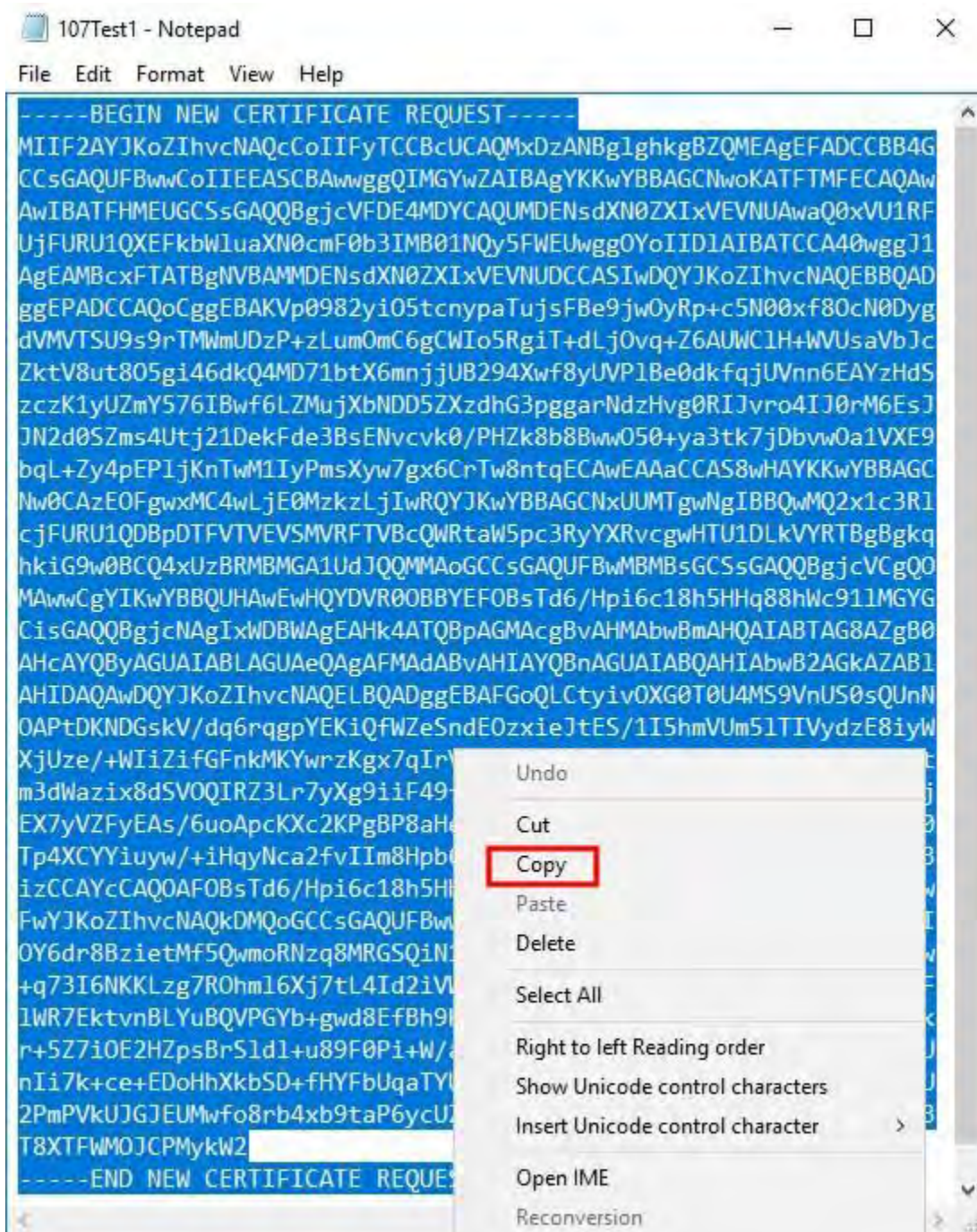
16.1.1 Laden Sie die .req-Datei hoch, um im Gegenzug ein signiertes Zertifikat zu erhalten.

Sie müssen den gesamten Text der REQ-Datei, einschließlich der Anfangs- und Endzeilen, kopieren und den Text in die interne Zertifizierungsstelle der Active Directory-Zertifikatdienste im Netzwerk einfügen. Weitere Informationen finden Sie unter [Installieren von Active Directory-Zertifikatdiensten auf Seite 74](#).

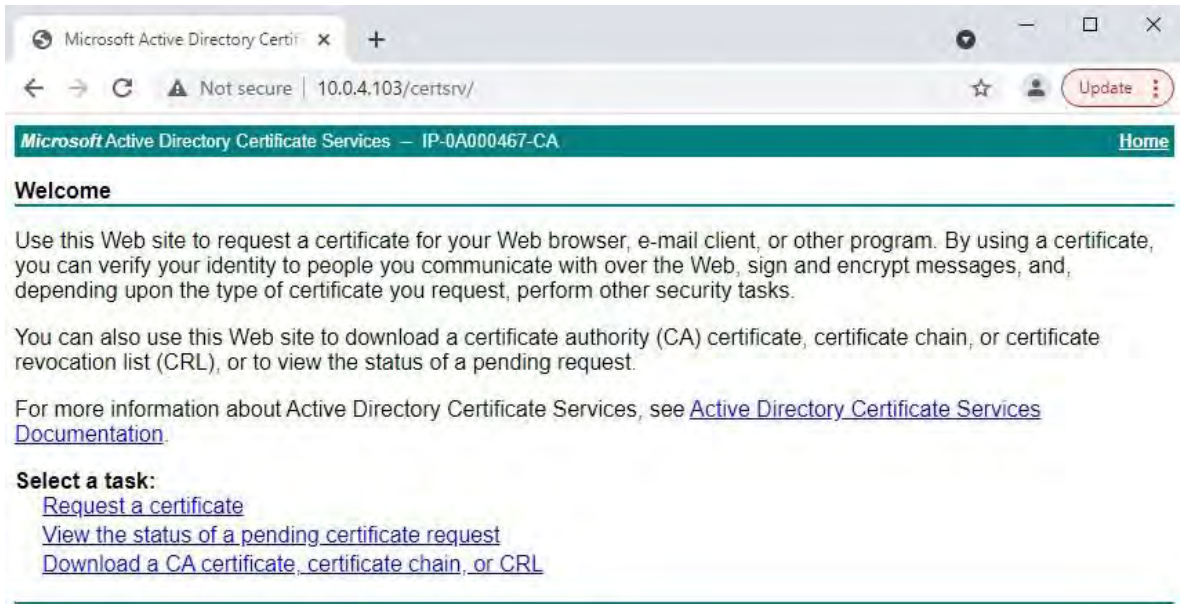


Sofern in Ihrer Domäne die Active Directory-Zertifikatdienste nicht erst kürzlich installiert wurden oder nur zu diesem Zweck installiert wurde, müssen Sie diese Anforderung nach einem separaten Verfahren senden, das von Ihrem Domänenverwaltungsteam konfiguriert wurde. Bitte bestätigen Sie diesen Vorgang mit ihnen, bevor Sie fortfahren.

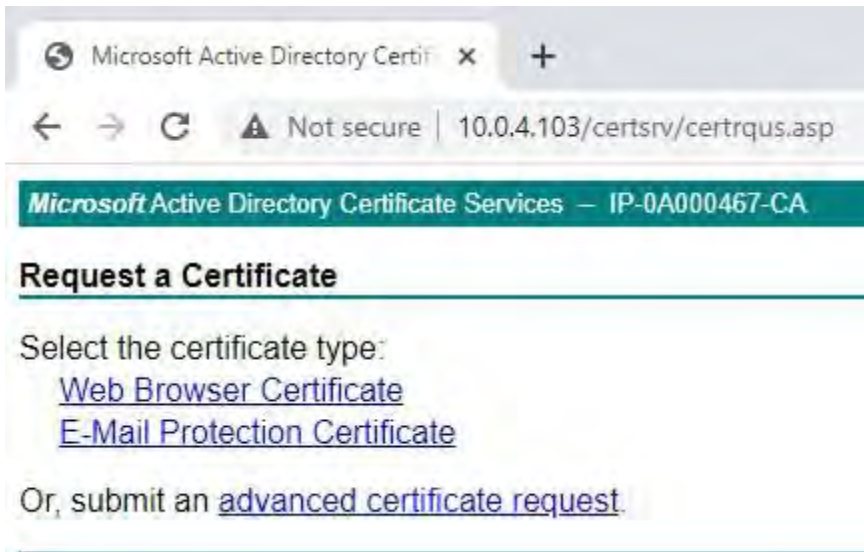
1. Navigieren Sie zum Speicherort der REQ-Datei, und öffnen Sie sie im Editor.



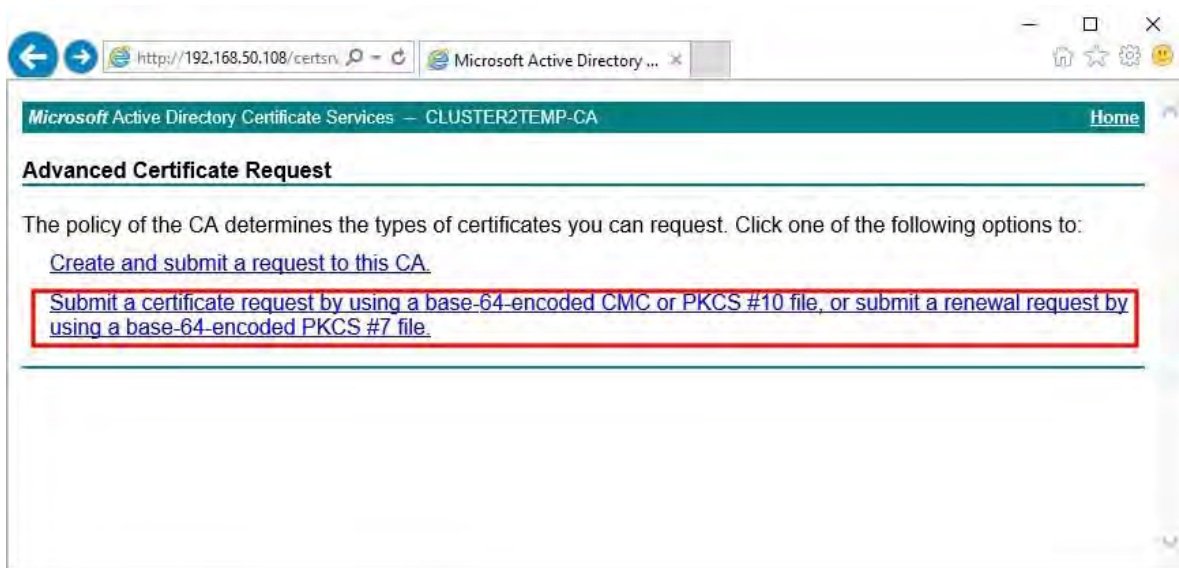
2. Kopieren Sie den gesamten Inhalt der Datei. Dazu gehören auch die gestrichelten Linien, die den Anfang und das Ende der Zertifikatsanforderung markieren.
3. Öffnen Sie einen Webbrowser und geben Sie die Adresse der internen Zertifizierungsstelle ein, die sich unter [ip.ad.dr.ess/certsrv] befinden sollte.
Dabei ist ip.ad.dr.ess die IP-Adresse oder der DNS-Name des AD CS-Hostservers des internen Netzwerks.



