SIEMENS

Ingenuity for life

Creating Your Own Certificates

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

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

Siemens Industry Online Support

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase the customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Contents

1 Introduction

1.1 Overview

Data security when transferring via the internet must be ensured for the remote control of HMI operator panels via Sm@rtClient.

Client and server certificates are installed for this.

Client and server certificates

You can use two types of certificate.

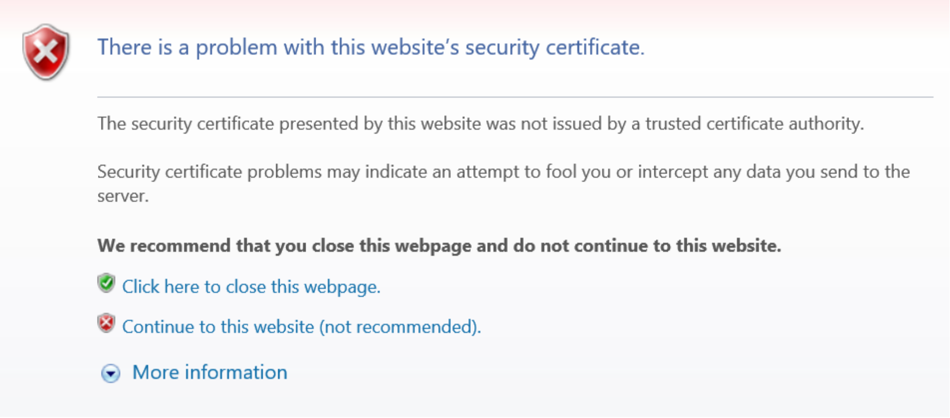
- Automatically generated certificate.
  (A certificate generated automatically by the operator panel).
- Self-signed certificate.
  (A self-signed certificate is a certificate whose signature comes from the certificate holder and not from an independent certification authority).

This FAQ response describes one way of creating your own signed certificate.

Typical warning message when accessing the Sm@rtServer

The following figure shows a typical message that is displayed if the certificate is not available or if it is not recognized.

Figure 1-1



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

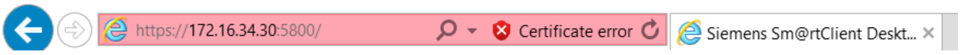
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

If, after calling the Sm@rtServer, the header has a red background, this indicates that a certificate is not available or is incorrect.

Figure 1-2



1.2 Brief Instructions

The following instructions describe how to proceed if a certificate is already present.

- Your own certificates must be stored as a file with the name "SmartServer.pfx" or "SmartServer.p12".
- On HMI devices with Windows CE, this file is saved under \flash\simatic.
- On PCs, it is saved under \ProgramData\Siemens\CoRtHmiRTm\SmartServer.
- You import the certificate to the certificate store using the "Sm@rtServer" dialog and
  install the corresponding client certificate in your web browser.

Importing the certificate into the certificate store of the operator panel:

1. Open "WinCC Internet Settings".
2. In the header you select "Remote".
3. Click the "Change Settings" button.
4. Select the "Certificate" tab.
5. Click the "Import" button.

After the import the SmartServer.pfx file is deleted. The certificates are stored in the certificate store on the operator panel under My Certificates and on the PC under WinCC Panel RT VNC Service.

2 Creating Self-signed Certificates

2.1 Requirements

Java version

The version of Java installed must correspond to the WinCC (TIA Portal) being used. If not, then modify the version accordingly (if the version of Java being used is higher than specified, then you have to uninstall it beforehand).

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

WinCC (TIA Portal) 15.1 and higher ➔ Java V8, all updates

Note Older versions of Java are available in the internet (under https://www.filehorse.com/, for example).

Internet browser

Use the "Microsoft Internet Explorer" for the application.

2.2 Software Tool "XCA"

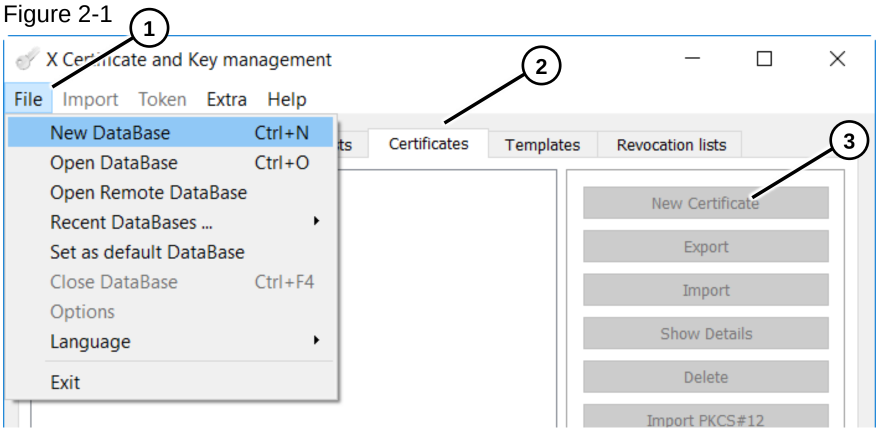
There are different software tools for creating self-signed certificates. In this case we are using the software tool "**XCA**" and procedure for creating certificates.

Note The user interface of the software tool "XCA" can be changed for different languages. The translations of the functions shown are partially translated incorrectly.

Create a certificate

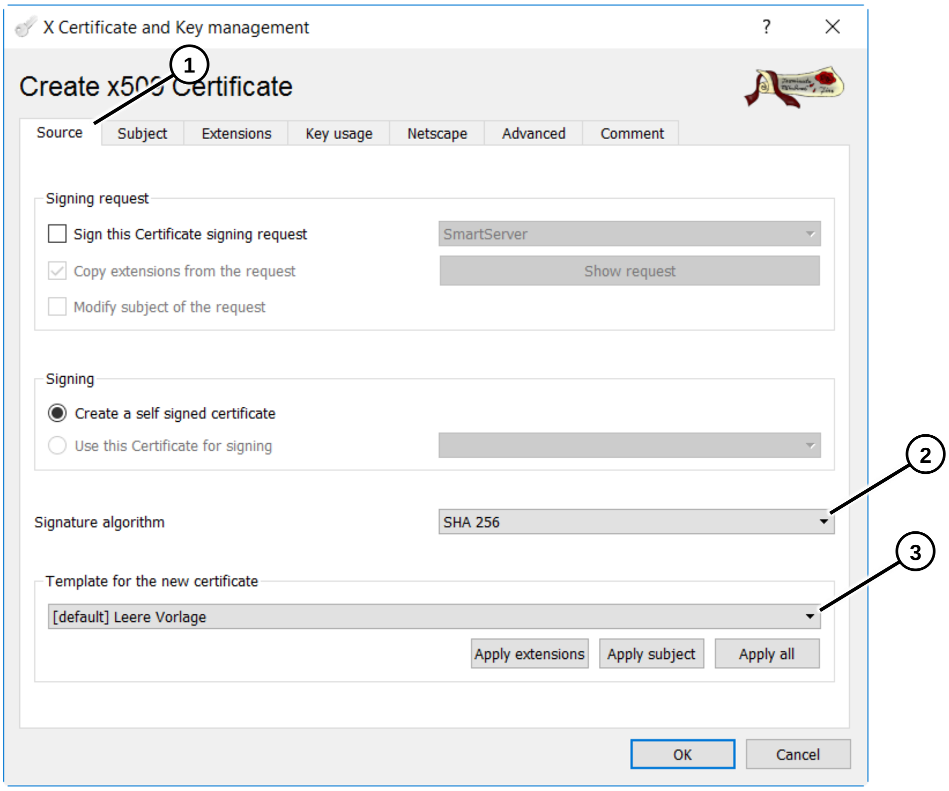
1. Open the "XCA" tool and create a new database.
   (Tab "File > New Database". Then follow the instructions) (1).
2. In the menu bar you select "Certificates" (2).
3. Click the "New Certificate" button (3).

