

SIEMENS

Ingenuity for life



Using Certificates with TIA Portal

SIMATIC, TIA Portal

<https://support.industry.siemens.com/cs/ww/en/view/109769068>

Siemens
Industry
Online
Support



Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

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 constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: <https://www.siemens.com/industrialsecurity>.

Table of contents

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Principle of operation.....	5
1.2.1 General information on certificates	5
1.2.2 Certificate manager of TIA Portal	6
1.2.3 Self-signed device certificate.....	8
1.2.4 Certificate signed by a certification authority.....	9
1.2.5 Decision-making aids	10
2 Using Certificate management	11
2.1 Activate and understand.....	11
2.2 Installing certificate directly	15
2.3 Export certificate.....	18
3 Safe Web server connection	20
3.1 Web Server and Web Server Certificates	20
3.2 Setting up and testing the browser.....	26
3.2.1 Internet Explorer or Edge	27
3.2.2 Google Chrome	35
3.2.3 Firefox.....	46
3.2.4 Operating system Android.....	51
3.2.5 Operating system iOS	59
3.3 Checking certificates	67
4 Secure OPC UA connection	70
4.1.1 Security settings in the Server	71
4.1.2 Security settings in the Client.....	86
4.1.3 Test secure OPC UA connection	94
5 Appendix	99
5.1 Service and support	99
5.2 Links and literature	100
5.3 Change documentation	100

1 Introduction

1.1 Overview

Document contents

This document describes the handling of web server and OPC UA certificates in the PLC environment. You will learn what possibilities TIA Portal currently offers and how it is handled.

You will receive instructions for the following points:

- Establishing a secure connection to the web server of a SIMATIC S7-1500 CPU.
- Establishing a secure connection between the integrated OPC UA server of a SIMATIC S7-1500 CPU and an OPC UA client.

Requirements

The following software environment is required for a successful implementation:

- TIA Portal V15.1
- Windows 7 Prof. or Windows 10
- An https-enabled browser, e.g. Internet Explorer V11 or Google Chrome V75
- An OPC UA client that supports a secure connection, e.g. UaExpert from Unified Automation
- One runtime license for the OPC UA server

A SIMATIC S7-1500 CPU from firmware V2.5 is required as hardware component, which serves as OPC UA server.

Preparation

Create a new TIA Portal project with your used CPU. Assign a network address to the CPU.

Make sure that the time of the CPU is set to the current time. A certificate always contains a period of time in which it is valid. To be able to encrypt with the certificate, the time of the S7 CPU must also be within this period of time. With a brand new S7-CPU or after an overall reset of the S7-CPU, the internal clock is set to a default value that lies outside the certificate runtime. The certificate is then marked as invalid.

1.2 Principle of operation

1.2.1 General information on certificates

Description

A device certificate (end-entity certificate) is required to establish a secure connection to a SIMATIC S7-1500 CPU. A device certificate is, for example, a server certificate for the Web or OPC server.

When the hardware configuration is loaded into the CPU, the device certificate generated by TIA Portal or created by the user is also loaded automatically.

Creating certificates

Device certificates for the CPU can be obtained in the following ways:

- Manually created and generated by the user.
- Automatically generated by TIA Portal.
For S7-1500 CPUs with firmware V2.0 or higher, TIA Portal automatically generates the device certificate for the CPU as soon as you activate the web server of the CPU with the option "HTTPS" or the OPC UA server.

Certificate types

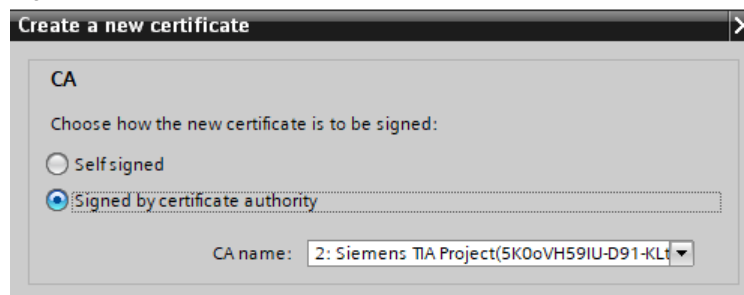
A distinction is made between the following certificate types:

- Self-signed certificate:
Each participant generates his own certificate and signs it. No new certificates can be derived from a self-signed certificate. However, you must load all self-signed certificates of the partner devices into the CPU (STOP required).
Application examples: Static configuration with limited number of communication participants.
- Device certificate signed via a certification authority (short: CA (Certificate Authority)) and its CA certificate:
All certificates are created and signed by a certification authority. You only have to load the certificate of the certification authority into the CPU. The certification authority may generate new certificates. The addition of partner devices is possible without STOP of the CPU.
Application examples: Dynamically growing plants.