- 4. Klicken Sie auf den Link Zertifikat anfordern.
- 5. Klicken Sie auf den Link für die Anforderung eines erweiterten Zertifikats.

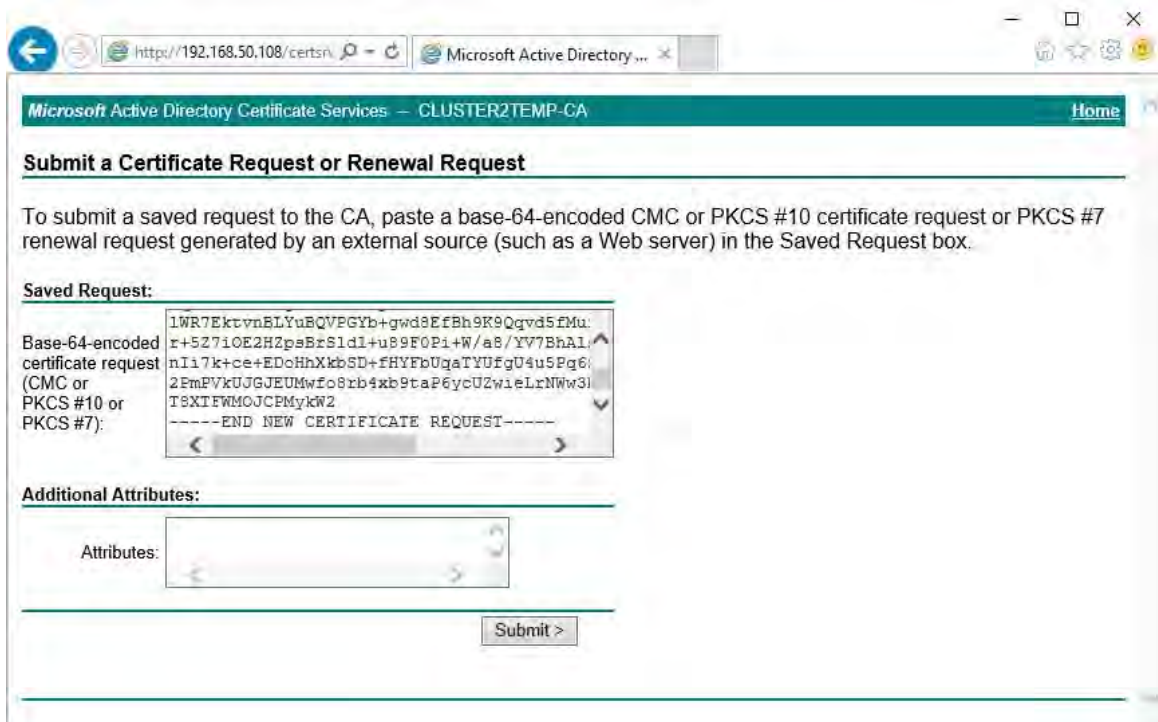


- 6. Wählen Sie aus, ob Sie eine Zertifikatanforderung mithilfe einer Base64-codierten CMC-Datei übermitteln möchten.



7. Fügen Sie den Inhalt der .req-Datei in das Formular ein. Wenn es erforderlich ist, eine Zertifikatvorlage auszuwählen, wählen Sie

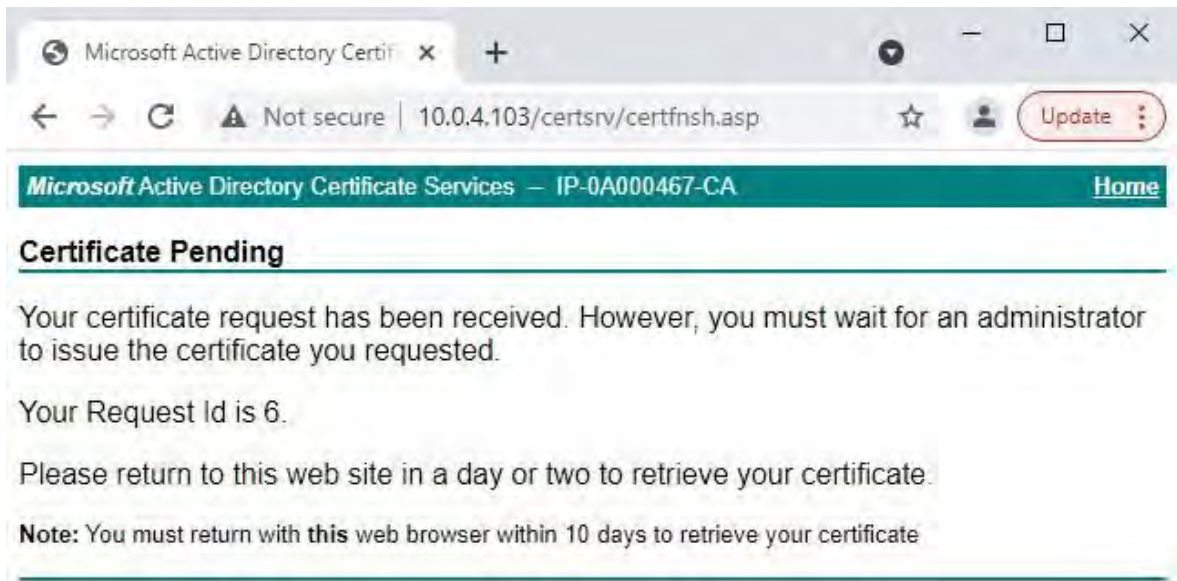
Webserver aus der Liste Zertifikatvorlage.



8. Klicken Sie auf **Senden**.

Auf der Website wird eine Meldung angezeigt, dass das Zertifikat in einigen Tagen ausgestellt wird.

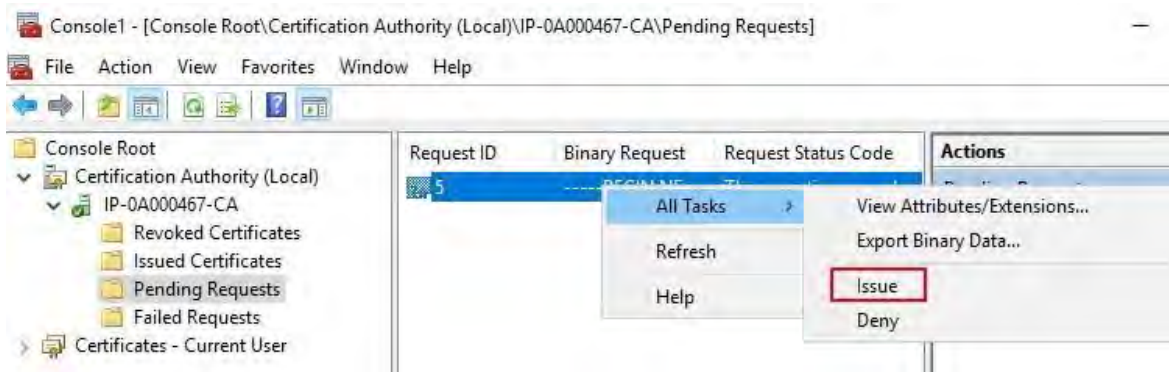
- Interne CA-Server können zum manuellen Ausstellen von Zertifikaten verwendet werden
- Notieren Sie sich das Datum und die Uhrzeit, zu der die Zertifikatsanforderung eingereicht wurde.



16.1.2 Manuelles Ausstellen von Zertifikaten

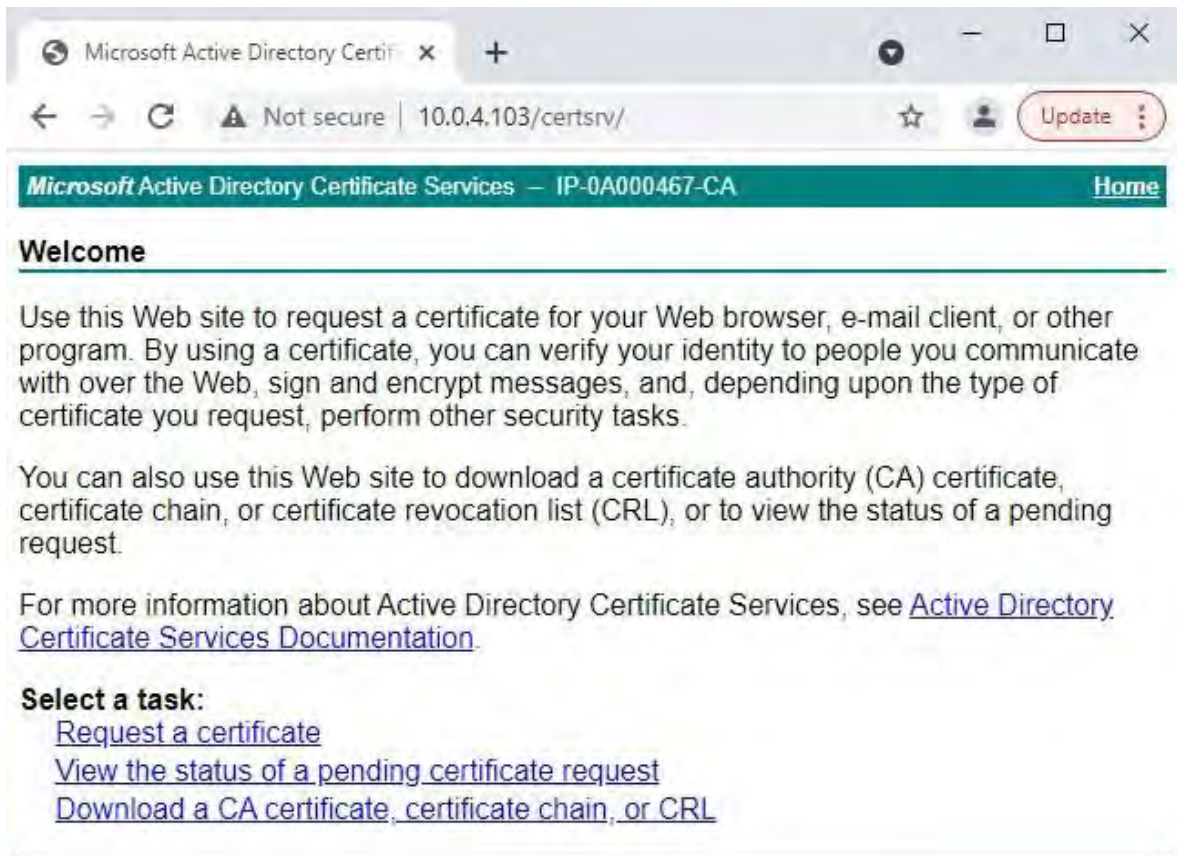
Sie können Zertifikate manuell von dem Computer ausstellen, auf dem die Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) gehostet werden.