Figure 2-1



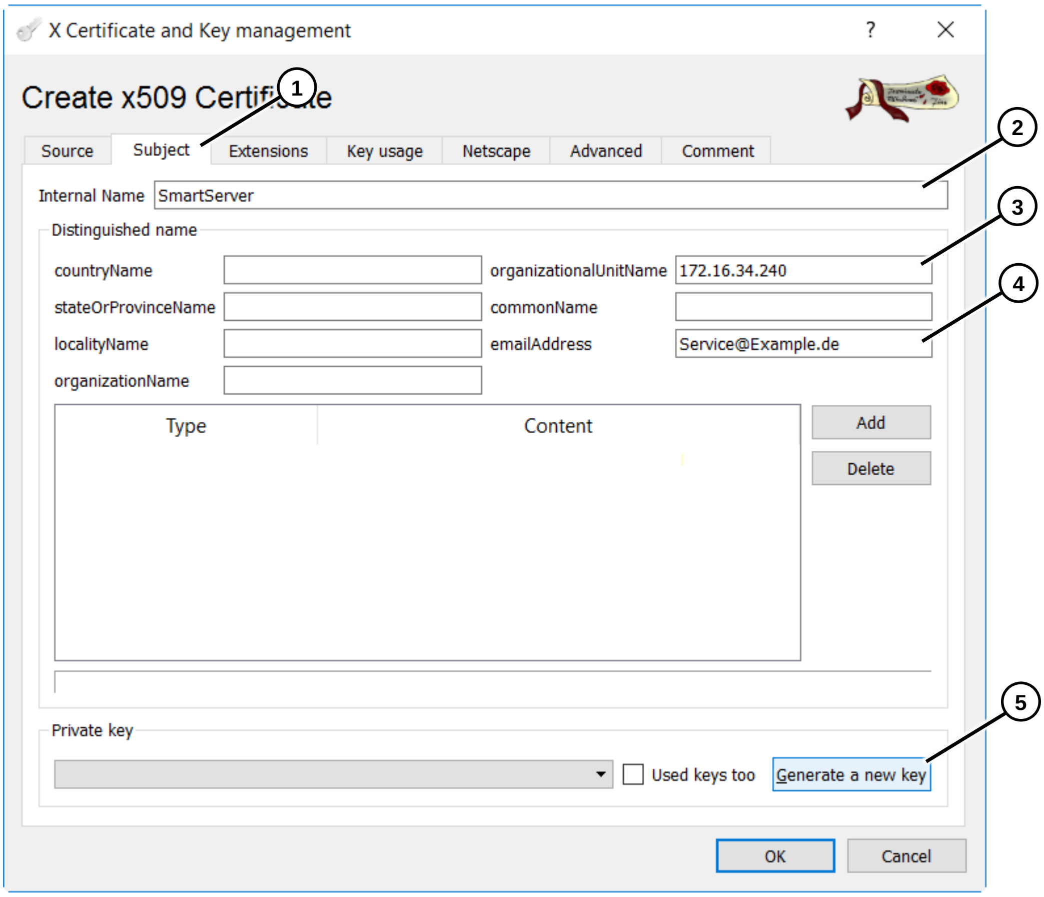
4. Tab "Source" (1).
   Select the settings shown.
   - Signature algorithm: SHA 256 (2)
   - Template for the new certificate: Default (empty template) (3)

Figure 2-2


1
2
3
X Certificate and Key management
?
Create x509 Certificate
Source
Subject
Extensions
Key usage
Netscape
Advanced
Comment
Signing request
□ Sign this Certificate signing request
SmartServer
☑ Copy extensions from the request
Show request
□ Modify subject of the request
Signing
● Create a self signed certificate
○ Use this Certificate for signing
Signature algorithm
SHA 256
Template for the new certificate
[default] Leere Vorlage
Apply extensions
Apply subject
Apply all
OK
Cancel

5. Tab "Subject" (1).
   Select the settings shown.
   - Internal Name: Here you enter the name of the certificate. In this case it must be "**SmartServer**" (2).
   - Organizational Unit Name: Here you enter the IP address of the operator panel (3).
   - Email Address: You have the option of entering an e-mail address here (4).

Figure 2-3



X Certificate and Key management

Create x509 Certificate

Internal Name: SmartServer

Distinguished name

countryName:

stateOrProvinceName:

localityName:

organizationName:

organizationalUnitName: 172.16.34.240

commonName:

emailAddress: Service@Example.de

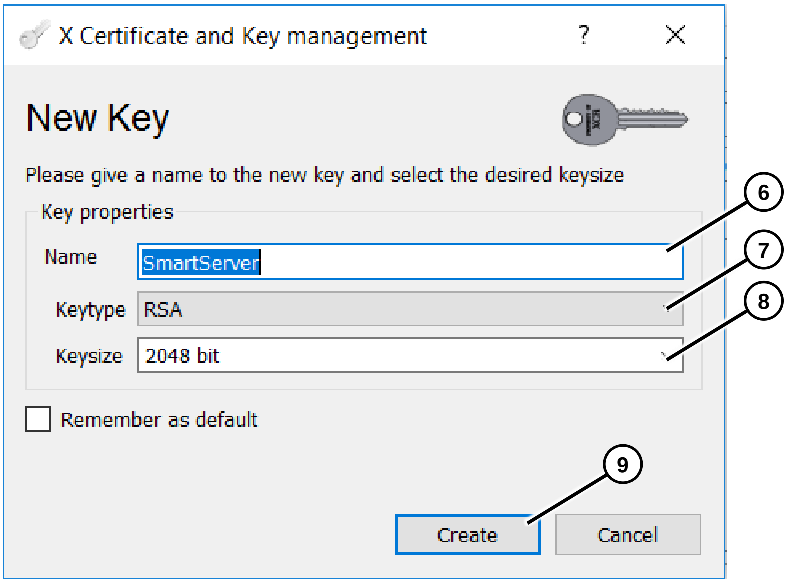
Private key

☐ Used keys too

Generate a new key

   - Click the "Generate a new key" button (5). The following window then opens.

