Erstellung eigener Zertifikate.

WinCC (TIA Portal) / V15.1 / Sm@rtService

https://support.industry.siemens.com/cs/ww/de/view/109763500

Siemens Industry Online Support

Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (www.siemens.com/nutzungsbedingungen).

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter http://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 Einleitung

1.1 Übersicht

Für die Fernbedienung von HMI Bediengeräten über Sm@rtClient, muss die Datensicherheit bei der Übertragung übers Internet gewährleistet sein.

Hierzu werden Client- und Server-Zertifikate installiert.

Client- und Server-Zertifikate

Es können zwei Arten von Zertifikaten eingesetzt werden.

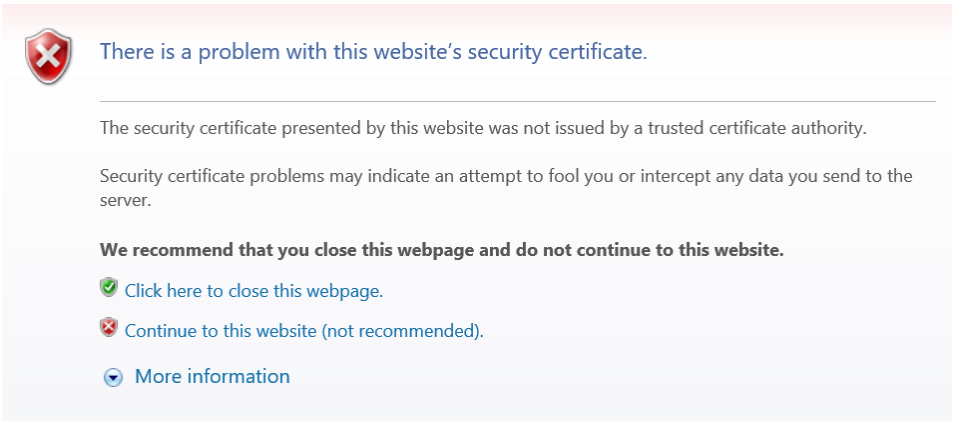
- Automatisch generiertes Zertifikat.
  (Vom Bediengerät automatisch generiertes Zertifikat).
- Selbst signiertes Zertifikat.
  (Selbstsignierte Zertifikate sind Zertifikate, dessen Signatur vom Zertifikatsinhaber stammt und nicht von einer unabhängigen Zertifizierungsstelle).

Dieser FAQ beschreibt eine Möglichkeit, wie Sie ein eigenes signiertes Zertifikat erstellen können.

Typische Warnmeldung beim Zugriff auf den Sm@rtServer

Die nachfolgende Abbildung zeigt eine typische Meldung, wenn z. B. das Zertifikat nicht vorhanden ist oder nicht erkannt wurde.

Abbildung 1-1



Ist die Kopfzeile nach dem Aufruf des Sm@rtServers rot hinterlegt, ist das ebenfalls ein Indiz für ein nicht vorhandenes bzw. fehlerhaftes Zertifikat.

Abbildung 1-2

1.2 Kurzanleitung

Die nachfolgende Anleitung beschreibt die Vorgehensweise, wenn bereits ein Zertifikat vorhanden ist.

- Die eigenen Zertifikate müssen als Datei mit dem Namen "SmartServer.pfx" bzw. SmartServer.p12 gespeichert werden.
- Auf den Bediengeräten mit Windows CE werden diese Datei unter \flash\simatic,
- auf PCs unter \ProgramData\Siemens\CoRtHmiRTm\SmartServer abgelegt.
- Importieren Sie das Zertifikat über den Dialog "Sm@rtServer" in den Zertifikatspeicher des Bediengeräts und installieren Sie das zugehörige Client-Zertifikat in Ihrem Webbrowser.

Zertifikat in den Zertifikatsspeicher des Bediengeräts importieren:

1. Öffnen Sie die "WinCC Internet Settings".
2. Wählen Sie in der Kopfzeile "Remote".
3. Betätigen Sie die Schaltfläche "Change Settings".
4. Wählen Sie das Register "Certificate".
5. Klicken Sie auf die Schaltfläche "Import".

Nach dem Import wird die Datei SmartServer.pfx gelöscht. Die Zertifikate werden im Zertifikatspeicher auf dem Bediengerät unter My Certificates und auf dem PC unter WinCC Panel RT VNC Service abgelegt.

2 Selbstsignierte Zertifikate erstellen

2.1 Voraussetzungen

Java Version

Abhängig von der verwendeten WinCC (TIA Portal), muss die zugehörige Java Version installiert sein. Ist das nicht der Fall, dann passen Sie die Version entsprechend an (ist die verwendete Java Version höher als vorgegeben, dann muss diese zuvor deinstalliert werden).

WinCC (TIA Portal) < 15.1 ➔ Java V8 < update 171

WinCC (TIA Portal) ab 15.1 ➔ Java V8, alle updates

Hinweis Ältere Java-Update Versionen finden Sie im Internet (z. B. unter https://www.filehorse.com/).

Internet Browser

Verwenden Sie für die Anwendung den "Microsoft Internet Explorer".

2.2 Software-Tool "XCA"

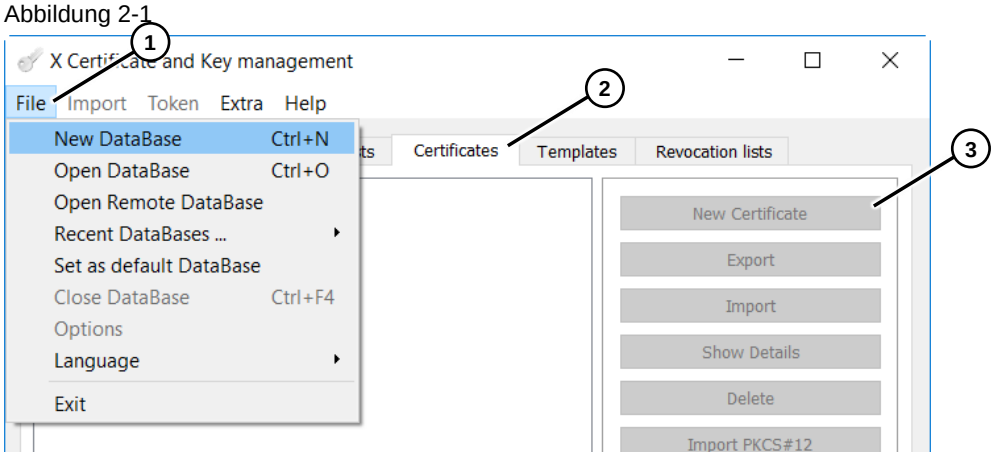
Es gibt verschiedene Softwareanbieter zum Erstellen von selbstsignierten Zertifikaten. In diesem Fall wird das Software Tool "**XCA**" verwendet und die Vorgehensweise zum Erstellen von Zertifikaten beschrieben.