The automatically generated device certificates are issued and signed by the TIA Portal internal certification authority.

If you manually create the device certificates in TIA Portal, you can select the option "Self signed" or "Signed by certificate authority".

Figure 1-1



1.2.2 Certificate manager of TIA Portal

Description

You can use the TIA Portal project as a certification authority by selecting the option "Use global security settings for certificate manager".

A certification authority is a trusted authority that confirms the identity of the certificate and its creator.

The option decides whether you have access to all certificates in the project or not and whether you can have the device certificates signed by the CA certificates of the certification authority or not.

- If you do not use the certificate manager in the global security settings, then you only have access to the local certificate store of the CPU. You have no access, for example, to imported certificates or root certificates. Without these certificates only a limited functionality is available. For example, you can only generate self-signed certificates.
- If you use the certificate manager in the global security settings, you have access to the global, project-wide certificate store. For example, you can assign imported certificates to the CPU or create device certificates issued and signed by the project's certification authority.

TIA Portal provides two root certificates (CA certificates) for the entire project.

Note

In this example, the TIA Portal Global Certification Manager is activated and used.

Properties of the certificate manager

If you use the certificate manager in the global security settings, you get an overview of all certificates used in the project, such as CA certificates and device certificates, with information about the certificate owner, issuer, validity, use, and existence of a private key. With the appropriate authorization, you can also manage certificates for the project there.

Figure 1-2

ID	Common name of subject	Issuer	Valid to	Used as	Private key
1	Siemens TIA Project'sZuqHXrGka...	Siemens TIA Project's...	06/27/2037	Certification authorit...	Yes
2	Siemens TIA Project'sK0oVH59IU...	Siemens TIA Project's...	06/27/2037	Certification authorit...	Yes

Functions of the certificate manager

The following functions are available in the certificate manager of the global security settings:

- Import new certificates and certification authorities.
- Export the certificates and certification bodies used in the project.
- Renewal of expired certificates and certification bodies.
- Replace existing certification bodies.
- Add trusted certificates and certificate authorities.

Figure 1-3

Certificate authority (CA)			
ID	Common name of subject	Issuer	Valid to
1	Siemens TIA Project(sZuqHXriGka...	Siemens TIA Project(s...	06/27/2037
2	Siemens TIA Project(5K0oVH59IU-...	Siemens TIA Project(

- Import
- Export
- Assign
- Show
- Renew
- Replace

1.2.3 Self-signed device certificate

Description

Self-signed certificates are certificates whose signature originates from the certificate holder and not from an independent certification authority.

If you use self-signed certificates, a device certificate is created in TIA Portal for each CPU and then loaded into the CPU. You must also install this device certificate in the PC that you are using to access the Web or Internet connection. OPC server of the CPU.

Self-signed certificates cannot be verified with the CA certificates of the TIA Portal project.

Manual acquisition

When creating device certificates in TIA Portal, you can select the "Self-signed" option. You can create self-signed certificates without being signed up for global security settings.

Automatic generation

If you do not use the certificate manager in the global security settings, TIA Portal generates the device certificate as a self-signed certificate.

Important note

If you address the Web or OPC server of the CPU via the IP address of the CPU, a new device certificate must be created and loaded with each change of the IP address of an Ethernet-interface of the CPU. The reason is that the identity of the CPU changes with the IP address.

You can avoid this problem by addressing the CPU with a domain name instead of its IP address, e.g. "myconveyer-cpu.room13.myfactory.com". To do this, you must manage the domain names of the CPUs via a DNS server.

1.2.4 Certificate signed by a certification authority

Description

Signed certificates are certificates whose signature comes from an independent certification authority.

If you use certificates signed by a certification authority, one device certificate per CPU is created in TIA Portal and then loaded into the CPU.

On the PC with which you want to access the web server or OPC server of the CPU, you do not have to perform any action first.

Manual acquisition

If you use the certificate manager in the global security settings of the CPU, then you can have the device certificates of the CPU signed by the certification authority of the project (CA certificate).