Figure 2-4



X Certificate and Key management

New Key

Please give a name to the new key and select the desired keysize

Key properties

Name: SmartServer

Keytype: RSA

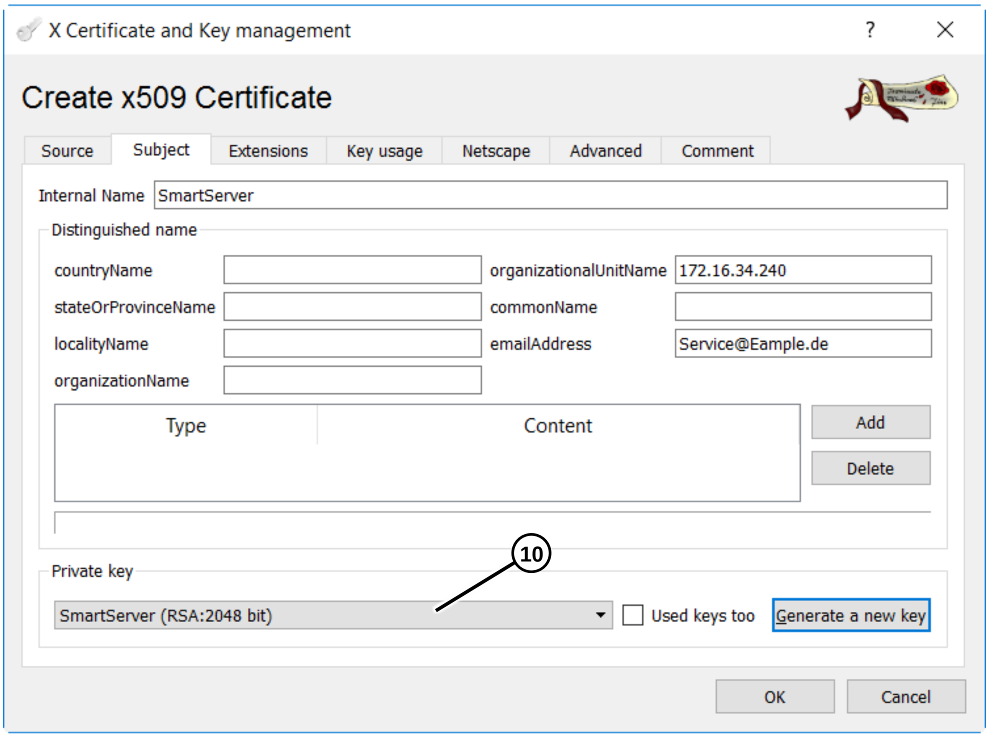
Keysize: 2048 bit

□ Remember as default

- Name: The name is applied automatically. Do not change this (6).
- Key type: RSA (7).
- Key size: 2048 bits (8).
- Click the "Create" button (9). A new key is created.

You return to the "Subject" page. Under "Private key" you see the newly created key displayed (10).

Figure 2-5



X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced | Comment

Internal Name: SmartServer

Distinguished name

countryName:

stateOrProvinceName:

localityName:

organizationName:

organizationalUnitName: 172.16.34.240

commonName:

emailAddress: Service@Eample.de

Type	Content

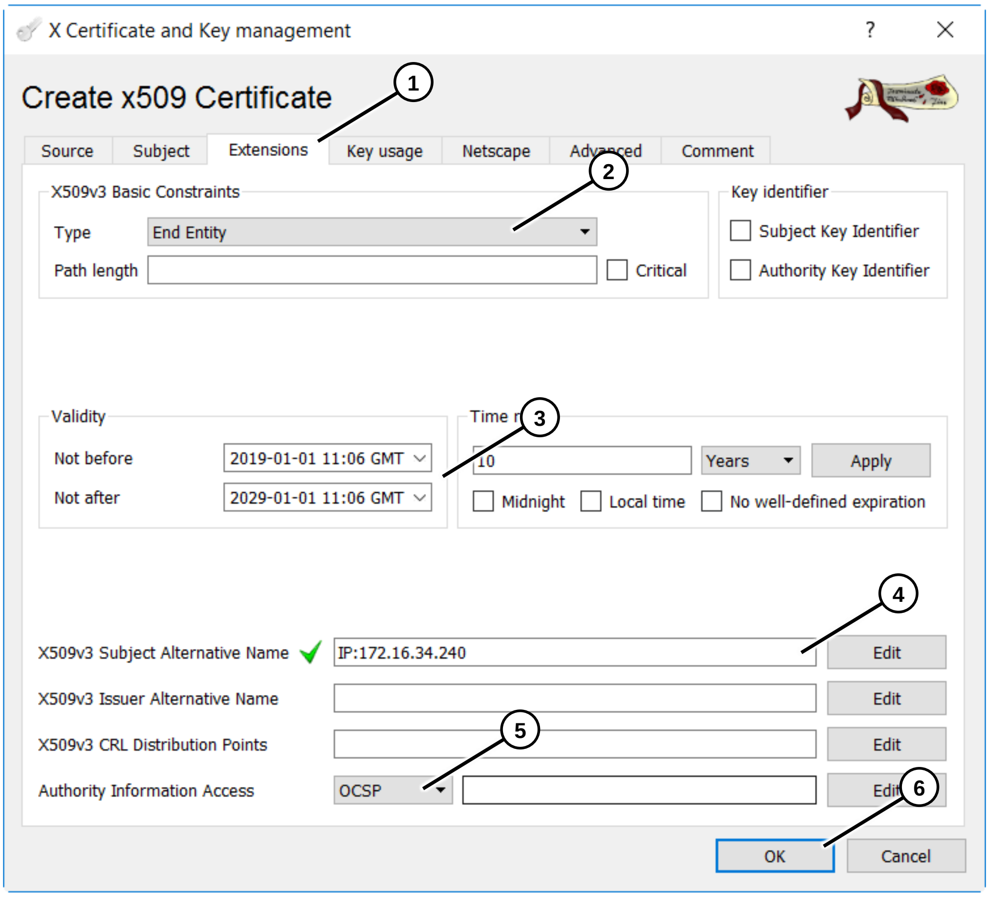
Private key

SmartServer (RSA:2048 bit)

□ Used keys too

6. Tab "Extensions" (1).
   Select the settings shown.
   - Type: Select the "End Entity" option (2).
   - Validity / Time range: Here you specify how long the certificate is to be valid. For this you enter the beginning and end dates (3).
   - X509v3 Subject Alternative Name: You have the option of entering the IP address of the operator panel here. You must also enter "**IP:**" (4).
   - Authority Information Access: Here you select the "OSCP" option (5).