Hinweis Die Bedienoberfläche des Software-Tools "XCA" kann für verschiedene Sprachen umgestellt werden. Die Übersetzungen der abgebildeten Funktionen sind teilweise falsch übersetzt.

Zertifikat erstellen

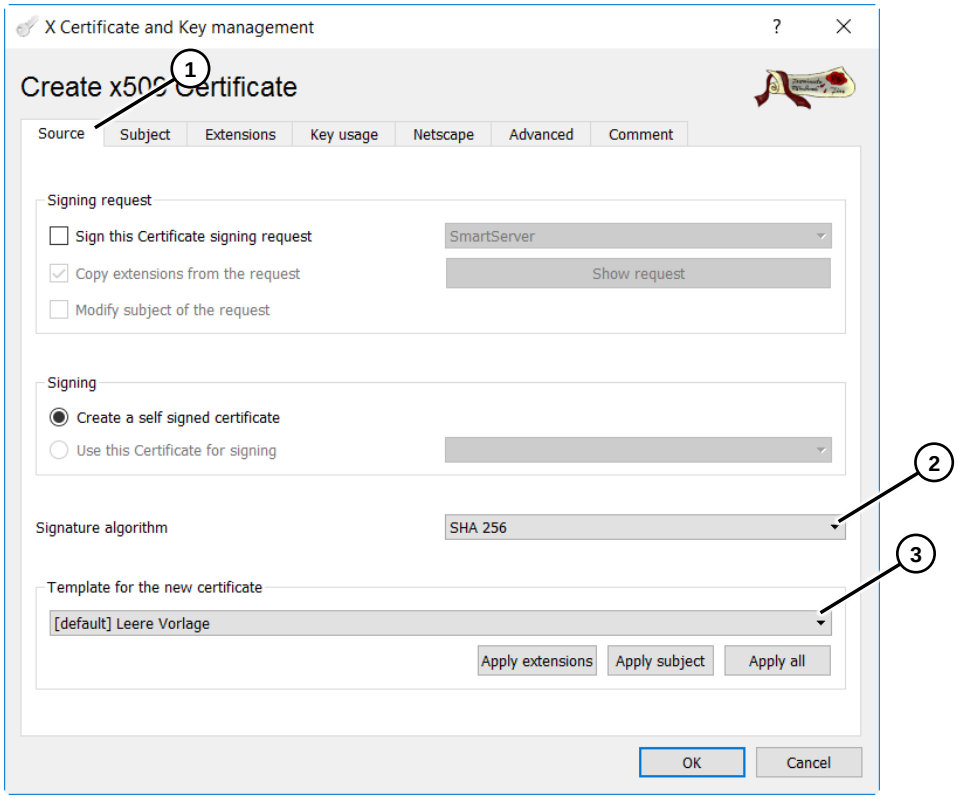
1. Öffnen Sie das Tool "XCA" und erstellen Sie eine neue Datenbank. (Register "Datei > Neue Datenbank". Folgen Sie anschließend den Anweisungen) (1).
2. Wählen Sie in der Menüleiste "Zertifikate" an (2).
3. Betätigen Sie die Schaltfläche "Neues Zertifikat" (3).

Abbildung 2-1



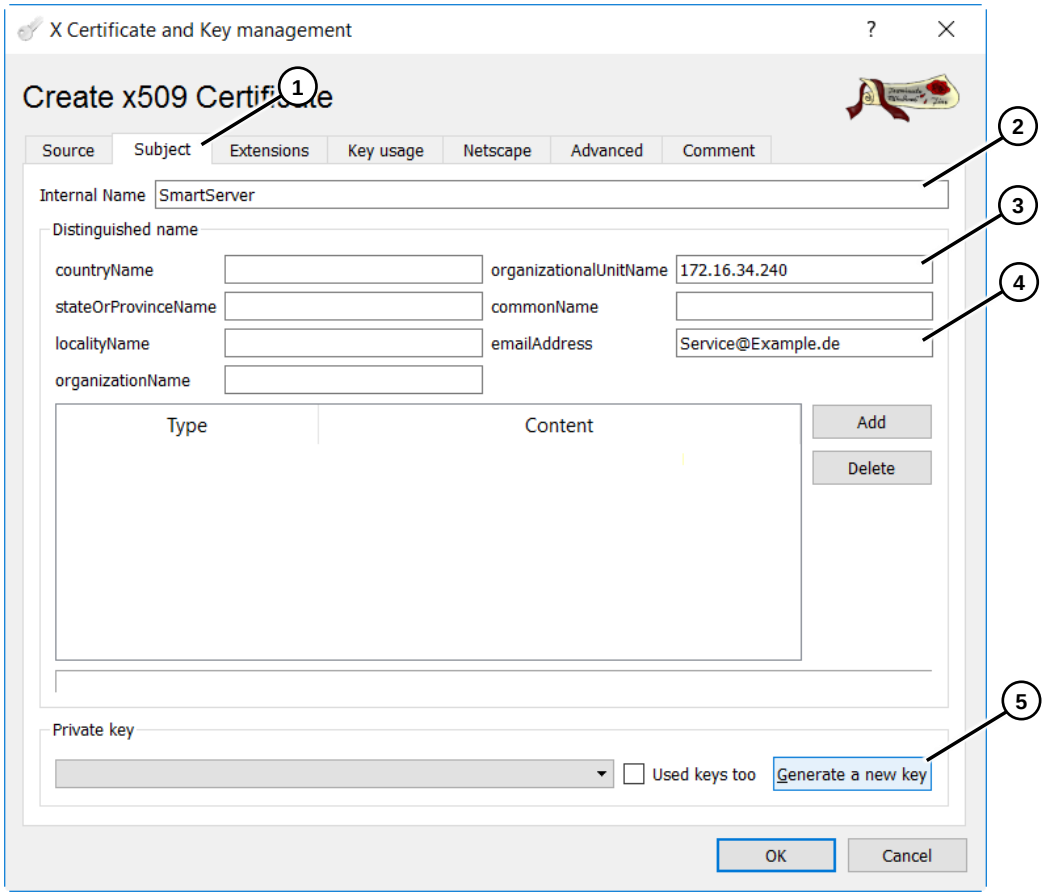
4. Register "Inhaber" (1).
   Wählen Sie die abgebildeten Einstellungen.
   - Signatur Algorithmus: SHA 256 (2)
   - Vorlage für das neue Zertifikat: Default (leere Vorlage) (3)