You can determine which CA certificate you want to use yourself.

Automatic generation

If you use the certificate manager in the global security settings, TIA Portal generates a device certificate signed using a CA certificate provided by TIA Portal.

When loading, the CA certificate of the project is also loaded automatically.

Important note

You can access the web server of the CPU via HTTPS from a PC. However, your web browser will warn you not to use this page, as the web server cannot be considered trustworthy. To see the page, you must explicitly add the Web page as an exception. The cause is the missing CA certificate with which the server certificate of the CPU was signed.

For this reason, it is recommended that you install the CA certificate of the CPU. Once the CA certificate is installed, your web browser will no longer display a warning because the web server can be verified.

To install the CA certificate, you have the following options:

- You can download the valid CA certificate directly from the "Intro" homepage of the web server under "Download certificate". (see [section 3.2](#)).
- You can export the CA certificate from TIA Portal and then import the CA certificate into the browser (see [section 2.3](#)).
- You can install the CA certificate directly from TIA Portal (see [section 2.2](#)).

Note

For more information, refer to the [section 3](#).

1.2.5 Decision-making aids

Whether it is better to use self-signed device certificates or device certificates that have been signed by a certification authority depends, among other things, on the number of CPUs to be reached and the number of accessing PCs.

Self-signed certificates

If you use self-signed device certificates, you must create a separate device certificate for each CPU, self-sign it, and install this device certificate on your PC.

It becomes complicated if you use several CPUs or PCs:

- If you have several CPUs, you must install the device certificates of all CPUs on the PC.
- If you want to reach multiple CPUs with multiple PCs, you must install the device certificates of all CPUs on all PCs.

You must also note that the IP address of the CPU must not change, otherwise you will have to generate, load and install new device certificates.

Device certificates signed by a CA

If you want to access different CPUs from different PCs or if you want to add more CPUs later, then the use of certification authorities is preferred.

You must also create a separate device certificate for each CPU. However, since all device certificates were signed with the same CA certificate, you only need to install this one CA certificate on the PC(s).

Regardless of whether you want to reach only one CPU or several CPUs, it is sufficient to install only one certificate (the CA certificate) on the PC.

You can easily install, export, or download the CA certificate directly from the Global Certification Manager from the web server home page of the CPU.

Since only the CA certificate must be installed on the PC, you can also change the IP address of the CPU afterwards without any consequences for the PC side.

Summary

The following table serves as an additional decision-making aid:

Table 1-1

	Self-signed	Certificate authority
1 CPU, 1PC / Client, no changes planned	+	-
n CPUs, m PC / Clients, changes possible	-	+
Download the certificate via web server	-	+

2 Using Certificate management

In TIA Portal, the certificates are managed in the certificate manager of the global security settings. The certificate manager contains an overview of all certificates used in the project. In the certificate manager, for example, you can import new certificates and export, renew, or replace existing certificates. Each certificate is assigned an ID that can be used to reference the certificate in the program modules.

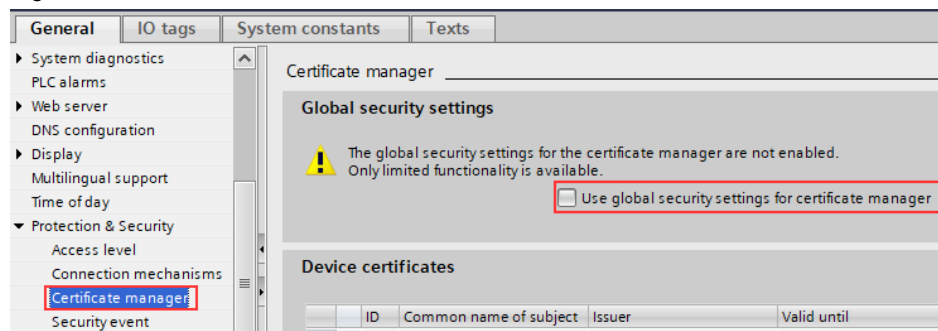
2.1 Activate and understand

Activate Certificate management

To activate the global security settings, proceed as follows:

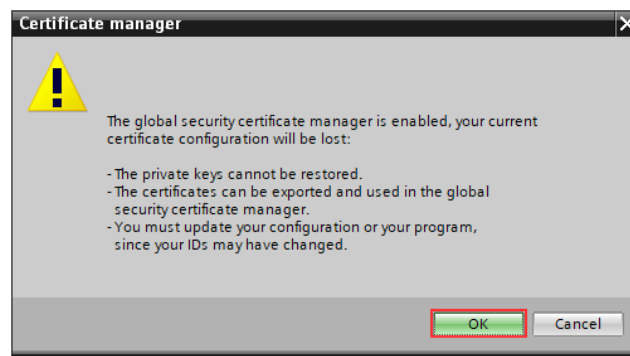
1. Mark the CPU in the device or network view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "Properties" tab, select "Protection & Security > Certificate Manager". Activate the function "Use global security settings for certificate manager".