1. Öffnen Sie die Microsoft Management Console (MMC).
2. Navigieren Sie zum **Snap-In** Zertifizierungsstelle.
3. Erweitern Sie das **Objekt Zertifizierungsstelle**.
4. Klicken Sie im Ordner "**Ausstehende Anforderungen**" mit der rechten Maustaste auf die entsprechende Anforderungs-ID, und wählen Sie in der **Liste "Alle Aufgaben"** die Option "**Problem**" aus.
5. Öffnen Sie einen Browser, und rufen Sie die IIS-Site der internen Zertifizierungsstelle auf, die sich unter [

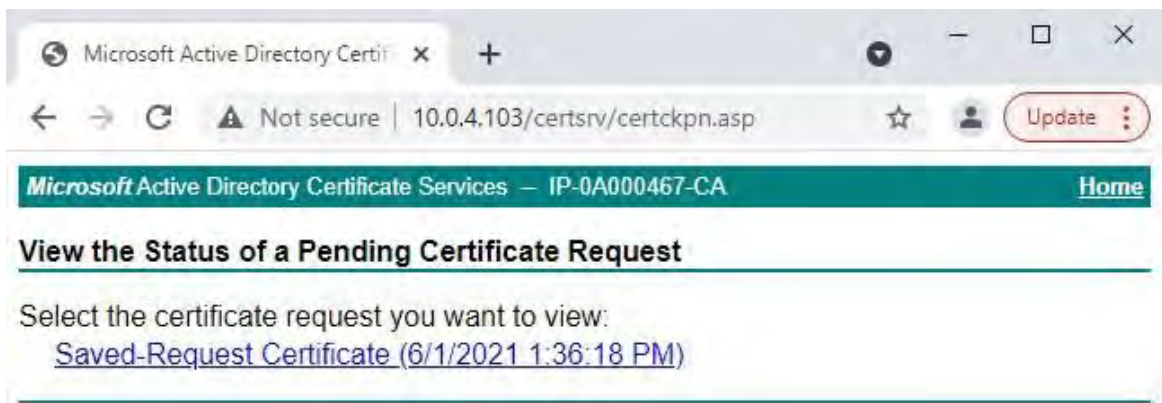


ip.ad.dr.ess/certsrv] befindet.

6. Klicken Sie auf den Link Status einer ausstehenden Zertifikatanforderung anzeigen.



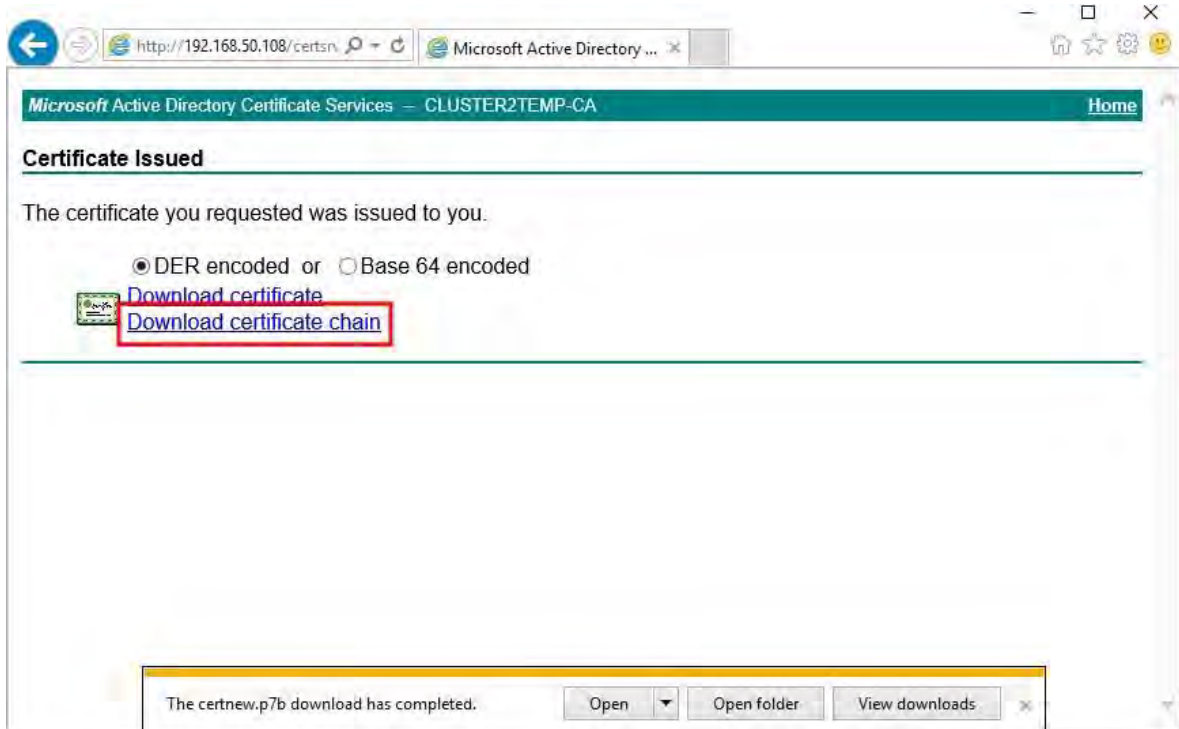
- 7. Wenn das Zertifikat ausgestellt wurde, ist auf der resultierenden Seite ein Link verfügbar, der das Datum der Zertifikatsanforderung enthält.



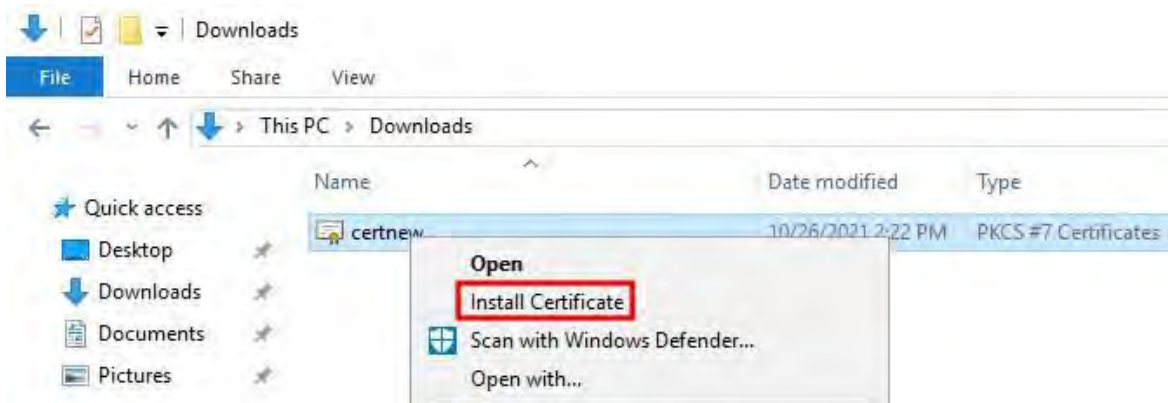
- 8. Wählen Sie **DER-codiert aus**, und laden Sie die Zertifikatkette herunter.

MOBOTIX HUB – Leitfaden für Zertifikate - Installieren von Zertifikaten in einer

Navigieren Sie zum Ordner Downloads, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **im**



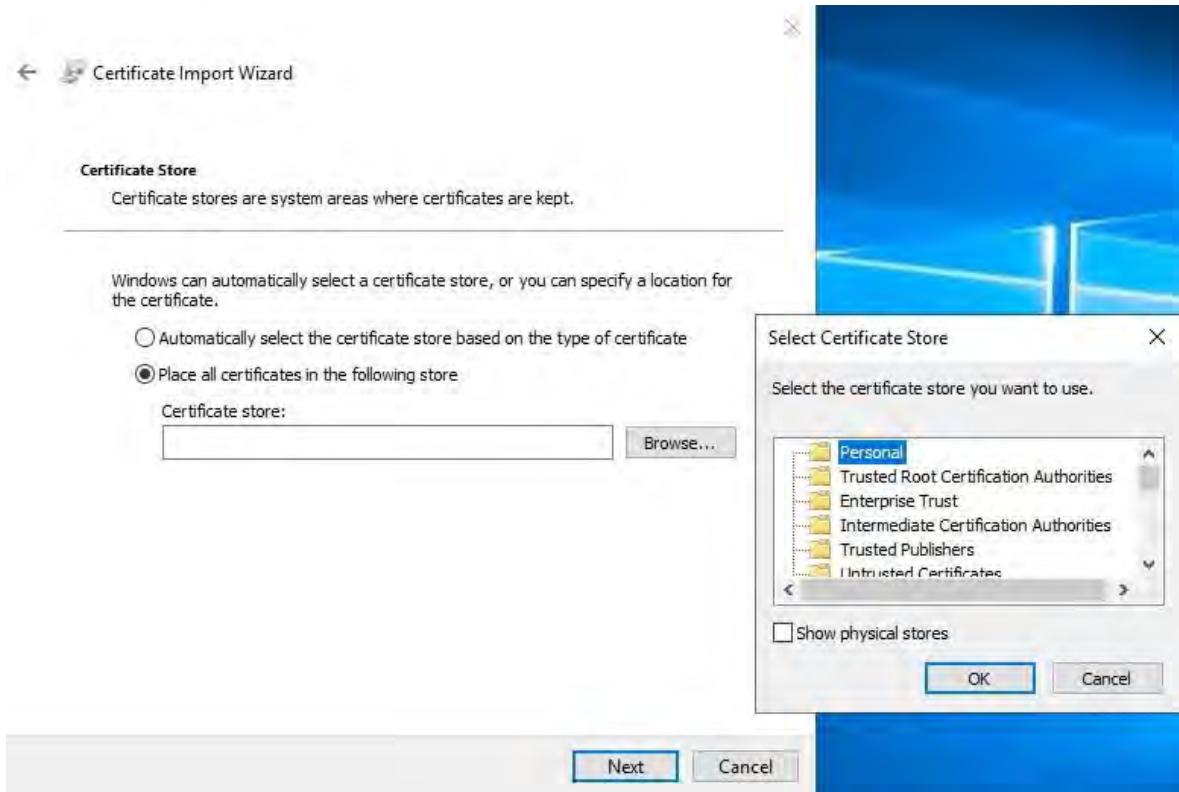
Kontextmenü die Option Zertifikat installieren aus.