Abbildung 2-2



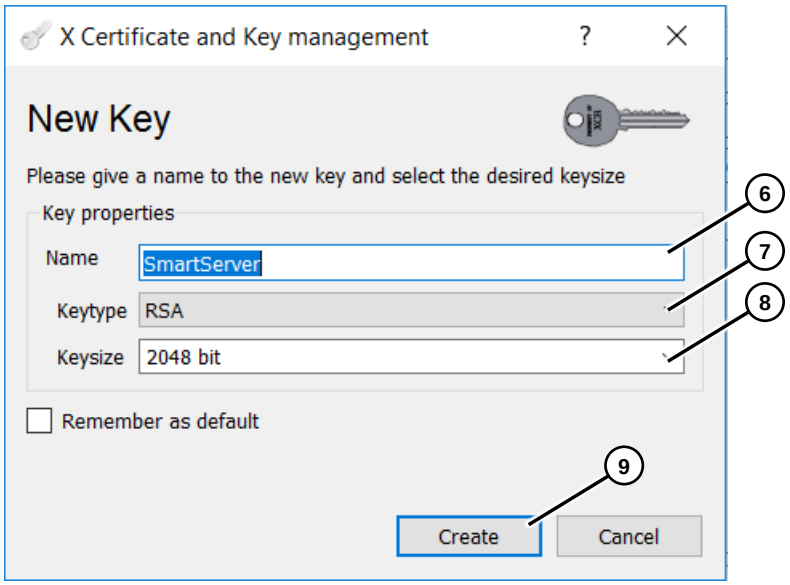
5. Register "Herkunft" (1).
   Wählen Sie die abgebildeten Einstellungen.
   - Interner Name: Tragen Sie hier den Namen des Zertifikats ein. Dieser muss in diesem Fall "**SmartServer**" heißen (2).
   - OrganizationalUnitName: Tragen Sie hier die IP-Adresse des Bediengeräts ein (3).
   - emailAddress: Optional, geben Sie hier eine eMail Adresse an (4).

Abbildung 2-3



- Betätigen Sie die Schaltfläche "Erstelle einen neuen Schlüssel" (5). Es öffnet sich das nachfolgende Fenster.

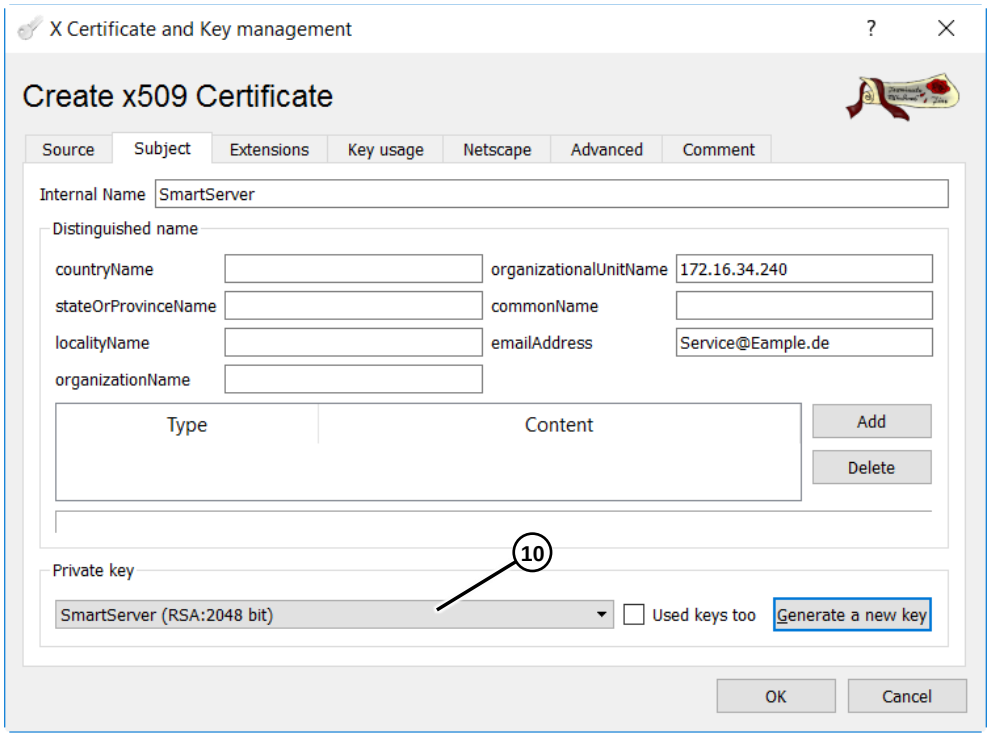
Abbildung 2-4



- Name: Der Name wird automatisch übernommen. Verändern Sie diesen nicht (6).
- Schlüsseltyp: RSA (7).
- Schlüssellänge: 2048 bit (8).
- Betätigen Sie die Schaltfläche "Erstellen" (9). Es wird ein neuer Schlüssel erstellt.

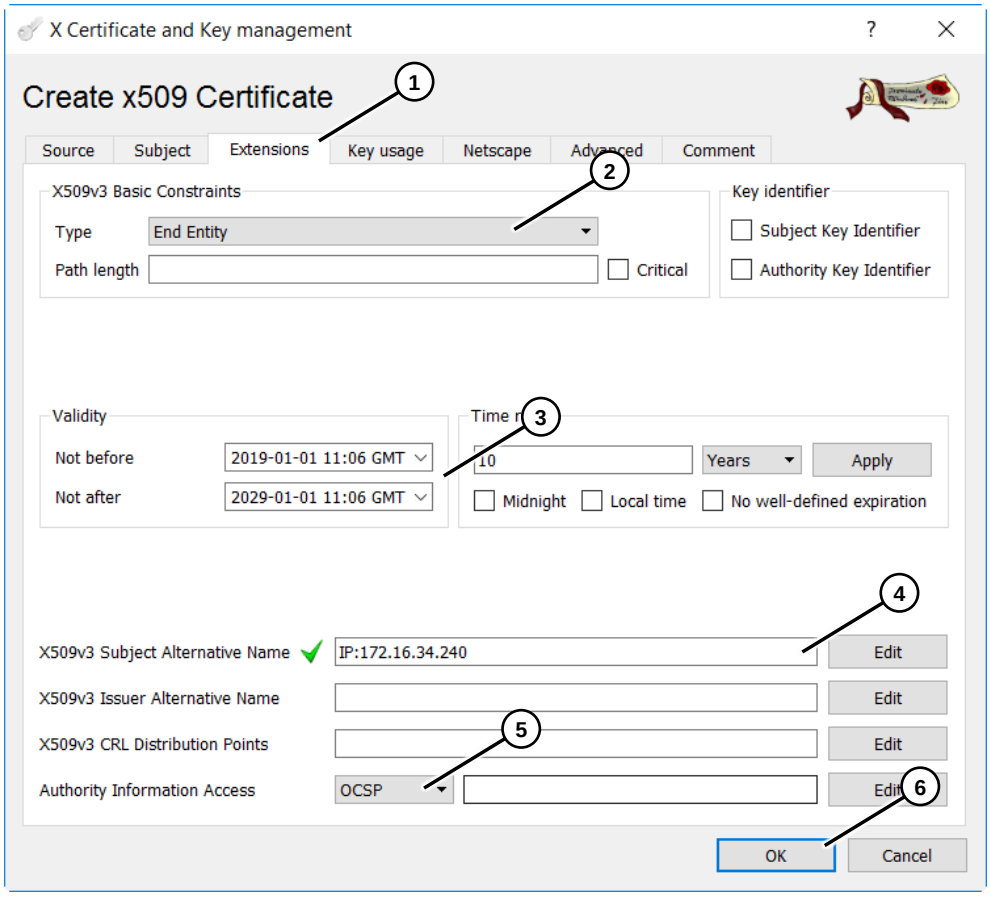
Sie gelangen wieder auf die Seite "Inhaber". Unter dem Punkt "Privater Schlüssel", wird der neu angelegte Schlüssel angezeigt (10).