Figure 2-1



3. Confirm the following message with the "OK" button.

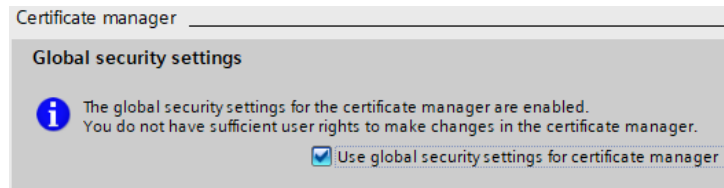
Figure 2-2



Result

The Global Certification Manager is enabled.

Figure 2-3



Protect project

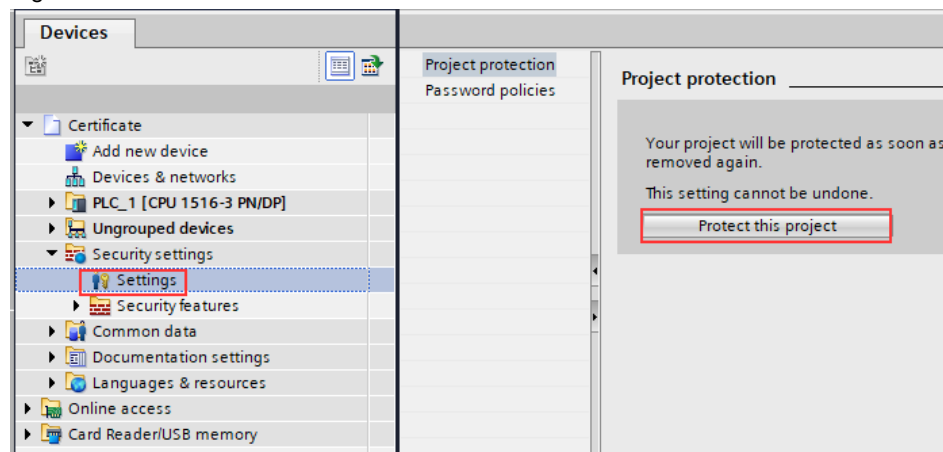
After you have activated the global security settings for the certificate manager, you must protect the project from unauthorized access.

You protect the project by defining a project administrator and logging on with this user later. You cannot access the certificate manager of the global security settings without logging in.

Create a project administrator as described below:

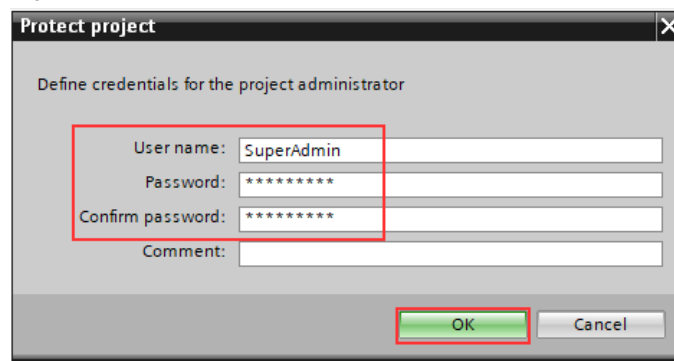
1. Double-click on the entry "Settings" in the project navigation under "Security settings".
Click the "Protect this project" button.

Figure 2-4



2. Define a user name and password. Confirm the password. Click the "OK" button.

Figure 2-5



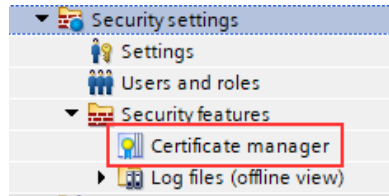
Result

You have protected the project and appointed a project administrator.

From now on, you can only open the project if you have previously logged on as the project administrator.