Figure 2-6



X Certificate and Key management ? ✕

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced | Comment

X509v3 Basic Constraints
Type: End Entity
Path length: □ Critical

Key identifier
□ Subject Key Identifier
□ Authority Key Identifier

Validity
Not before: 2019-01-01 11:06 GMT
Not after: 2029-01-01 11:06 GMT

Time range
10 Years Apply
□ Midnight □ Local time □ No well-defined expiration

X509v3 Subject Alternative Name ✓ IP:172.16.34.240 Edit
X509v3 Issuer Alternative Name Edit
X509v3 CRL Distribution Points Edit
Authority Information Access OCSP Edit

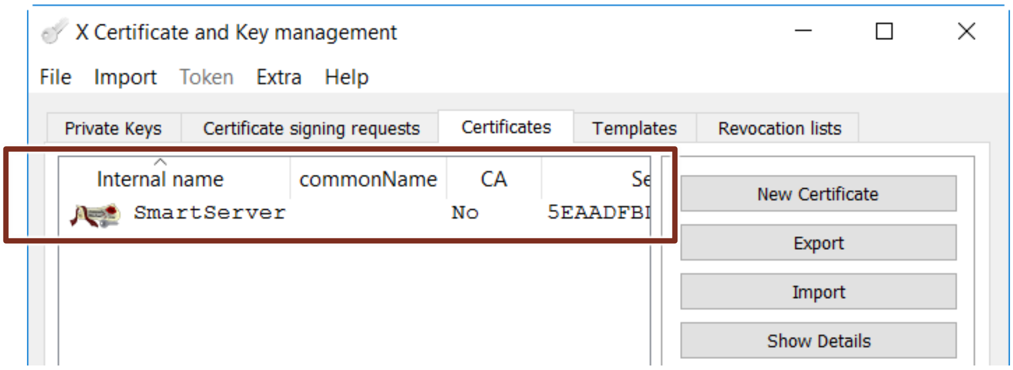
OK Cancel

You do not have to make any entries/changes in the "Key usage", "Netscape", "Advanced" and "Comment" tabs.

- Complete the inputs with the "OK" button.

View the newly created certificate.

Figure 2-7



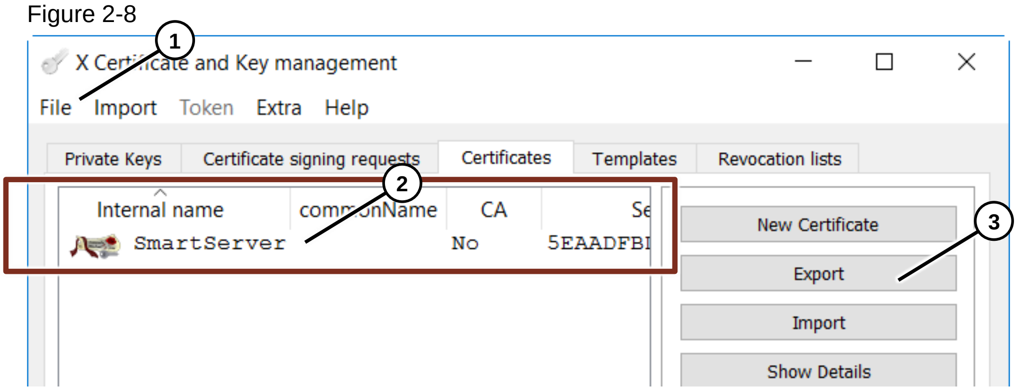
Internal name	commonName	CA	Se
SmartServer		No	5EAADFBI

Export a certificate

In order to be able to import the certificate into the operator panel you must first export the certificate.

1. Open the "XCA" tool.
2. Open the library in which the certificate is stored.
   Menu bar: "File > Certificates" (1).
3. Mark the certificate to be exported (2).
4. Click the "Export" button (3).
   The "Certificate export" window opens.

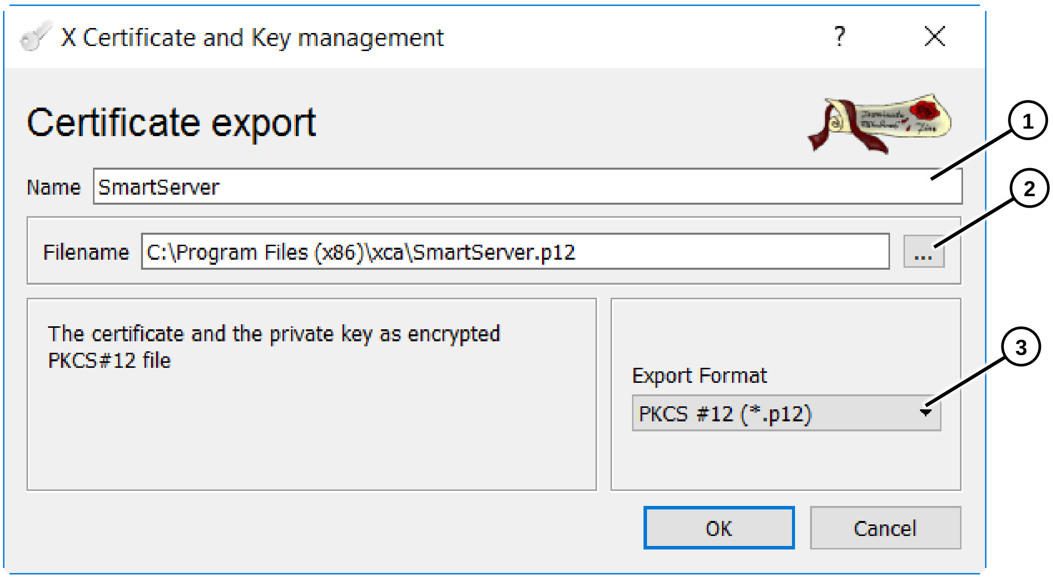
Figure 2-8



Internal name	commonName	CA	Se
SmartServer		No	5EAADFBI

5. "Certificate export" window
   - Name: The name is applied automatically. Do not change this (1).
   - File path: Specify a storage path for the certificate (2).
   - Export Format: Here you select the format "**PKCS #12 (*.p12)**" in the drop-down list box (3).
   - Confirm the entries with "OK". A window with a password request opens.

Figure 2-9



X Certificate and Key management

Certificate export

Name: SmartServer

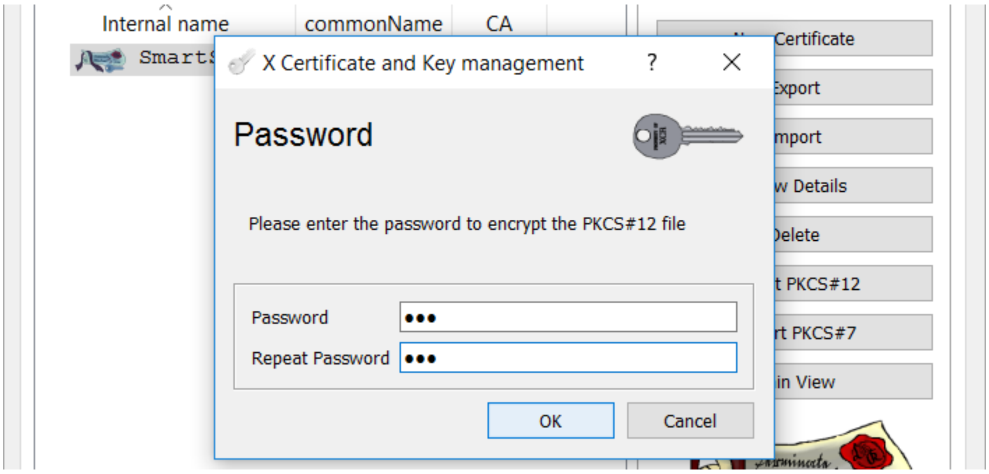
Filename: C:\Program Files (x86)\xca\SmartServer.p12

The certificate and the private key as encrypted PKCS#12 file

Export Format: PKCS #12 (*.p12)

6. Password request window
   - Enter a password. The password that you assign here will be requested later when importing the certificate to the operator panel and in the MS Internet Explorer. In this example it is "100".
   - Confirm the entries with "OK".