9. Akzeptieren Sie die Sicherheitswarnung, wenn sie angezeigt wird.
10. Wählen Sie aus, um das Zertifikat für den aktuellen Benutzer zu installieren, und klicken Sie auf **Weiter**.



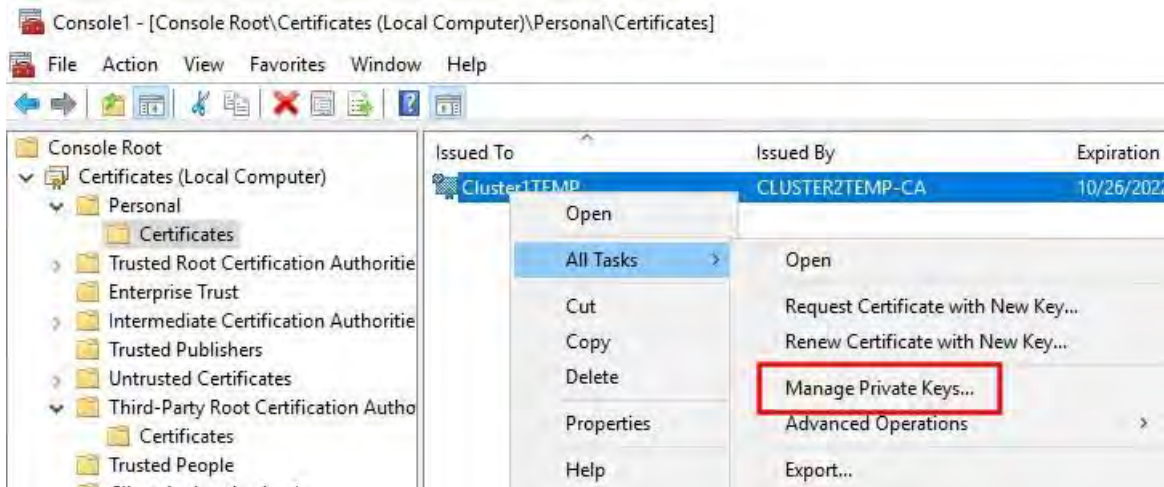
11. Wählen Sie einen Geschäftsstandort aus. Wählen Sie **Alle Zertifikate im folgenden Speicher speichern aus**, und klicken Sie auf die **Schaltfläche Durchsuchen**, um das Fenster **Zertifikatspeicher auswählen zu** öffnen. Navigieren Sie zum **Speicher für persönliche Zertifikate**, und klicken Sie auf **OK**.
12. Klicken Sie auf **Weiter**.



13. Beenden Sie den Zertifikatimport-Assistenten.

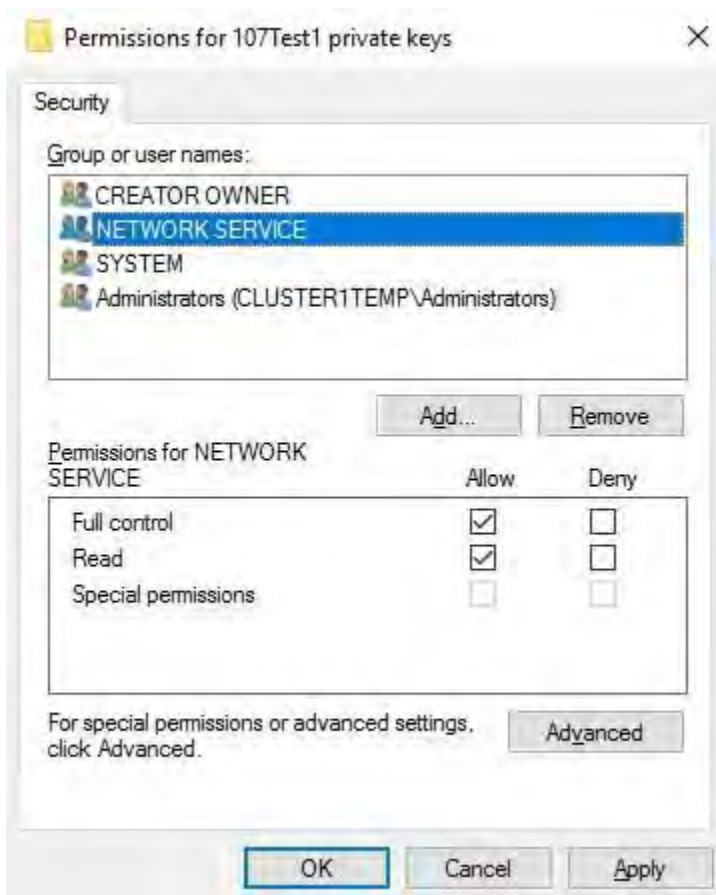
14. Wechseln Sie zum Zertifikat-Snap-In der Microsoft Management Console (MMC).

15. Navigieren Sie in der Konsole zum persönlichen Speicher, in dem das Zertifikat installiert ist. Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie **Alle Aufgaben > Private Schlüssel verwalten**.



16. Fügen Sie das Konto, auf dem die MOBOTIX HUB Management Server-, Recording Server- oder Mobile Server-Software ausgeführt wird, der Liste der Benutzer hinzu, die zur Verwendung des Zertifikats berechtigt sind.
17. Stellen Sie sicher, dass für den Benutzer sowohl die Berechtigung Vollzugriff als auch die Leseberechtigung aktiviert sind.

Standardmäßig verwendet die MOBOTIX HUB-Software das NETWORK SERVICE-Konto.

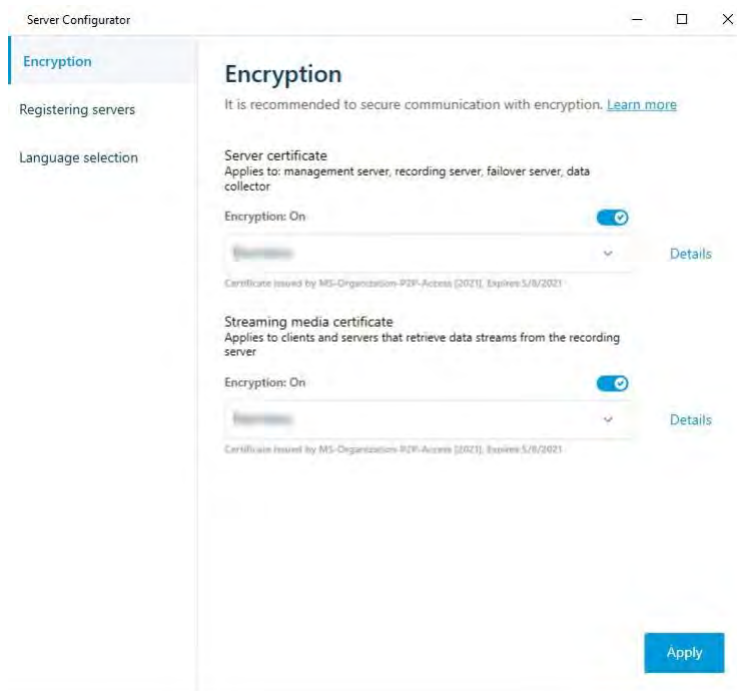


16.1.3 Aktivieren der Serververschlüsselung für Management-Server und Aufzeichnungsserver

Nachdem das Zertifikat mit den richtigen Eigenschaften und Berechtigungen installiert wurde, gehen Sie wie folgt vor.

1. Öffnen Sie auf einem Computer, auf dem ein Management-Server oder Aufzeichnungsserver installiert ist, den **Server-Konfigurator** über:
 - Das Windows-Startmenü
oder
 - Der Server-Manager, indem Sie mit der rechten Maustaste auf das Server-Manager-Symbol in der Taskleiste des Computers klicken
2. Aktivieren Sie im Server-Konfigurator unter Serverzertifikat die Option Verschlüsselung.
3. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
4. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Aufzeichnungsserver, dem Verwaltungsserver, dem Failover-Server und dem Datensammlerserver zu verschlüsseln.
5. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.

Dem Benutzer des Aufzeichnungsserver-Dienstes wurde Zugriff auf den privaten Schlüssel gewährt. Es ist erforderlich, dass dieses Zertifikat auf allen Clients vertrauenswürdig ist.



6. Klicken Sie auf **Übernehmen**.



Wenn Sie Zertifikate anwenden, wird der Aufzeichnungsserver gestoppt und neu gestartet. Das Beenden des Aufzeichnungsserver-Dienstes bedeutet, dass Sie keine Live-Videos aufzeichnen und anzeigen können, während Sie die Grundkonfiguration des Aufzeichnungsservers

16.2 Installieren von Zertifikaten für die Kommunikation mit dem Ereignisserver

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln. Wenn Sie die Verschlüsselung auf dem Ereignisserver aktivieren, gilt sie für Verbindungen von allen Komponenten, die eine Verbindung mit dem Ereignisserver herstellen. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem



Wenn die Event-Server-Kommunikation verschlüsselt ist, gilt dies für die gesamte Kommunikation mit diesem Event-Server. Das heißt, es wird jeweils nur ein Modus unterstützt, entweder http oder https, aber nicht gleichzeitig.