If you have logged in, a line "Certificate manager" will appear under the entry "Security settings > Security functions" ("Security settings > Security features").

Figure 2-6



Understanding the Certificate manager

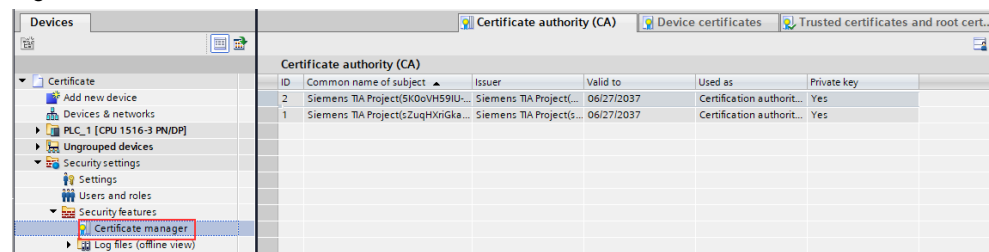
With a double click on the newly appeared line "Certificate manager" in the project navigation you get access to all certificates in the project, divided into the registers

- Certification authority (CA),
- "Device certificates" and
- "Trusted certificates and root certificates".

TIA Portal provides two root certificates (CA certificates) for the entire project, which differ in the encryption strength of the hash algorithms for the certificate signature.:

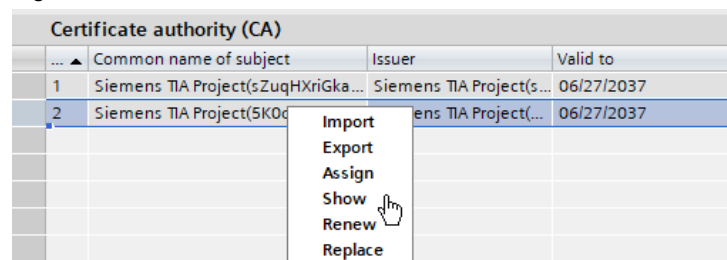
- The CA certificate with the "ID: 1" contains the certificate signature encrypted with SHA1.
- The CA certificate with the "ID: 2" contains the certificate signature encrypted with SHA256.

Figure 2-7



With the certificate manager in the global security settings, you now have the option to view, export, or import the two root certificates into the TIA portal.

Figure 2-8



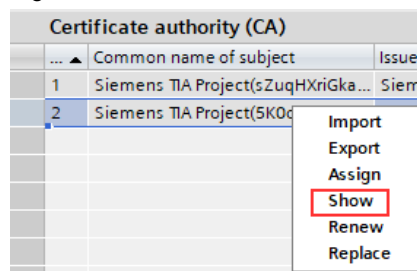
2.2 Installing certificate directly

The certificates can also be installed directly on the local PC via the certificate manager of the global security settings. In the following instructions, the CA certificate is installed in the Windows certificate store.

Follow these steps for this purpose:

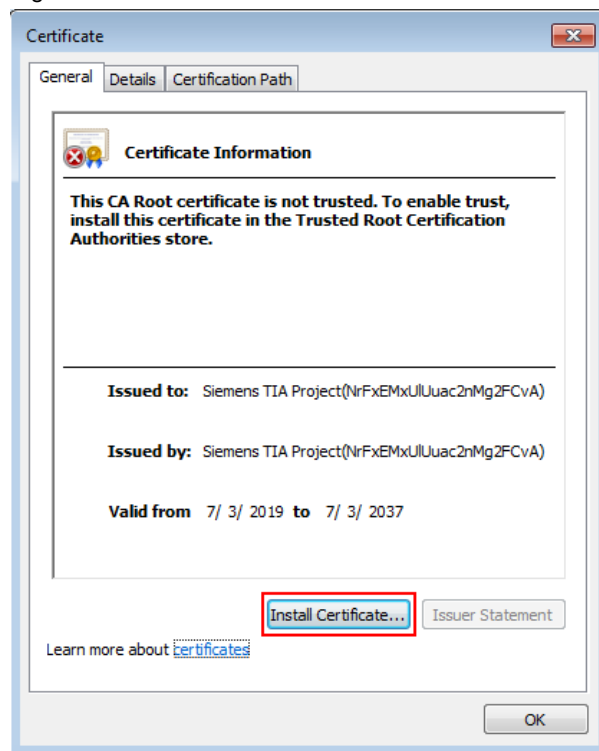
1. In the project navigation, open the "Security settings > Security features" menu. Double-click on the "Certificate manager" line.
2. Select a certificate and use the right mouse button to open the context menu. Select the "Show" entry.