Figure 2-10



X Certificate and Key management

Password

Please enter the password to encrypt the PKCS#12 file

Password: •••

Repeat Password: •••

This completes export of the certificate.

3 Inserting a Certificate in the PC Certificate Folder

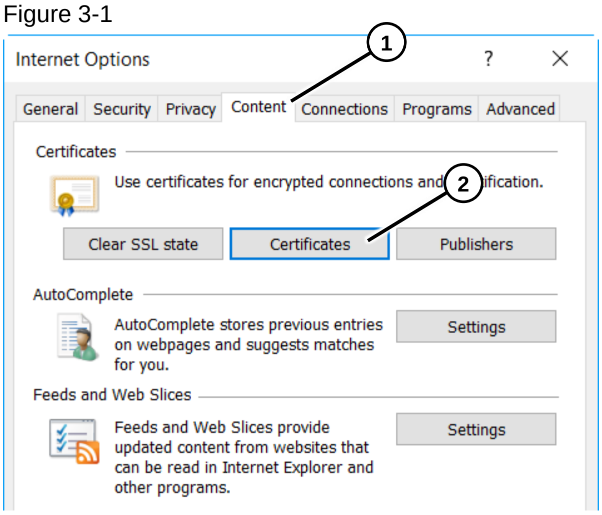
You can use the interface of the Internet Explorer or the Microsoft Management Console (MMC) to insert a certificate in the certificate folder of the Windows PC.

In this entry we show the option using the MS Internet Explorer.

MS Internet Explorer

1. Call the Internet Options of the MS Internet Explorer and select "Content" in the menu bar (1).
2. Then under "Certificates" you click the "Certificates" button (2).

Figure 3-1



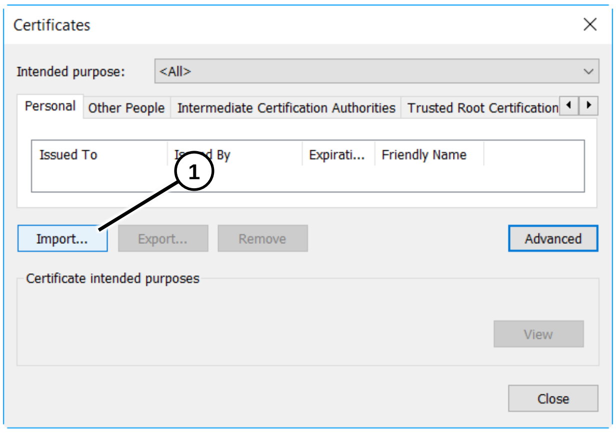
Use certificates for encrypted connections and ification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

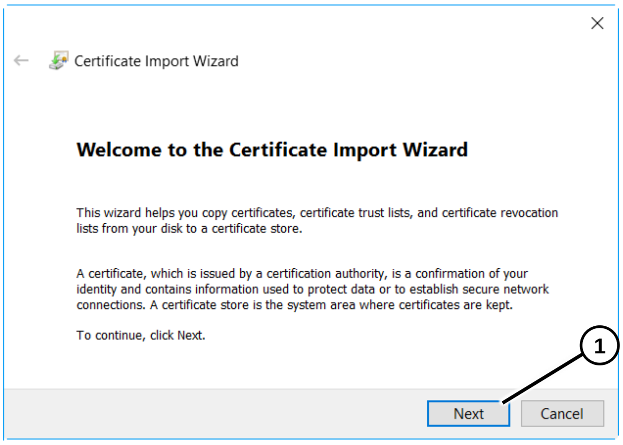
3. Click the "Import..." button (1).

Figure 3-2



4. Click the "Next" button (1).

Figure 3-3



Certificate Import Wizard

Welcome to the Certificate Import Wizard

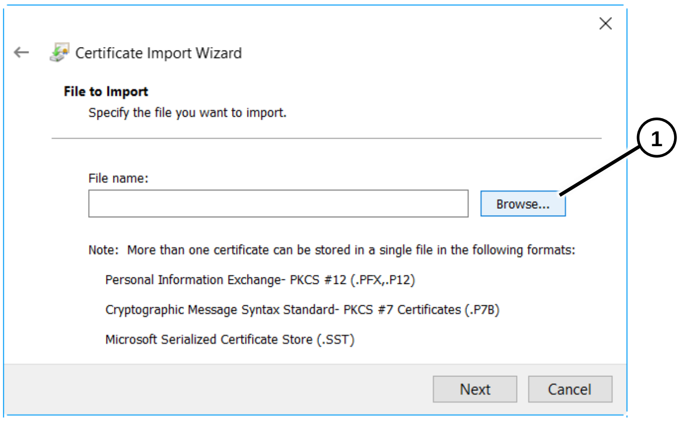
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. In the next window you click the "Browse..." button (1).

Figure 3-4



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

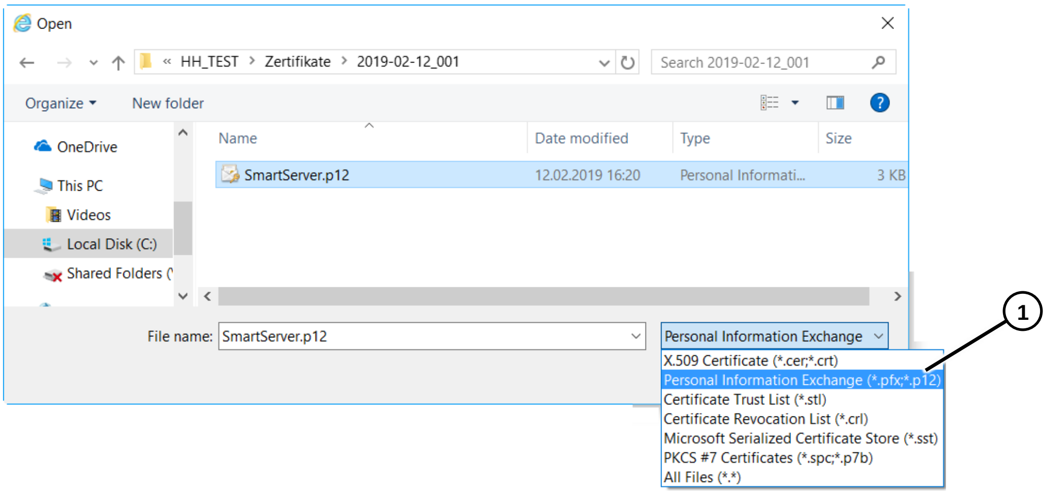
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

6. Here you navigate to the path in which the certificate is stored.
   Note:
   Make sure that you select the file format "*:p12" beforehand (1).