Ereignisserver und allen Verbindungskomponenten installieren.

Die Verschlüsselung gilt für jeden Dienst, der auf dem Ereignisserver gehostet wird, einschließlich Transact, Maps, GisMap und Intercommunication.



Bevor Sie die Verschlüsselung im Event Server aktivieren, müssen alle Clients (Desk Client und Management Client) und das MOBOTIX HUB LPR-Plug-In mindestens auf Version 2022 R1 aktualisiert werden.
HTTPS wird nur unterstützt, wenn jede Komponente mindestens auf Version 2022 R1 aktualisiert wurde.

Die Erstellung der Zertifikate ist je nach Zertifikatsumgebung die gleiche wie in diesen Abschnitten beschrieben:

[Installieren von Zertifikaten von Drittanbietern oder kommerziellen Zertifizierungsstellen für die Kommunikation mit dem Management Server oder Recording Server auf Seite 57](#)

[Installieren von Zertifikaten in einer Domäne für die Kommunikation mit dem Management Server oder Recording Server auf Seite 86](#)

[Installieren von Zertifikaten in einer Arbeitsgruppenumgebung für die Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver auf Seite 104](#)

16.3 Aktivieren der MOBOTIX HUB Event Server-Verschlüsselung

Nachdem das Zertifikat installiert wurde, können Sie es für die gesamte Kommunikation mit dem Ereignisserver aktivieren.



Nachdem alle Clients mindestens auf Version 2022 R1 aktualisiert wurden, können Sie die Verschlüsselung auf dem Ereignisserver aktivieren.

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln.



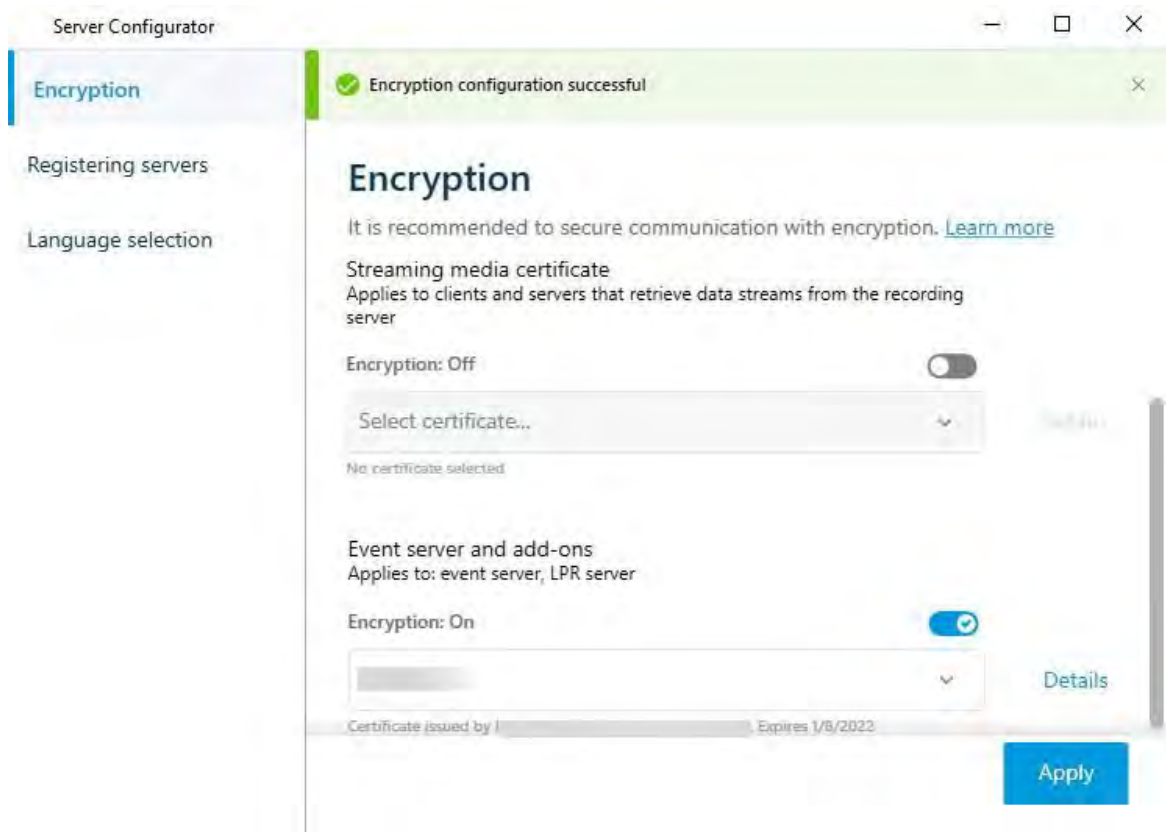
Wenn Sie die Verschlüsselung für eine Servergruppe konfigurieren, muss sie entweder mit einem Zertifikat aktiviert werden, das zum selben Zertifizierungsstellenzertifikat gehört, oder, wenn die Verschlüsselung deaktiviert ist, auf allen Computern in der Servergruppe deaktiviert

16.3.1 Voraussetzungen:

Auf dem Computer, auf dem der Ereignisserver gehostet wird, ist ein Serverauthentifizierungszertifikat vertrauenswürdig. Aktivieren Sie zunächst die Verschlüsselung auf dem Ereignisserver.

Schritte:

7. Öffnen Sie auf einem Computer, auf dem ein Ereignisserver installiert ist, den **Serverkonfigurator** über:
 - Das Windows-Startmenü
oder
 - Den Ereignisserver, indem Sie mit der rechten Maustaste auf das Ereignisserverymbol in der Taskleiste des Computers klicken
8. Aktivieren Sie im Serverkonfigurator unter Ereignisserver und Add-Ons die Option Verschlüsselung.
9. Klicken Sie auf Zertifikat auswählen, um eine Liste mit eindeutigen Antragstellernamen von Zertifikaten zu öffnen, die über einen privaten Schlüssel verfügen und auf dem lokalen Computer im Windows-Zertifikatspeicher installiert sind.
10. Wählen Sie ein Zertifikat aus, um die Kommunikation zwischen dem Ereignisserver und den zugehörigen Add-Ons zu verschlüsseln.
11. Wählen Sie **Details** aus, um Informationen zum Windows-Zertifikatspeicher für das ausgewählte Zertifikat anzuzeigen.



12. Klicken Sie auf **Übernehmen**.

Um die Aktivierung der Verschlüsselung abzuschließen, besteht der nächste Schritt darin, die Verschlüsselungseinstellungen auf jedem zugehörigen Add-on-LPR-Server zu aktualisieren .

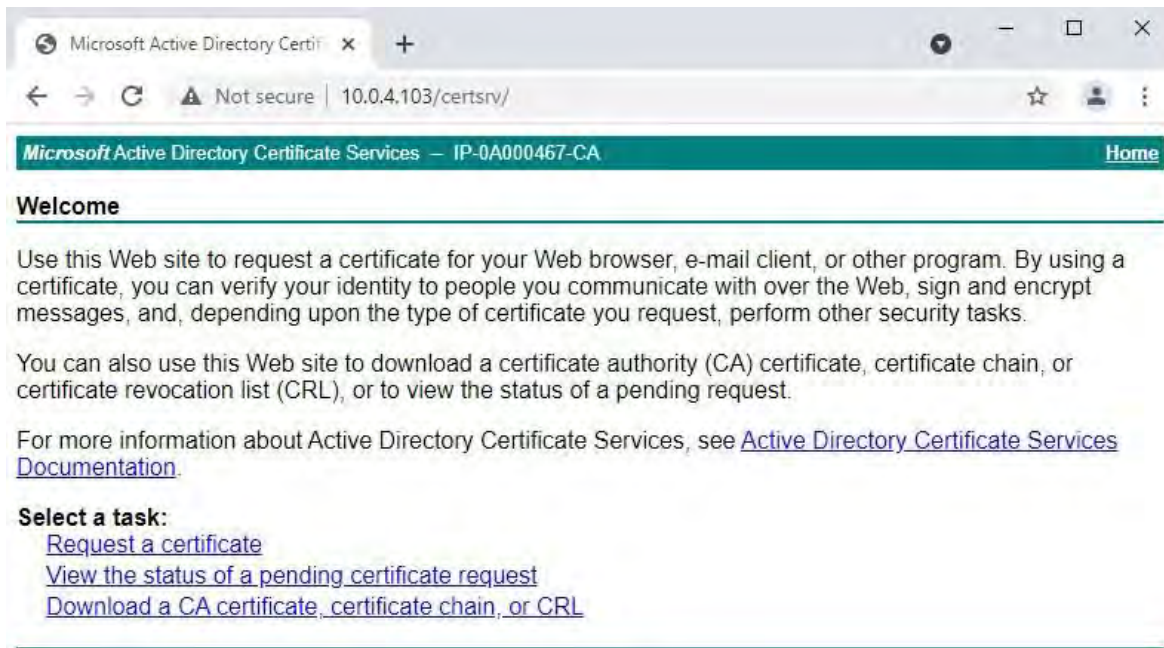
16.3.2 Importieren von Clientzertifikaten

In diesem Abschnitt wird beschrieben, wie Clientzertifikate auf eine Client-Workstation oder ein Client-Gerät importiert werden.