Figure 2-9



3. The certificate is shown. To install the certificate locally on the PC, click the "Install certificate" button.

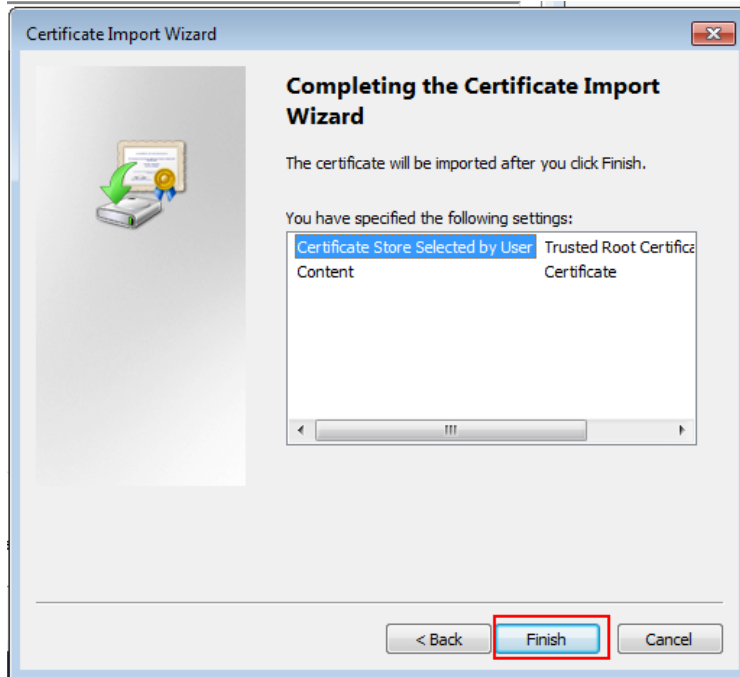
Figure 2-10



4. Follow the instructions of the Wizard.
 - Select the local storage as the storage location.
 - Select the certificate store yourself and locate the Trusted Root Certification Authorities folder.

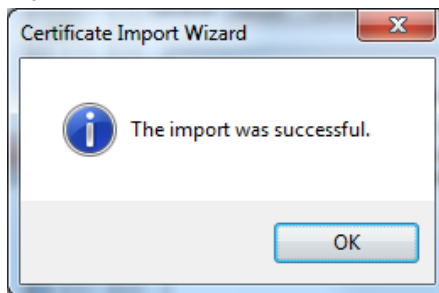
The "Finish" button imports the certificate into the selected folder. Before the wizard issues a security warning, which must be acknowledged with "Yes".

Figure 2-11



5. The wizard completes the successful import process with the following message, which you can confirm with "OK".

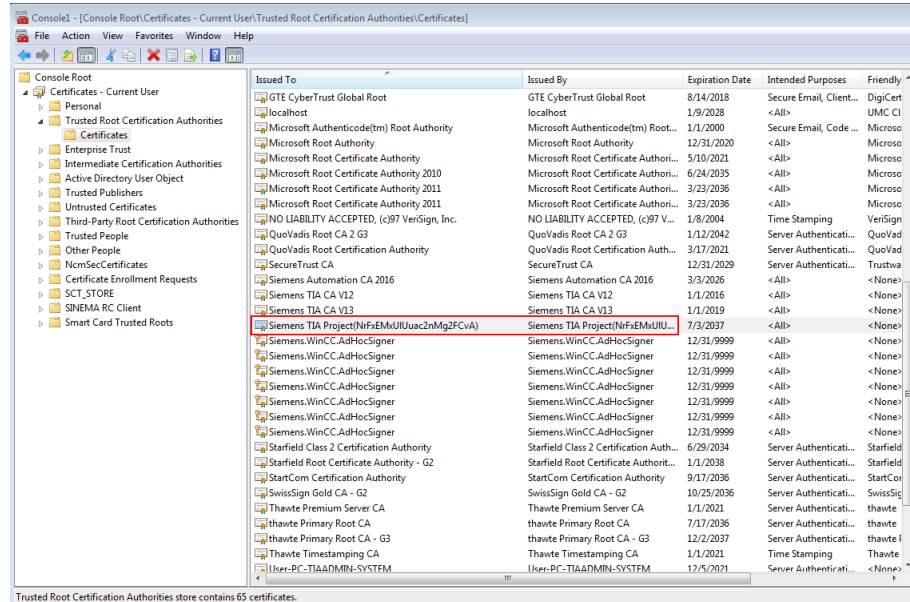
Figure 2-12



Result

You have imported the certificate from TIA Portal into the Windows certificate store. To check the import, you can use the Microsoft mmc management console. To do this, add the Certificates snap-in to the console.