Figure 3-5



Open

« HH_TEST › Zertifikate › 2019-02-12_001

Search 2019-02-12_001

Name	Date modified	Type	Size
SmartServer.p12	12.02.2019 16:20	Personal Informati...	3 KB

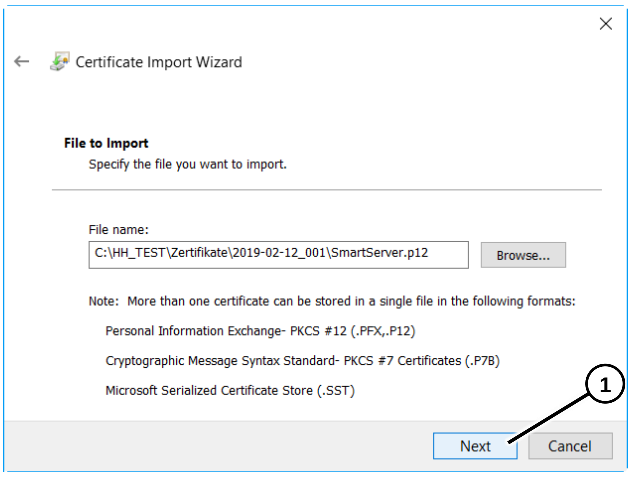
File name: SmartServer.p12

Personal Information Exchange

X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p12)
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.sst)
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)

7. Click the "Next" button (1).

Figure 3-6



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\HH_TEST\Zertifikate\2019-02-12_001\SmartServer.p12

Note: More than one certificate can be stored in a single file in the following formats:

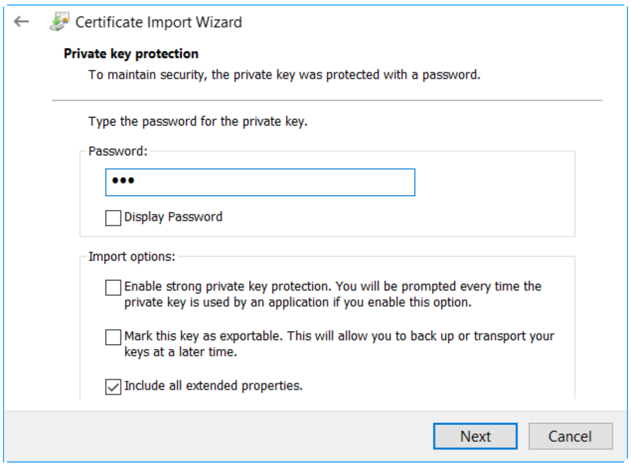
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

8. Enter the password that you assigned in the certificate parameters. In this case "100". Then click "Next".

Figure 3-7



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●

□ Display Password

Import options:

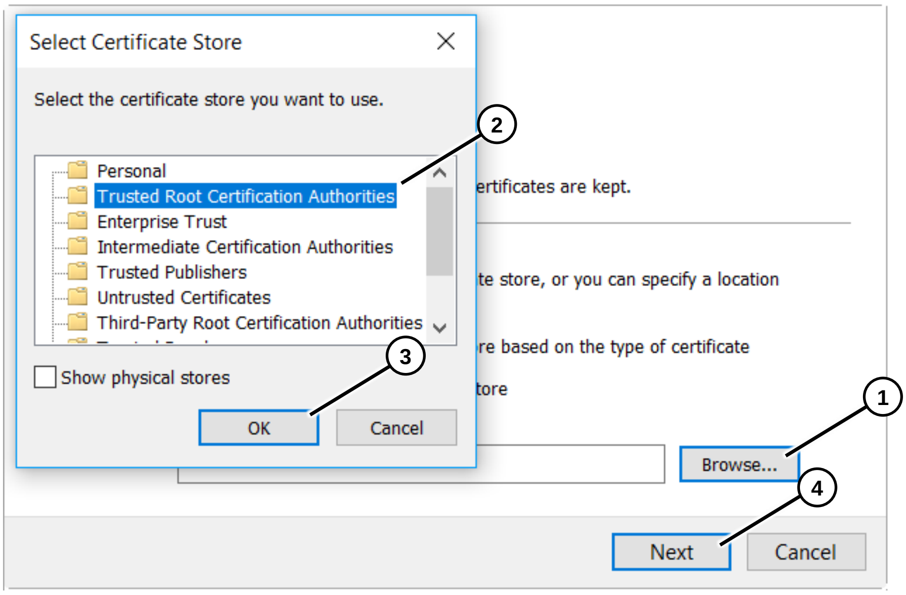
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

9. Click the "Browse..." button (1).
10. In the certificate store you select the "Trusted Root Certification Authorities" folder (2).
11. Confirm the entry with "OK" (3).
12. Click the "Next" button (4).

Figure 3-8



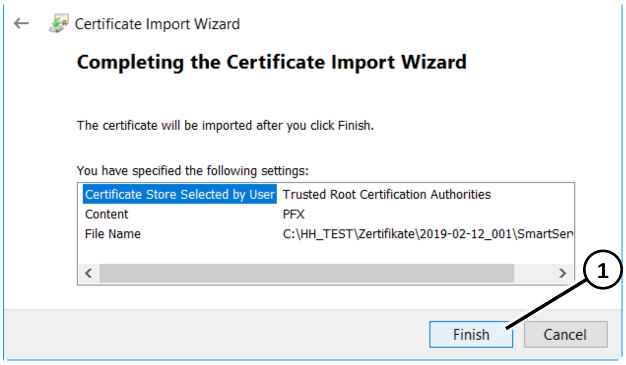
Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
□ Show physical stores
OK
Cancel
ertificates are kept.
te store, or you can specify a location
re based on the type of certificate
tore
Browse...
Next
Cancel
1
2
3
4

13. Click the "Finish" button (1).

Figure 3-9



Certificate Import Wizard

Completing the Certificate Import Wizard

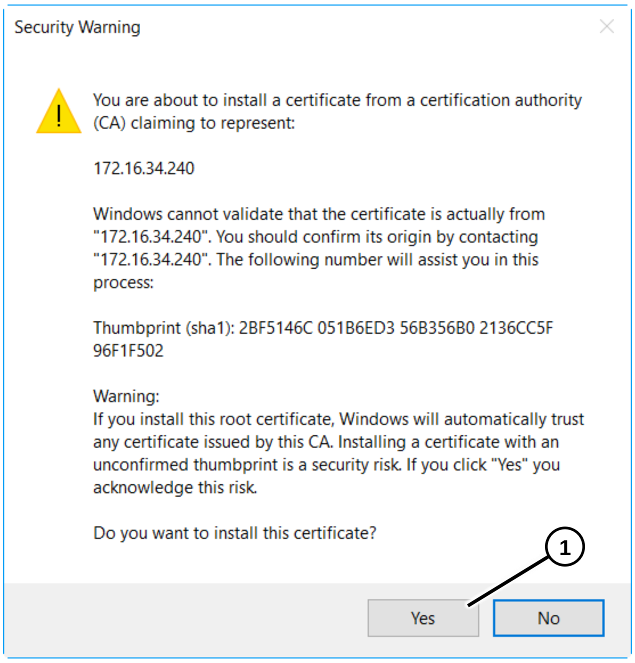
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	PFX
File Name	C:\HH_TEST\Zertifikate\2019-02-12_001\SmartSen

14. A security warning about installing the certificate is displayed. In this case you confirm the message with "Yes" (1).