1. Nachdem Sie ein CA-Zertifikat auf den Management-Server oder den Aufzeichnungsserver importiert haben, können Sie von jeder Workstation oder jedem Server im Netzwerk aus auf die folgende Adresse zugreifen:

<http://localhost/certsrv/>

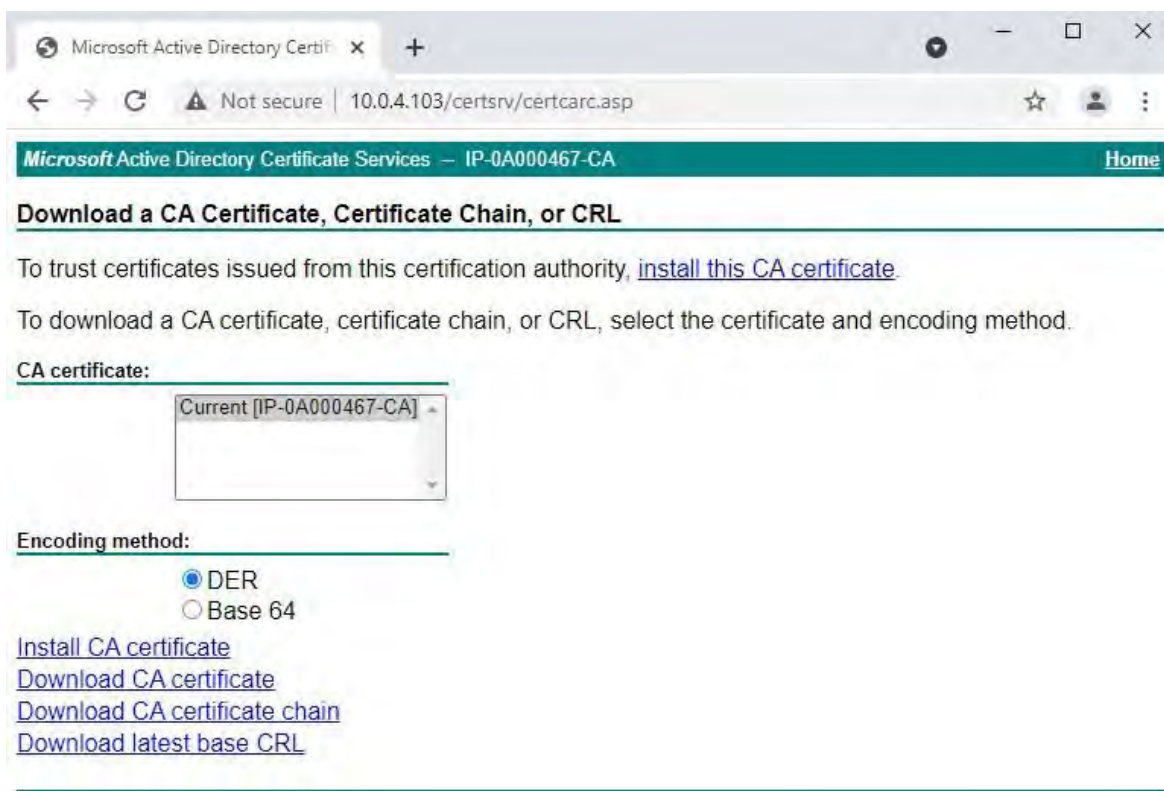
Die Adresse des Servers, auf dem sich das Zertifikat (privater Schlüssel) befindet, wird jedoch an die Stelle von "localhost" gesetzt. Zum Beispiel:



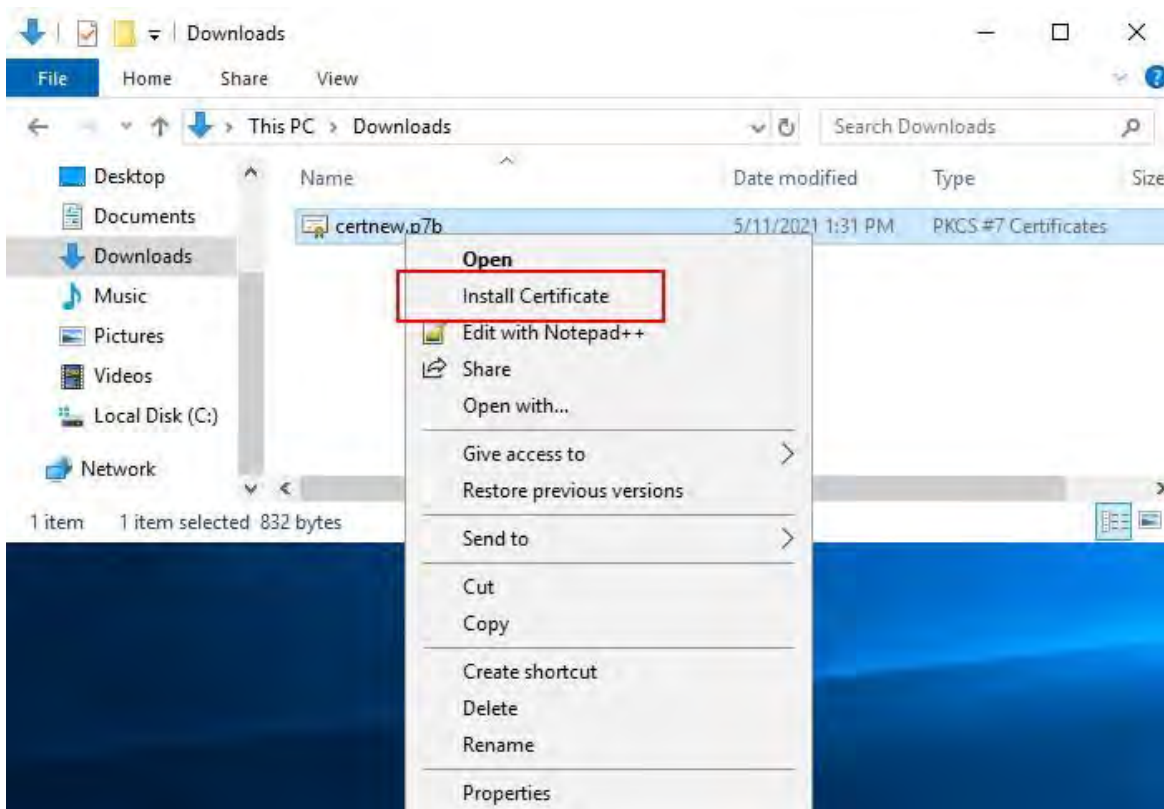
Dieser Webserver wird auf dem AD CS-Hostserver (Active Directory Certificate Services) gehostet, auf dem sich das Zertifizierungsstellenzertifikat befindet.

2. Klicken Sie auf Zertifizierungsstellenzertifikat, Zertifikatkette oder Zertifikatsperrliste herunterladen.
3. Wählen Sie im **Feld CA-Zertifikat** das CA-Zertifikat aus, das mit dem MOBOTIX HUB-System verwendet werden soll, und klicken Sie auf

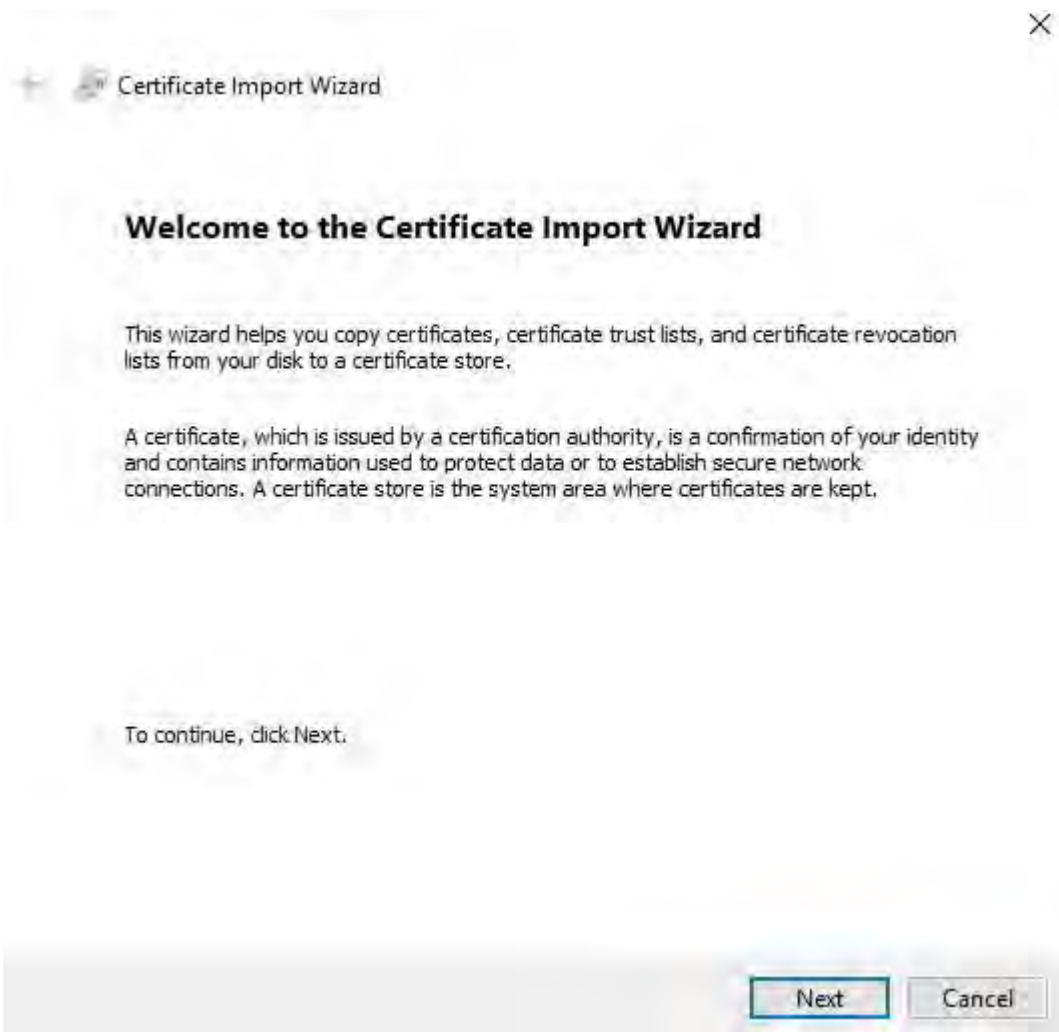
1. Laden Sie die CA-Zertifikatskette herunter.



4. Wählen Sie **DER-codiert aus**, und laden Sie die Zertifikatskette herunter.
5. Navigieren Sie zum Ordner Downloads, klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie **im** Kontextmenü die Option Zertifikat installieren aus.