Abbildung 2-5



6. Register "Erweiterungen" (1).
   Wählen Sie die abgebildeten Einstellungen.
   - Typ: Wählen Sie die Option "End Instanz" (2).
   - Gültigkeit / Zeitspanne: Geben Sie hier an, wie lange das Zertifikat gültig sein soll. Geben Sie hierzu den Beginn und das Enddatum ein (3).
   - X509v3 Subject Alternative Name: Optional, tragen Sie hier die IP-Adresse des Bediengeräts ein. Das Wort "**IP:**" muss mit aufgeführt werden (4).
   - Authority Information Access: Wählen Sie hier die Option "OSCP" aus (5).

Abbildung 2-6

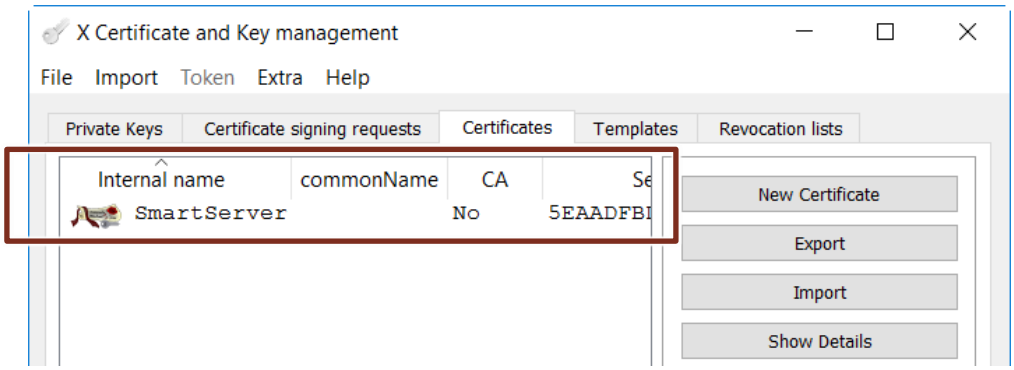


In den Registern "Schlüsselverwendung", "Netzscape", "Erweitert" und "Kommentar" müssen keine Einträge/Anpassungen vorgenommen werden.

- Schließen Sie die Eingaben über die Schaltfläche "OK" ab (6).

Ansicht des neu erstellten Zertifikats.

Abbildung 2-7

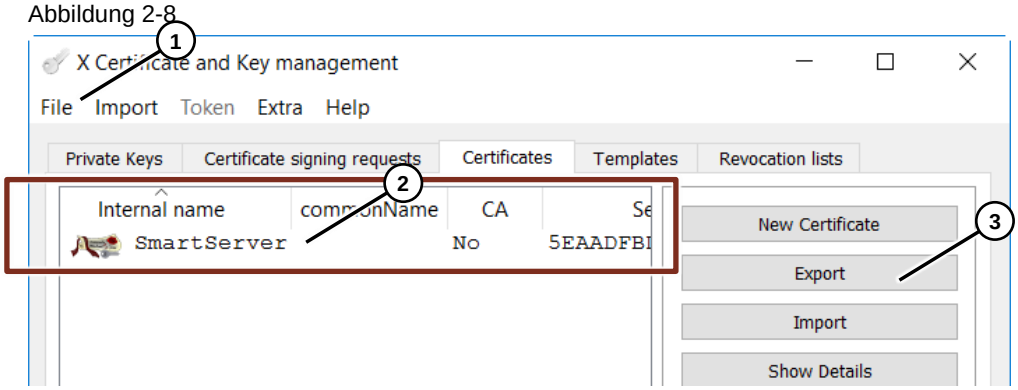


Zertifikat Exportieren

Um das Zertifikat ins Bediengerät importieren zu können, muss zunächst das Zertifikat exportiert werden.

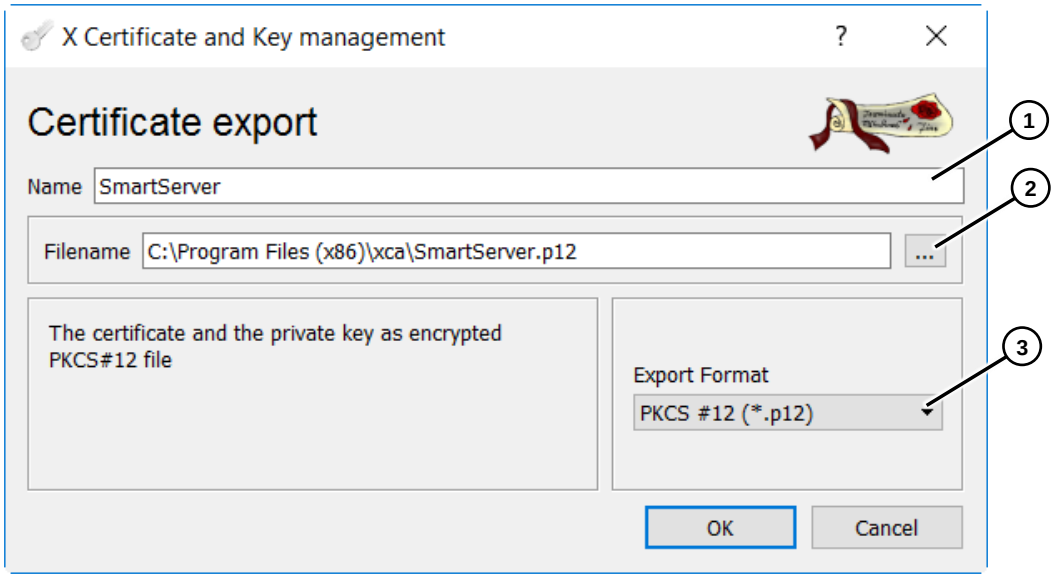
1. Öffnen Sie das Tool "XCA".
2. Öffnen Sie die Bibliothek, in dem das Zertifikat hinterlegt ist.
   Menüleiste: "Datei > Datenbank öffnen (1).
3. Markieren Sie das zu exportierende Zertifikat (2).
4. Betätigen Sie die Schaltfläche "Export" (3).
   Das Fenster "Zertifikat Export" wird geöffnet.