Figure 2-13



Note

The MMC does not update the display automatically. The MMC does not update the display automatically.

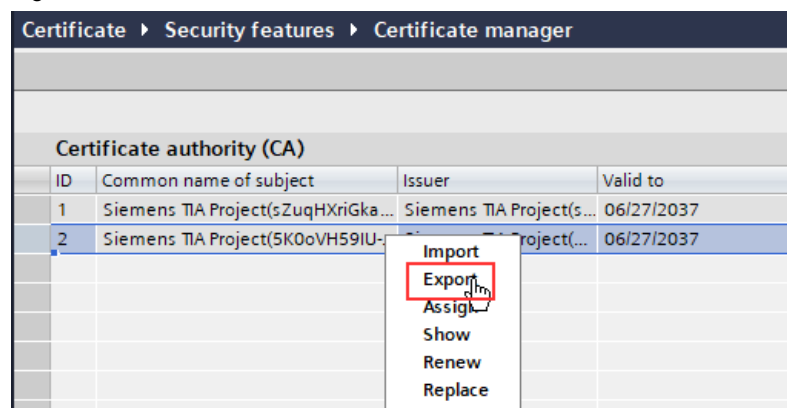
2.3 Export certificate

The certificates can also be exported in various formats via the certificate manager of the global security settings and installed at a later date or on another PC or imported into another application, e.g. UaExpert. In the following instructions, the CA certificate is exported.

Follow these steps for this purpose:

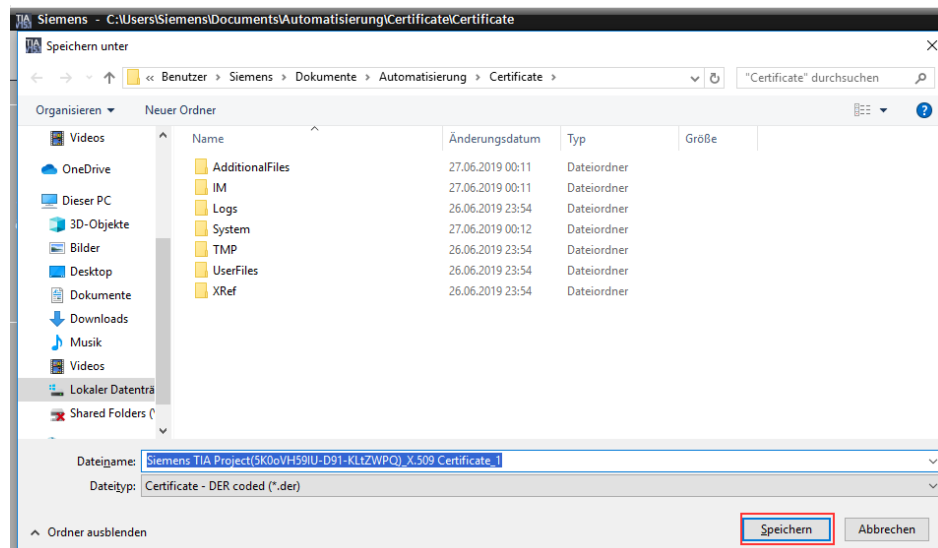
1. In the project navigation, open the "Security settings > Security features" menu. Double-click on the "Certificate manager" line.
2. Select a certificate and use the right mouse button to open the context menu. Select the entry "Export" ("Export").

Figure 2-14



3. A dialog box opens. Select the storage location of the certificate. Change the file type if necessary. Click on the "Save" button.

Figure 2-15



Note

By default, the certificate is exported as file type "*.der".
If you need a different file type, you can change the default setting in the selection list under "File type" ("Data type").

Result

You have exported the certificate from TIA Portal and saved it on the PC. You can now transfer the certificate to another PC or import it into another application, e.g. UaExpert.