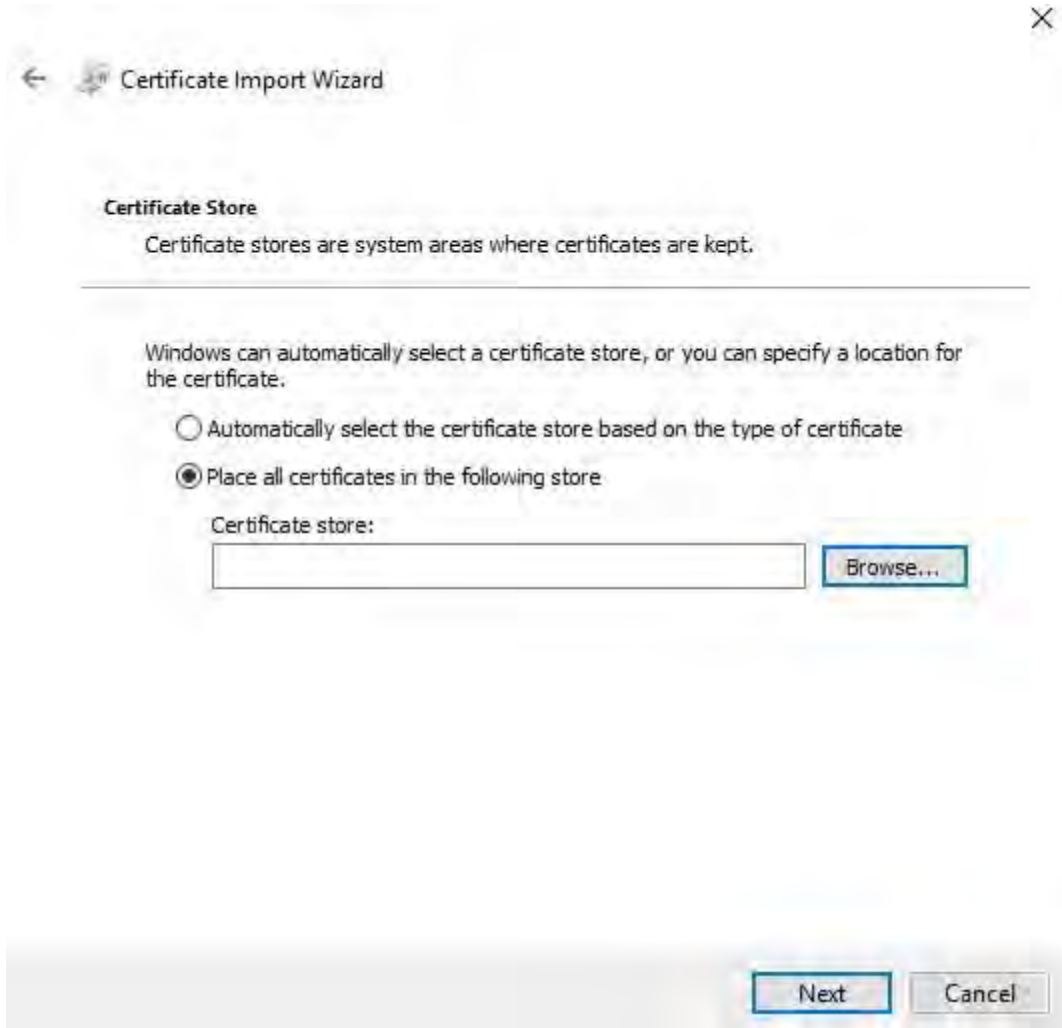


- 6. Dadurch wird der Zertifikatimport-Assistent gestartet.
- 7. Klicken Sie auf Weiter.

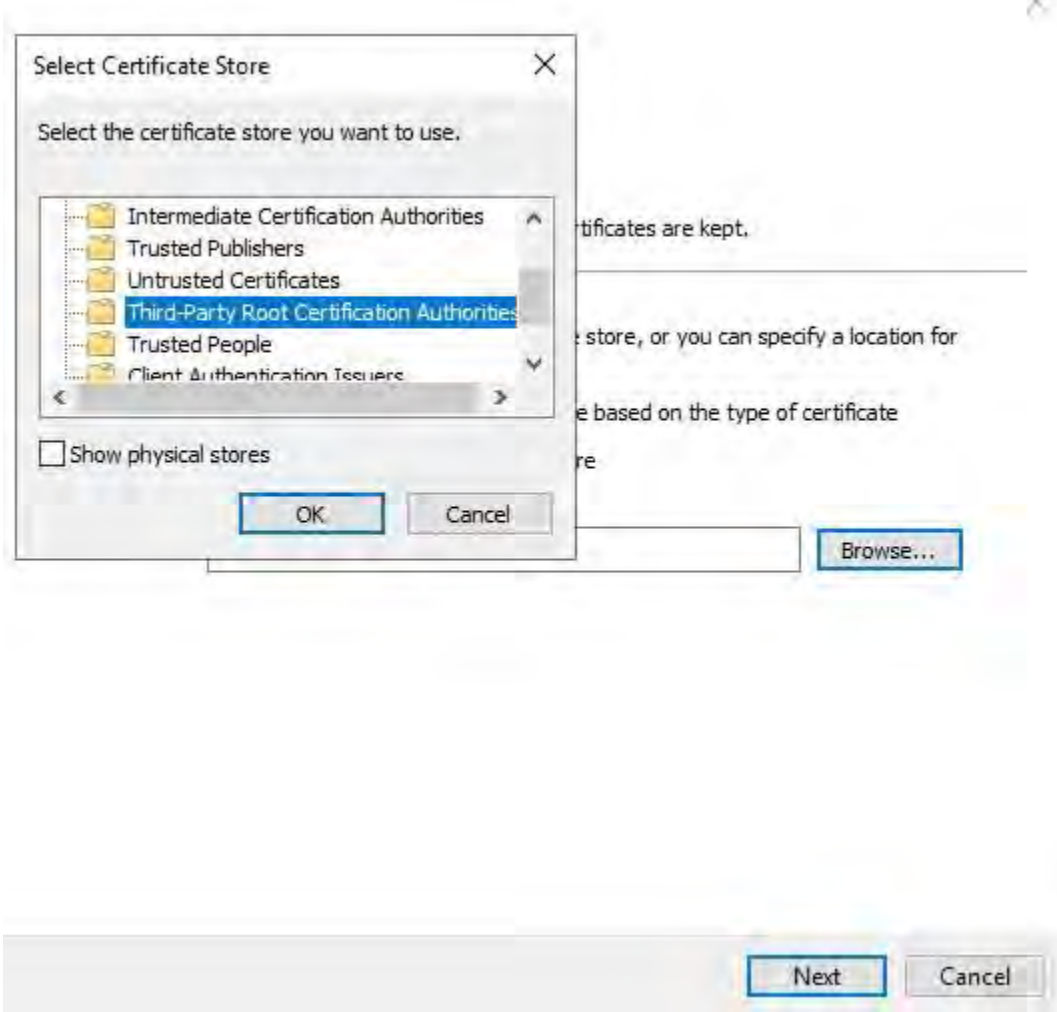


8. Wählen Sie einen Geschäftsstandort aus. Wählen Sie Alle Zertifikate im folgenden Speicher speichern aus, und klicken Sie auf die Schaltfläche Durchsuchen , um das Fenster **Zertifikatspeicher auswählen zu** öffnen.

9. Navigieren Sie zum Zertifikatspeicher für **Stammzertifizierungsstellen von Drittanbietern**, und



klicken Sie auf **OK**. Klicken Sie auf **Weiter**.



10. Beenden Sie den Zertifikatimport-Assistenten.

Jetzt hat die Workstation die Zertifikatskomponenten importiert, die für die sichere Kommunikation mit dem Management-Server oder dem Aufzeichnungsserver erforderlich sind.

16.4 Anzeigen des Verschlüsselungsstatus für Clients

So überprüfen Sie, ob Ihr Aufzeichnungsserver Verbindungen verschlüsselt:

1. Öffnen Sie den Management Client.
2. Wählen Sie im **Bereich Sitenavigation** die Option **Server > Aufzeichnungsserver aus**. Daraufhin wird eine Liste der Aufzeichnungsserver geöffnet.
3. Wählen Sie im **Bereich Übersicht** den entsprechenden Aufnahmeserver aus und wechseln Sie zur **Registerkarte Info**.

Wenn die Verschlüsselung für Clients und Server aktiviert ist, die Datenströme vom Aufzeichnungsserver abrufen, wird ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der optionalen Webserveradresse angezeigt.