Abbildung 2-8



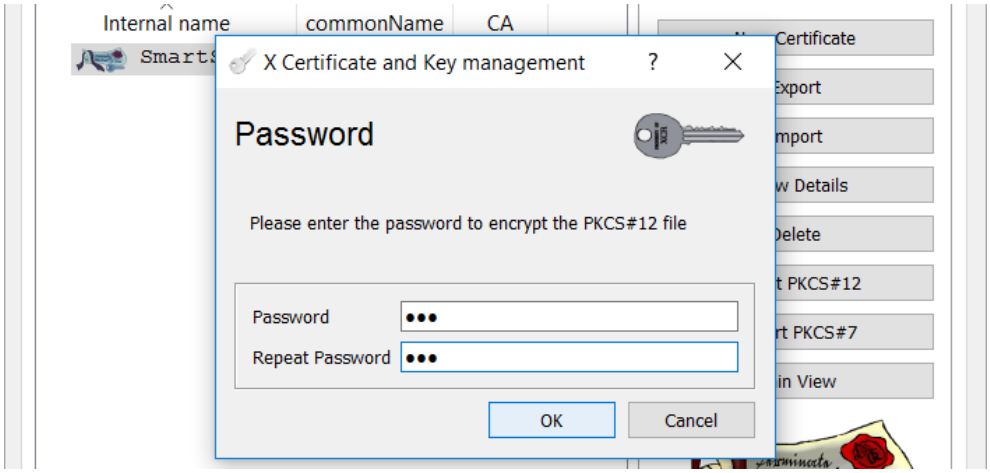
5. Fenster "Zertifikat Export"
   - Name: Der Name wird automatisch übernommen. Verändern Sie diesen nicht (1).
   - Dateipfad: Geben Sie den Ablagepfad für das Zertifikat an (2).
   - Export Format: Wählen Sie hier über die Klappliste das Format "**PKCS #12 (*.p12)**" an (3).
   - Bestätigen Sie die Angaben mit "OK". Es wird ein Fenster mit einer Passwortabfrage eingeblendet.

Abbildung 2-9



6. Fenster Passwortabfrage
   - Geben Sie ein Passwort vor. Das Passwort, das Sie hier vergeben, wird später beim Import des Zertifikats am Bediengerät und dem MS Internet Explorer abgefragt. In diesem Beispiel "100".
   - Bestätigen Sie die Angaben mit "OK".

Abbildung 2-10



Damit ist der Export des Zertifikats abgeschlossen.

3 Zertifikat in den PC-Zertifikatsordner einfügen

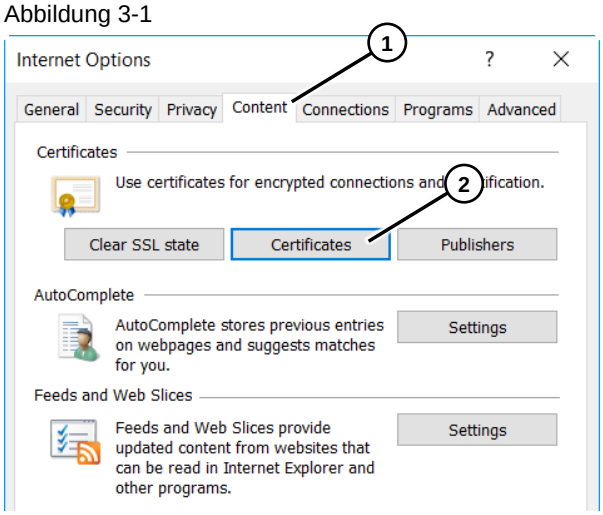
Zum Einfügen des Zertifikats in den Zertifikatsordner des Windows PCs, können Sie die Oberfläche des Internet Explorers verwenden oder die Microsoft Management Console (MMC).

In diesem Beitrag wird die Vorgehensweise bei der Verwendung des MS Internet Explorers gezeigt.

MS Internet Explorer

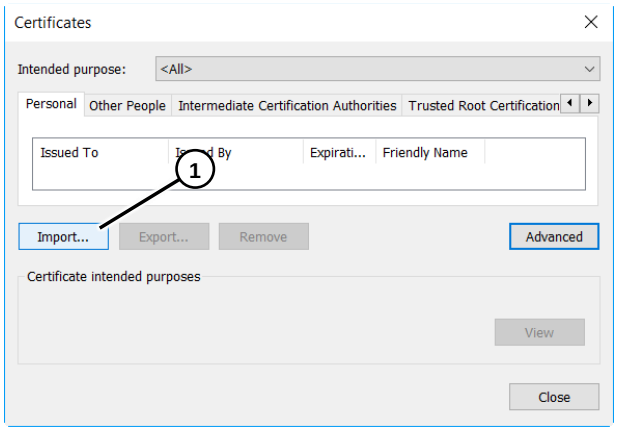
1. Rufen Sie die Internetoptionen des MS Internet Explorer auf und wählen Sie in der Menüleiste "Inhalte" an (1).
2. Betätigen Sie unter Zertifikate die Schaltfläche "Zertifikate" (2).

Abbildung 3-1



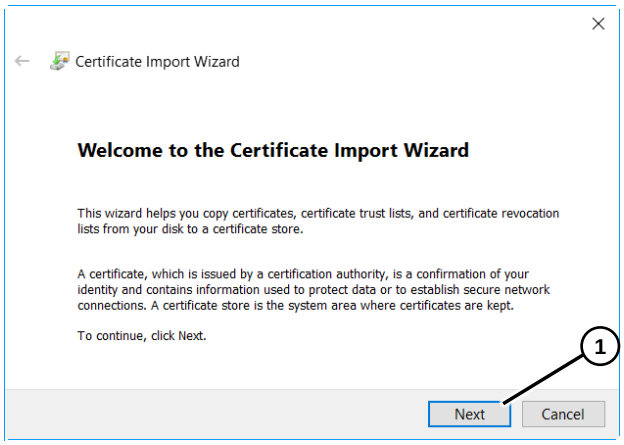
3. Klicken Sie auf die Schaltfläche "Import…" (1).

Abbildung 3-2



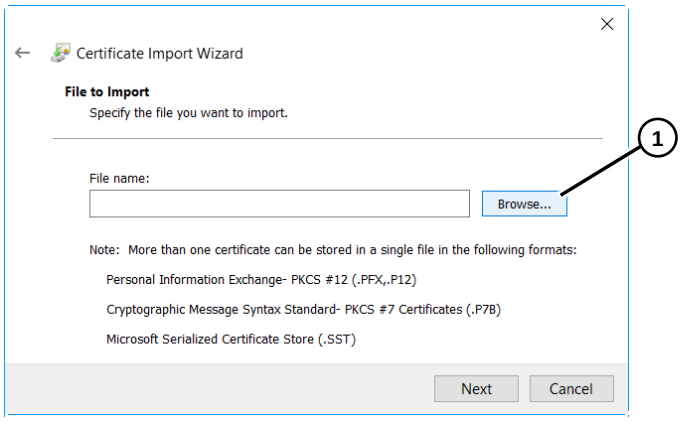
4. Klicken Sie auf die Schaltfläche "Weiter" (1).