Figure 3-10



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

172.16.34.240

Windows cannot validate that the certificate is actually from "172.16.34.240". You should confirm its origin by contacting "172.16.34.240". The following number will assist you in this process:

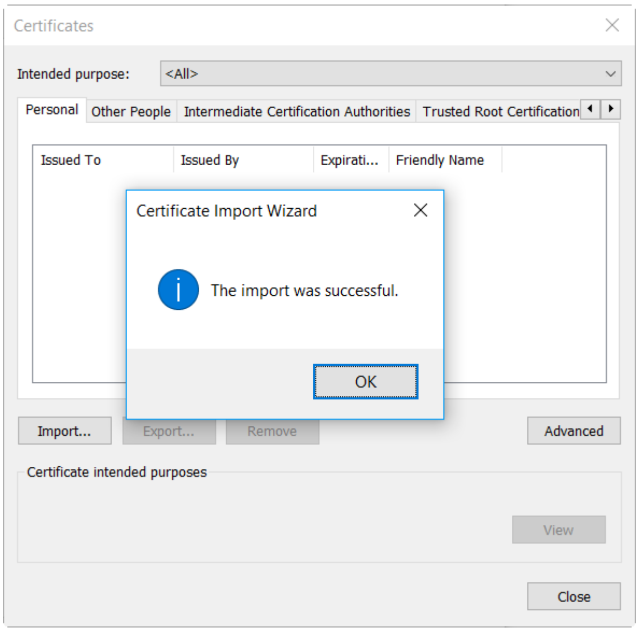
Thumbprint (sha1): 2BF5146C 051B6ED3 56B356B0 2136CC5F 96F1F502

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Installation of the certificate in the certificate store is now completed.

Figure 3-11



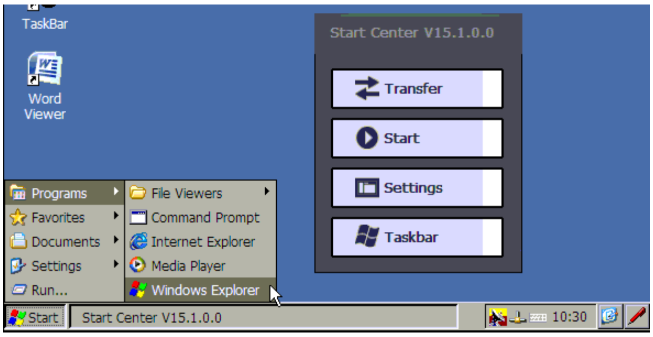
Certificate Import Wizard

The import was successful.

4 Transferring a Certificate to the Operator Panel

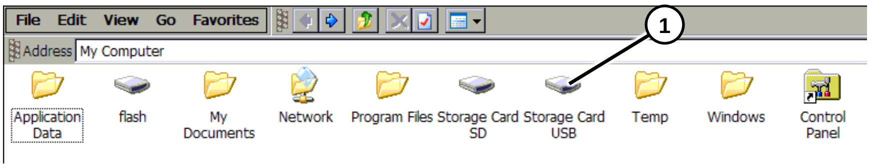
1. Copy the created certificate onto a USB stick.
2. Slot the USB stick into the operator panel.
3. On the operator panel you open the "Windows Explorer".
   In the "Start Center" you select "Taskbar > Programs > Windows Explorer".

Figure 4-1



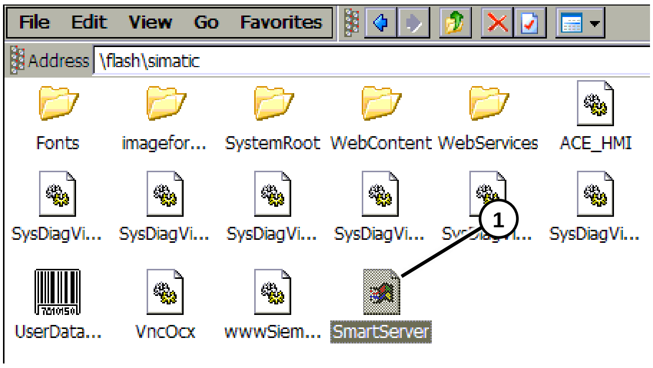
4. Select the drive "Storage Card USB" (1) and copy the certificate "SmartServer" (Edit > Copy).

Figure 4-2



5. Insert the copied certificate into the folder "flash > simatic" (Edit > Paste). View of the installed certificate (1).

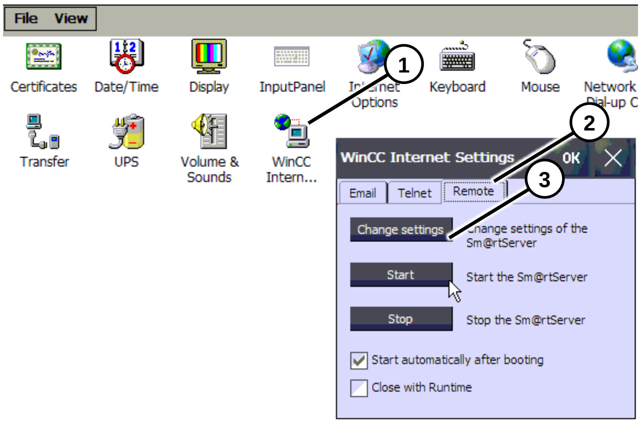
Figure 4-3



6. Close all the windows and via the "Start Center" you open the "Settings" of the operator panel.
7. Open the "WinCC Internet Settings" application (1).
   The "WinCC Internet Settings" menu opens.