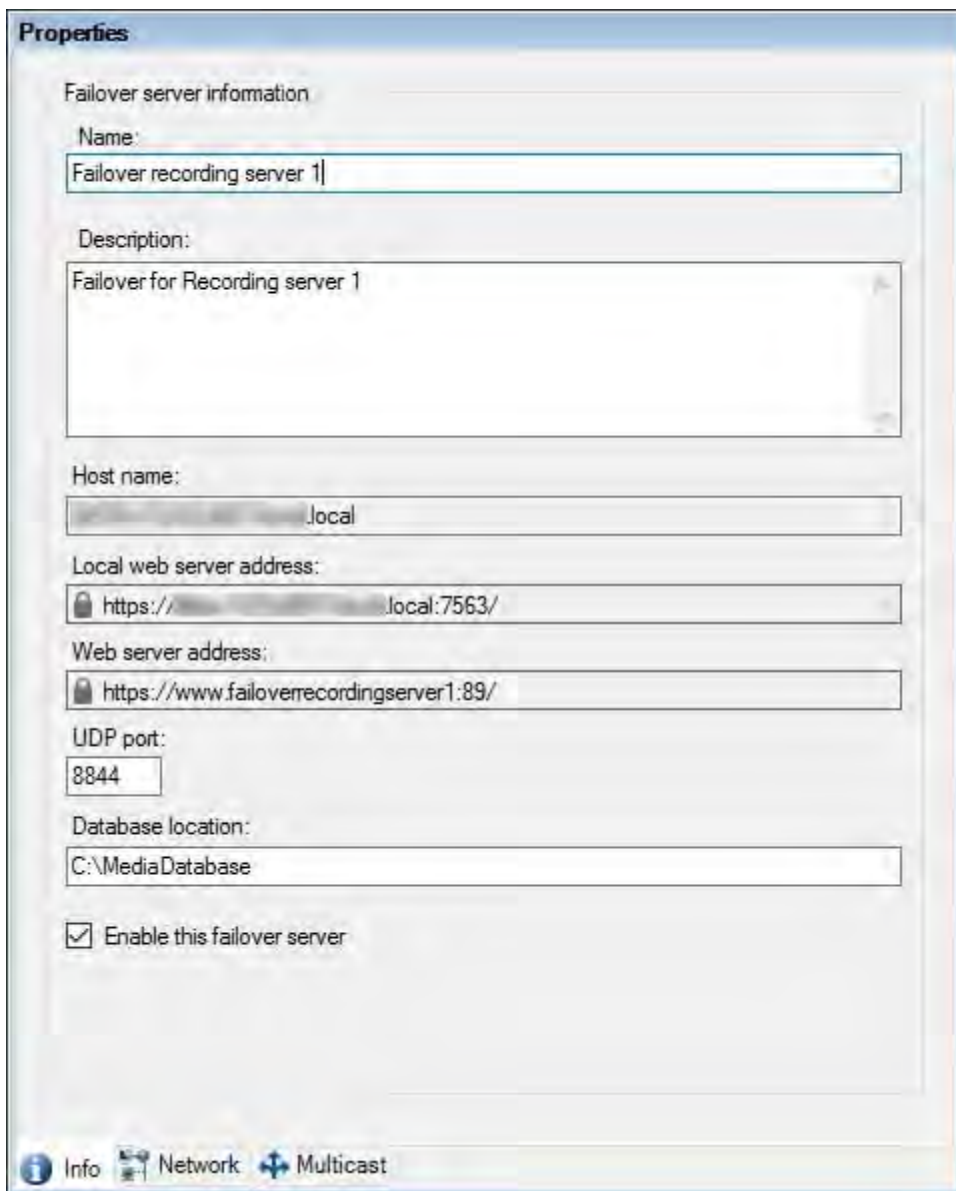


16.4.1 Anzeigen des Verschlüsselungsstatus auf einem Failover-Aufzeichnungsserver

Gehen Sie folgendermaßen vor, um zu überprüfen, ob Ihr Failover-Aufzeichnungsserver Verschlüsselung verwendet:

1. Wählen Sie im **Bereich Webseitennavigation** die Option **Server > Failoverserver aus**. Daraufhin wird eine Liste der Failover-Aufzeichnungsserver geöffnet.
2. Wählen Sie im **Bereich Übersicht** den entsprechenden Aufnahmeserver aus und wechseln Sie zur **Registerkarte Info**.

Wenn die Verschlüsselung für Clients und Server aktiviert ist, die Datenströme vom Aufzeichnungsserver abrufen, wird ein Vorhängeschloss-Symbol vor der Adresse des lokalen Webservers und der optionalen Webserveradresse angezeigt.



Führen Sie dieses Skript einmal aus, um ein Zertifikat zu erstellen, das SSL-Zertifikate mehrerer Server signieren kann

Privates Zertifikat zum Signieren anderer Zertifikate (im Zertifikatsspeicher)

```
$ca_certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -DnsName 'VMS-Zertifizierungsstelle' -KeyUsageProperty All '  
-KeyUsage CertSign, CRLSign, DigitalSignature -FriendlyName 'VMS-CA-Zertifikat' '  
-TextExtension @"(2.5.29.19={kritisch}{text}ca=WAHR)"
```

Fingerabdruck des privaten Zertifikats, das zum Signieren anderer Zertifikate verwendet wird

```
Set-Content -Path "$PSScriptRoot\ca_thumbprint.txt" -Wert $ca_Zertifikat.Fingerabdruck
```

Öffentliches CA-Zertifikat, dem vertraut werden soll (Stammzertifizierungsstellen von Drittanbietern)

```
export-certificate -cert "cert:\CurrentUser\My\${$ca_certificate.Fingerabdruck}" -FilePath "$PSScriptRoot\root-authority-public.cer"
```

```
# Führen Sie dieses Skript einmal für jeden Server aus, für den ein SSL-Zertifikat benötigt wird.
# Das Zertifikat sollte auf dem einzelnen Computer ausgeführt werden, auf dem sich das CA-Zertifikat befindet. # Das erstellte Server-SSL-
Zertifikat sollte dann auf den Server verschoben und in den dortigen Zertifikatsspeicher # importiert werden.
# Erlauben Sie nach dem Importieren des Zertifikats den Zugriff auf den privaten Schlüssel des Zertifikats für # den/die
Dienstbenutzer der Dienste, die das Zertifikat verwenden müssen.

# CA-Zertifikat aus dem Speicher laden (Fingerabdruck muss in ca_thumbprint.txt sein)
$ca_thumbprint = Get-Content -Pfad "$PSScriptRoot\ca_thumbprint.txt"
$ca_zertifikat = (Get-ChildItem -Pfad cert:\CurrentUser\Mein\$ca_Fingerabdruck)

# Benutzer zur Eingabe von DNS-Namen auffordern, die in das Zertifikat aufgenommen werden sollen
$dnsNames = Read-Host 'DNS-Namen für Server-SSL-Zertifikat (durch Leerzeichen getrennt - 1. Eintrag ist auch Gegenstand des Zertifikats)'
$dnsNamesArray = @($dnsNames -Split ' ' | foreach { $_. Trimmen() }) | wobei { $_ }

if ($dnsNamesArray.Length -gt 0) {
    Write-Host -ForegroundColor Red 'Mindestens ein DNS-Name sollte angegeben werden' exit
}
$subjectName = $dnsNamesArray[0]
$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'

# Erlauben Sie dem Benutzer optional, eine Liste von IP-Adressen einzugeben, die in das Zertifikat eingefügt werden sollen
$ipAddresses = Read-Host 'IP-Adressen für Server-SSL-Zertifikat (gelöscht durch Leerzeichen)'
$ipAddressesArray = @($ipAddresses -Teilen ' ' | foreach { $_. Trimmen() }) | where { $_ } if ($ipAddressesArray.Length -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

# Erstellen Sie eine Zeichenfolge für die endgültigen DNS-Einträge (z. B. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={Text}$dnsEntries"

# Der einzige erforderliche Zweck des Zertifikats ist die "Serverauthentifizierung"
$serverAuthentication = '2.5.29.37={kritisch}{Text}1.3.6.1.5.5.7.3.1'

# Erstellen Sie nun das SSL-Zertifikat des Servers
$certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate '
-FriendlyName 'VMS SSL-Zertifikat' -TextExtension @($dnsEntries, $serverAuthentication)

# Zertifikat auf Festplatte exportieren - mit Passwort schützen
$password = Read-Host -AsSecureString "Passwort für das SSL-Zertifikat des Servers"
export-pfxCertificate -cert "cert:\CurrentUser\My\$($certificate.Fingerabdruck)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Kennwort-$password

# Löschen Sie das SSL-Zertifikat des Servers aus dem lokalen Zertifikatsspeicher
$certificate | Artikel entfernen
```

```
# Führen Sie dieses Skript einmal für jeden Management-Server aus, für den ein Zertifikat benötigt wird.
# Das Zertifikat sollte auf dem einzelnen Computer ausgeführt werden, auf dem sich das CA-Zertifikat befindet. # Das erstellte Zertifikat
sollte dann auf die Management-Server verschoben werden und
# in den dortigen Zertifikatsspeicher importiert.

# CA-Zertifikat aus dem Speicher laden (Fingerabdruck muss in ca_thumbprint.txt sein)
$ca_thumbprint = Get-Content -Pfad "$PSScriptRoot\ca_thumbprint.txt"
$ca_Zertifikat = (Get-ChildItem -Pfad cert:\CurrentUser\Mein\$ca_Fingerabdruck)

# Benutzer zur Eingabe von DNS-Namen auffordern, die in das Zertifikat aufgenommen werden sollen
$dnsNames = Read-Host 'DNS-Namen für Management-Server-Zertifikat (komma getrennt - 1. Eintrag ist auch Gegenstand des Zertifikats)'
$dnsNamesArray = @($dnsNames -Split ',' | foreach { $_.Trimmen() } | wobei { $_ })

wenn ($dnsNamesArray. Länge -eq 0) {
    Write-Host -ForegroundColor Red 'Mindestens ein DNS-Name sollte angegeben werden' exit
}

$dnsEntries = ($dnsNamesArray | foreach { "DNS=$_" }) -Join '&'

# Erlauben Sie dem Benutzer optional, eine Liste von IP-Adressen einzugeben, die in das Zertifikat eingefügt werden sollen
$ipAddresses = Read-Host 'IP-Adressen für das Management-Server-Zertifikat (durch Kommas getrennt)'
$ipAddressesArray = @($ipAddresses -Teilen ',' | foreach { $_.Trimmen() } | wobei { $_ }) if ($ipAddressesArray. Länge -gt 0) {
    $ipEntries = ($ipAddressesArray | foreach { "IPAddress=$_" }) -Join '&'
    $dnsEntries = "$dnsEntries&$ipEntries"
}

$subjectName = $ipAddressesArray[0]

# Erstellen Sie eine Zeichenfolge für die endgültigen DNS-Einträge (z. B. "2.5.29.17={text}DNS=myhost&DNS=myhost.domain.com&IPAddress=10.0.0.103")
$dnsEntries = "2.5.29.17={Text}$dnsEntries"

# Der einzige erforderliche Zweck des Zertifikats ist die "Serverauthentifizierung"
$serverAuthentication = '2.5.29.37={kritisch}{Text}1.3.6.1.5.5.7.3.1'

# Erstellen Sie nun das Zertifikat des Management-Servers
$certificate = New-SelfSignedCertificate -CertStoreLocation cert:\CurrentUser\My -Subject $subjectName -Signer $ca_certificate '
-FriendlyName 'VMS-Serverzertifikat' -TextExtension @($dnsEntries, $serverAuthentication)

# Zertifikat auf Festplatte exportieren - mit Passwort schützen
$password = Read-Host -AsSecureString "Kennwort für das Zertifikat des Management-Servers"
export-pfxCertificate -cert "cert:\CurrentUser\My\$($certificate. Fingerabdruck)" -FilePath "$PSScriptRoot\$subjectName.pfx" -Password $password

# Löschen Sie das Zertifikat des Management-Servers aus dem lokalen Zertifikatsspeicher
$certificate | Artikel entfernen
```

MOBOTIX

BeyondHumanVision

EN_03/25-Ärmel

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com •
www.mobotix.com

MOBOTIX ist eine Marke der MOBOTIX AG, die in der Europäischen Union, den USA und in anderen Ländern eingetragen ist. Änderungen ohne vorherige Ankündigung vorbehalten. MOBOTIX übernimmt keine Haftung für technische oder redaktionelle Fehler oder Auslassungen. Alle Rechte vorbehalten. © MOBOTIX AG 2025