Abbildung 3-3



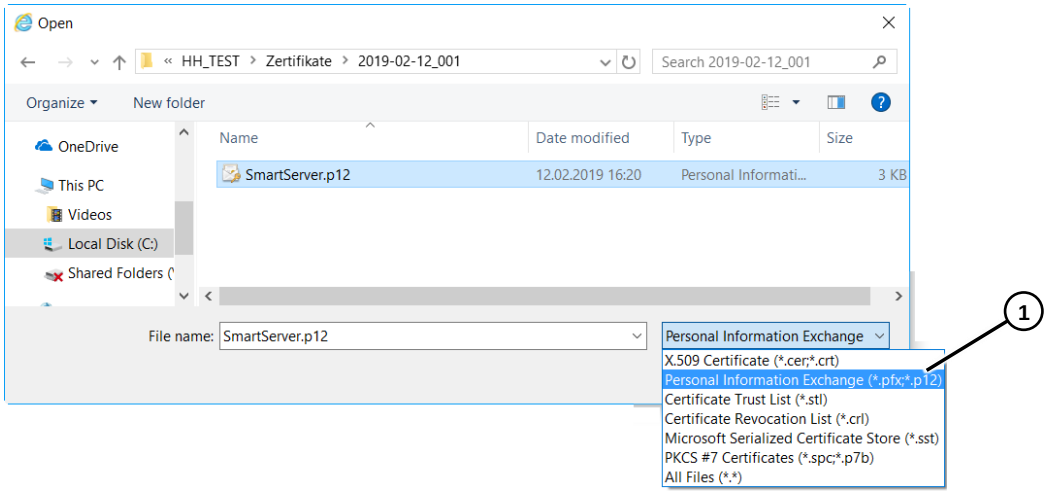
5. Klicken Sie im nächsten Bild auf die Schaltfläche "Durchsuchen…" (1).

Abbildung 3-4



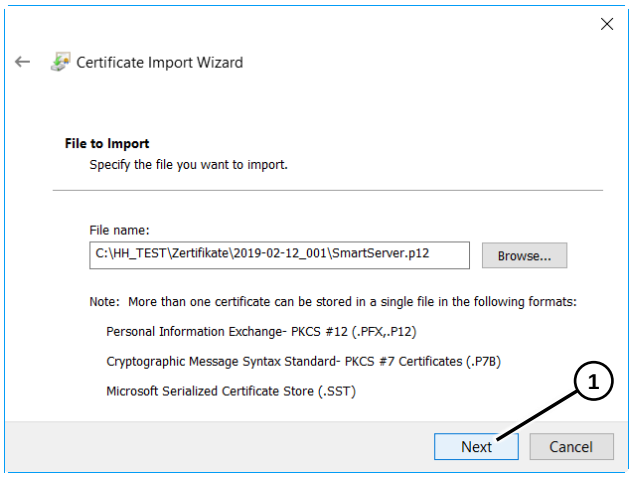
6. und navigieren Sie zu dem Pfad, in der das Zertifikat gespeichert ist.
   Hinweis:
   Achten Sie darauf, dass Sie vorher das Dateiformat "*:p12" anwählen (1).

Abbildung 3-5



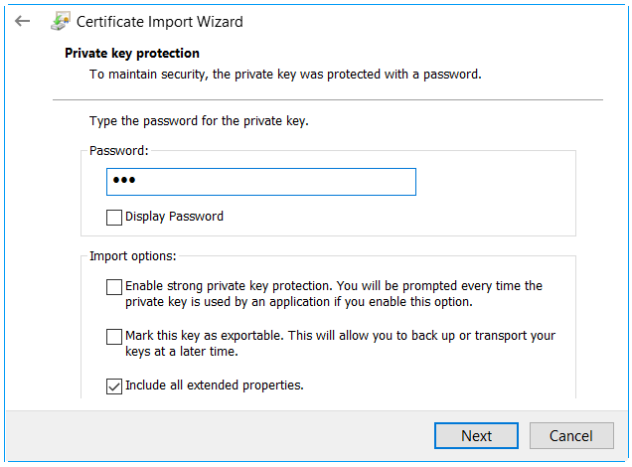
7. Klicken Sie auf die Schaltfläche "Weiter" (1).

Abbildung 3-6



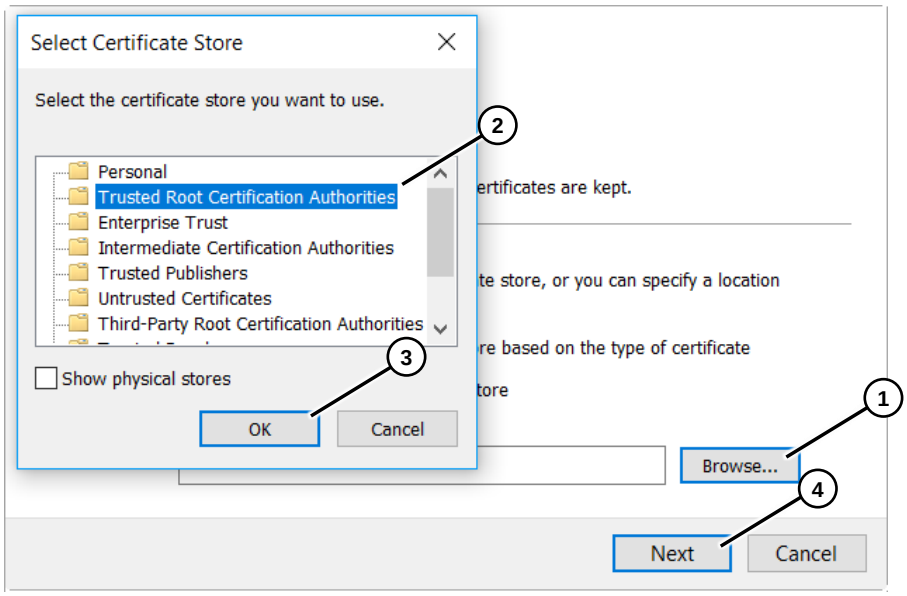
8. Geben Sie das Passwort an, dass Sie bei der Parametrierung des Zertifikats vergeben haben. In diesem Fall "100". Klicken Sie anschließend auf "Weiter".

Abbildung 3-7



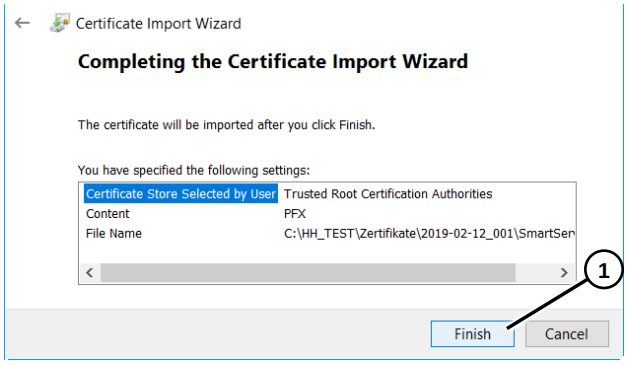
9. Klicken Sie auf die Schaltfläche "Durchsuchen…" (1).
10. Wählen sie in dem Zertifikatsspeicher den Ordner "Vertrauenswürdige Stammzertifizierungsstellen" an (2).
11. Bestätigen Sie die Angabe mit "OK" (3).
12. Klicken sie auf die Schaltfläche "Weiter" (4).