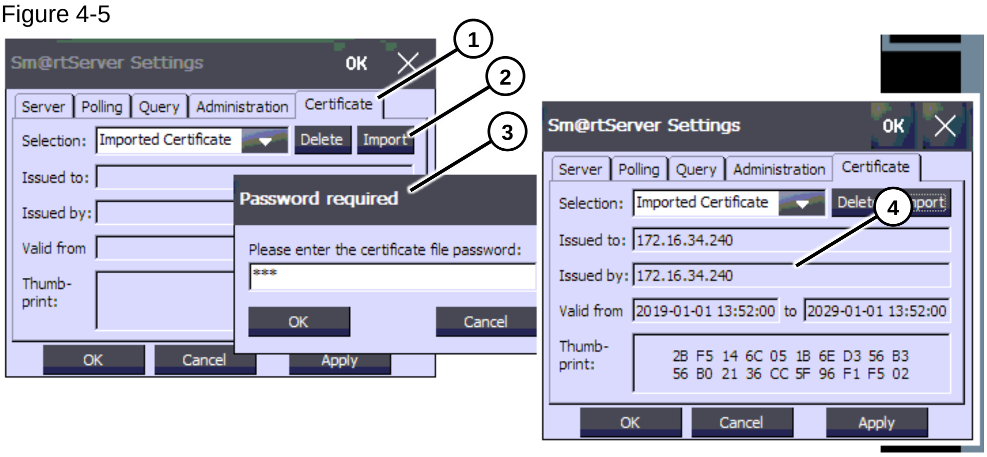
8. In the menu bar you select "Remote" (2).
9. Click the "Change settings" button (3).
   The "Sm@rtServer Settings" menu opens.

Figure 4-4



10. In the menu bar you select "Certificate" (1).
11. Click the "Import" button (2).
    A window with a password request opens (3).
    Enter the password that you assigned when creating the certificate. In this case "100".
12. Confirm the entries with "OK".
13. The certificate is now stored in "Certificates" on the operator panel (4).

Figure 4-5



Selection: Imported Certificate

Issued to:

Issued by:

Valid from

Thumb-print:

Please enter the certificate file password: ***

Selection: Imported Certificate

Issued to: 172.16.34.240

Issued by: 172.16.34.240

Valid from 2019-01-01 13:52:00 to 2029-01-01 13:52:00

Thumb-print: 2B F5 14 6C 05 1B 6E D3 56 B3 56 B0 21 36 CC 5F 96 F1 F5 02

Finish the import with the "OK" button and close all the windows.

5 Deleting a Certificate

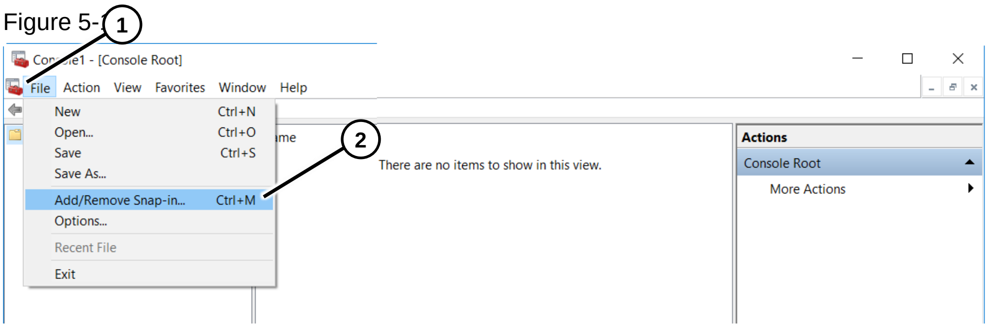
MMC Tool

You can use the Microsoft Management Console (MMC) for easy management of certificates. For example, you can use the tool to

- Insert certificates
- Delete certificates
- Save certificates

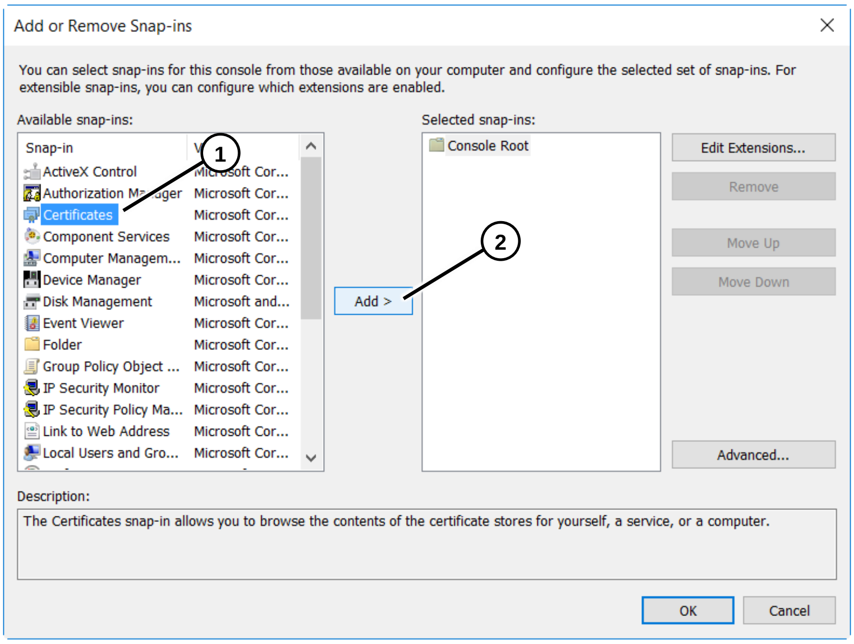
1. Call the MMC tool.
   - Search Windows > MMC.
2. In the menu bar you open the "Add/Remove Snap-In" function. "File > Add/Remove Snap-In...".

Figure 5-1



3. In the "Snap-in" column on the left you mark "Certificates" (1).
4. Click the "Add >" button (2). A window opens in which you can define the rights. Complete the input with "Finish".
5. Confirm the entries with "OK".

Figure 5-2



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Selected snap-ins:

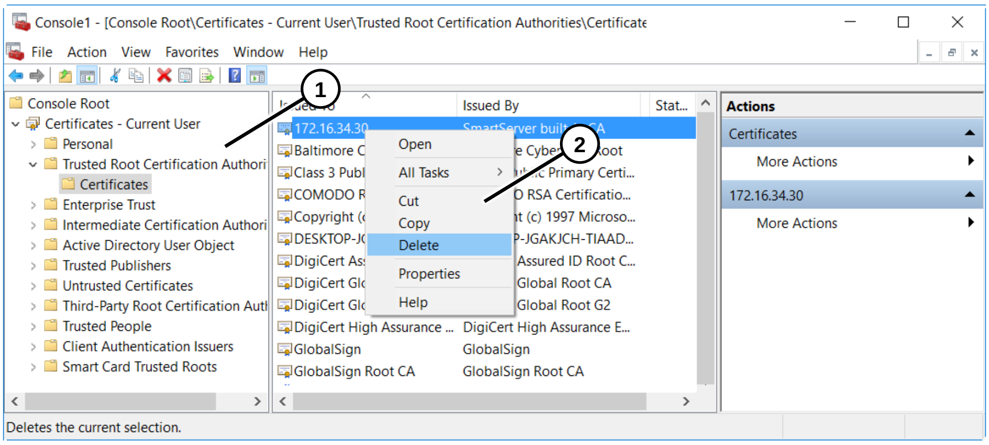
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

1. The separate certificate folders are displayed in the folder tree. The panel certificate is located in the "Trusted Root Certification Authorities" folder (1).
2. Right-click the certificate to be deleted. In the pop-up menu you select the functions to be executed (2).

Figure 5-3



Deletes the current selection.