Abbildung 3-8



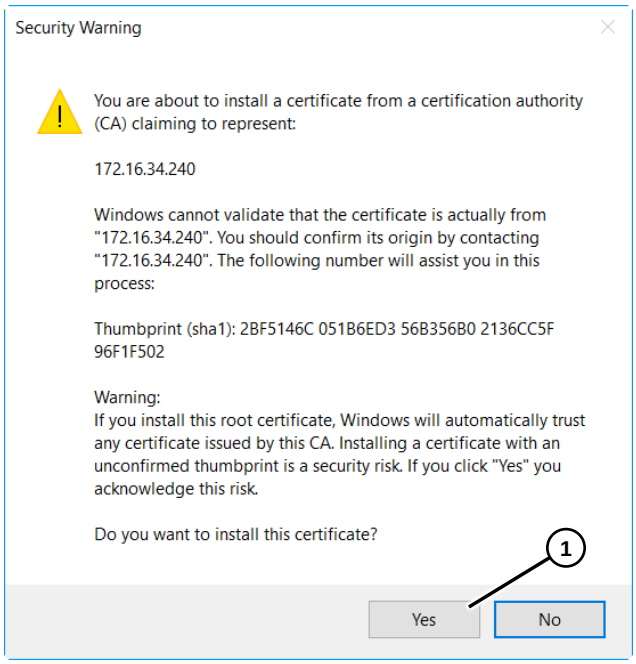
13. Klicken sie auf die Schaltfläche "Fertig stellen" (1).

Abbildung 3-9



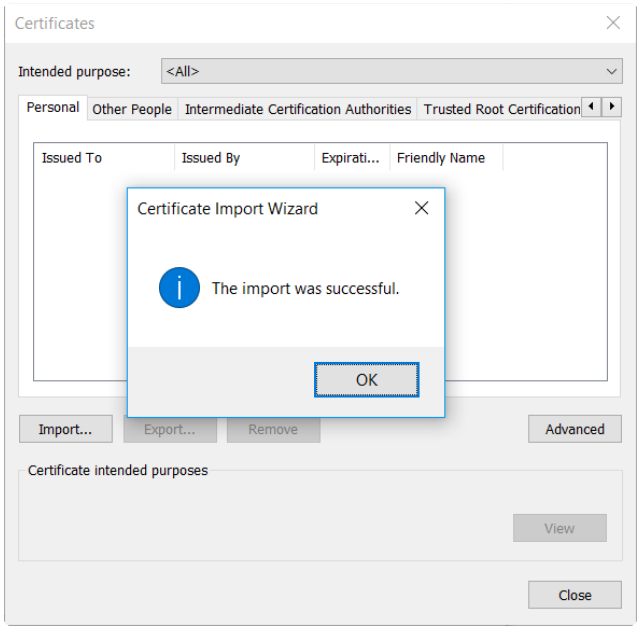
14. Es wird eine Sicherheitswarnung zum Installieren des Zertifikats eingeblendet. Bestätigen Sie in diesem Fall die Meldung mit "Ja" (1).

Abbildung 3-10



Damit ist die Installation des Zertifikats in den Zertifikatsspeicher abgeschlossen.

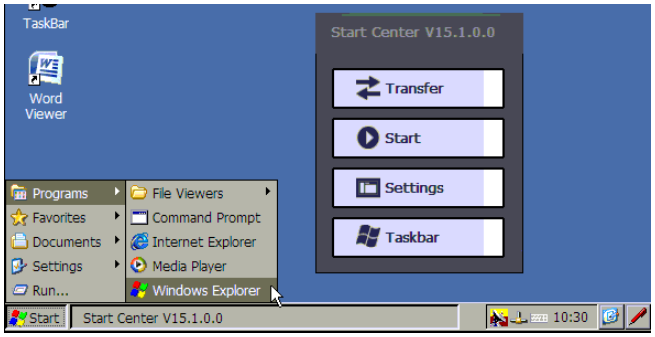
Abbildung 3-11



4 Zertifikat auf das Bediengerät übertragen

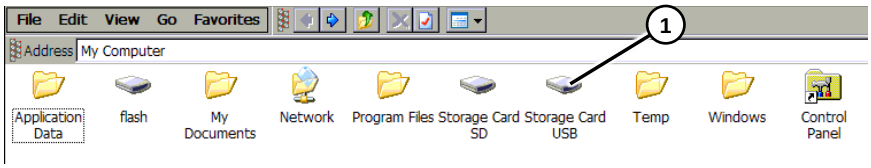
1. Kopieren Sie das erstellte Zertifikat auf einen USB-Stick.
2. Stecken Sie den USB-Stick an das Bediengerät an.
3. Prüfen Sie am Bediengerät den "Windows Explorer" auf.
   Klicken Sie im "Start Center" auf "Taskbar > Programs > Windows Explorer".

Abbildung 4-1



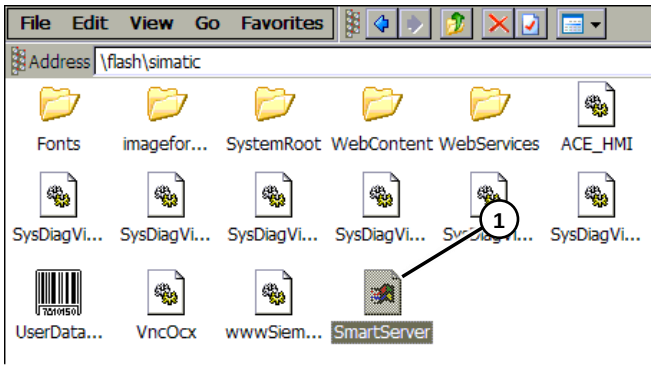
4. Wählen Sie das Laufwerk "Storage Card USB" an (1) und kopieren Sie das Zertifikat "SmartServer" (Edit > Copy).

Abbildung 4-2



5. Fügen Sie das kopierte Zertifikat in den Ordner "flash > simatic" ein (Edit > Paste). Ansicht des eingefügten Zertifikats (1).

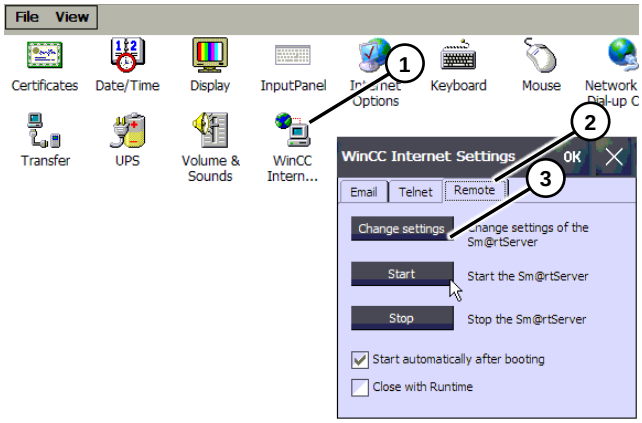
Abbildung 4-3



6. Schließen Sie alle Fenster und öffnen Sie über das "Start Center" die "Settings" des Bediengeräts.
7. Öffnen Sie die Anwendung "WinCC Internet Setting" (1).
   Es öffnet sich das Menü-Bild "WinCC Internet Settings".
8. Wählen Sie in der Menüleiste "Remote" an (2).

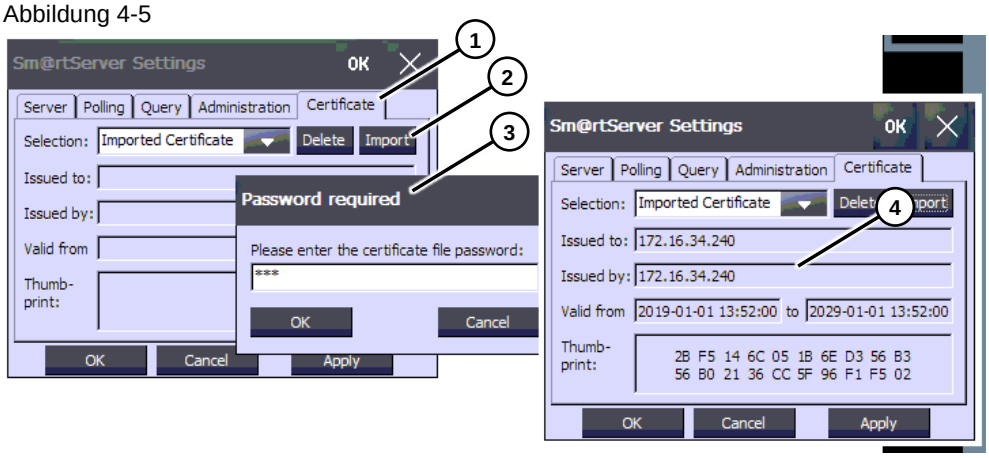
9. Klicken Sie auf die Schaltfläche "Change settings" (3).
   Es öffnet sich das Menü-Bild "Sm@rtServer Settings".

Abbildung 4-4



10. Wählen Sie in der Menüleiste "Certificate" (1).
11. Klicken Sie auf die Schaltfläche "Import" (2).
    Es erscheint ein Bild mit einer Passwortabfrage (3).
    Tragen Sie hier das Passwort ein, dass Sie bei der Erstellung des Zertifikats vergeben haben ein. In diesem Fall "100".
12. Bestätigen Sie die Eingabe mit "OK".
13. Das Zertifikat ist jetzt auf dem Bediengerät in "Certificates" hinterlegt (4).

Abbildung 4-5



Schließen Sie den Import über die Schaltfläche "OK" ab und schließen Sie alle Fenster.

5 Zertifikate löschen

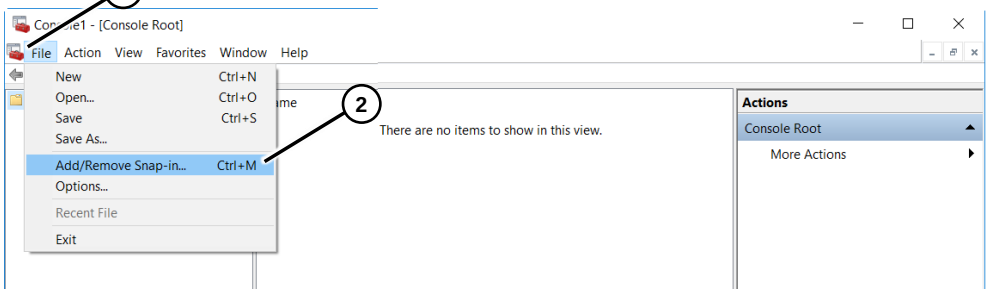
MMC Tool

Mit der Microsoft Management Console (MMC) können Sie auf einfache Weise Zertifikate verwalten. Mit dem Tool können Sie z. B.

- Zertifikate einfügen
- Zertifikate löschen
- Zertifikate sichern.

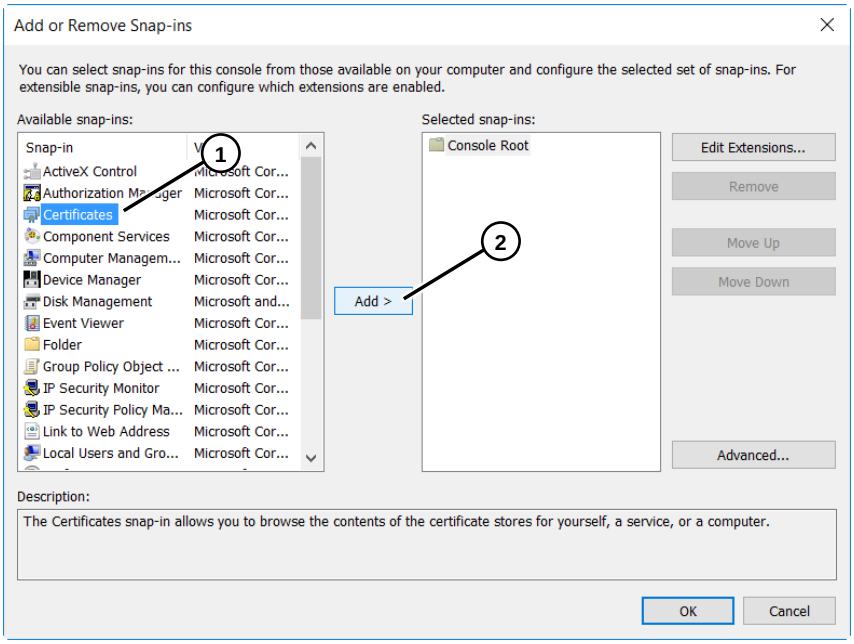
1. Rufen Sie das MMC Tool auf.
   - Windows durchsuchen > MMC.
2. Öffnen Sie über die Menüleiste die Funktion "Snap-In hinzufügen/entfernen". "Datei > Snap-In hinzufügen/entfernen".

Abbildung 5-1



3. Markieren Sie in der linken Spalte das "Snap-In" "Zertifikate" (1).
4. Betätigen Se die Schaltfläche "Hinzufügen >" (2). Es öffnet sich ein Fenster, in dem Sie die Rechte festlegen. Schließen Sie Eingabe mit "Fertig stellen" ab.
5. Bestätigen Sie die Angaben mit "OK".

Abbildung 5-2



1. Im verzeichnisbaum werden die einzelnen Zertifikatsordner angezeigt. Unter dem Ordner "Trusted Root Certification Authorities" befindet das Panel-Zertifikat (1).
2. Markieren Sie das zu löschende Zertifikat mit der rechten Maustaste. Über das Kontextmenü wählen Sie die auszuführenden Funktionen aus (2).

Abbildung 5-3