To install the exported certificate directly, double-click the exported certificate. The certificate is displayed and can be installed. (see step 2 in [section 2.2](#)).

3 Safe Web server connection

3.1 Web Server and Web Server Certificates

Overview

For a secure connection, the web server of the CPU is set up so that only one connection via HTTPS is allowed. For this the CPU needs a device certificate (server certificate).

For S7-1500 CPUs with firmware V2.0 or higher, TIA Portal automatically generates the server certificate for the CPU as soon as you activate the web server via HTTPS and translate the project.

You can view the server certificate

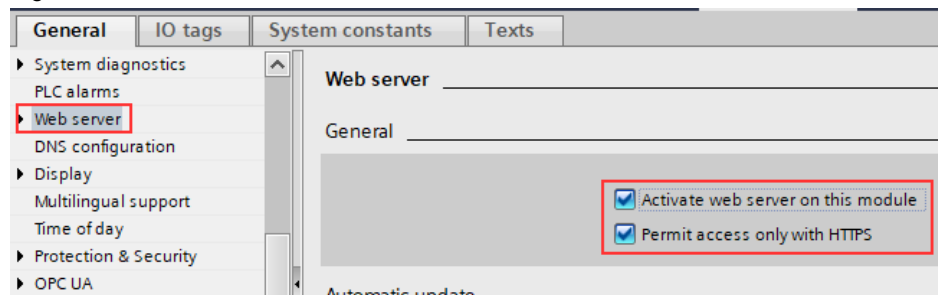
- in the properties of the CPU.
- Generate a new server certificate.
- Assign another server certificate to the Web server.

Activating Web Servers via HTTPS

To configure the Web server using HTTPS, proceed as follows:

1. Mark the CPU in the device or network view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "Properties" tab, select the "Web Server" entry. Activate the option "Activate web server on this module" and the option "Permit access only with HTTPS".

Figure 3-1



3. Translate your TIA Portal project.

Result

You have activated the web server with the "HTTPS" option. The web server of the CPU can be reached via the following address: "https://<IP address of the CPU>".

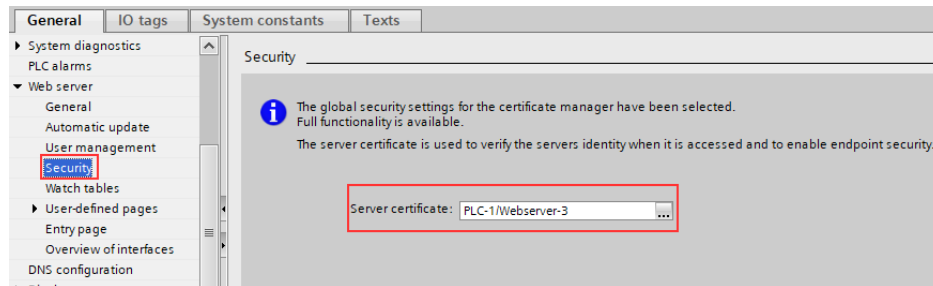
View Server Certificate

After you have enabled the "Permit access only with HTTPS" option and translated the TIA Portal project, TIA Portal generates a server certificate.

You can find the server certificate in the properties of the Web server.

In the area navigation, select Web Server > Security. Under "Server certificate" you can see that TIA Portal has already created a device certificate assigned to the web server.

Figure 3-2



Note

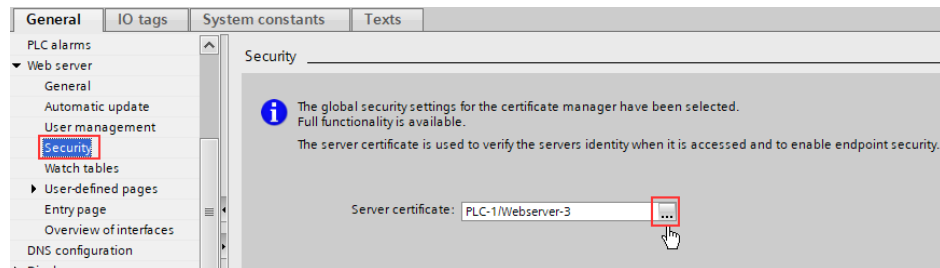
TIA Portal stores the server certificate in the local certificate directory of the CPU. You can view and manage this directory in the local certificate manager of the CPU and also in the certificate manager of the global security settings (export or delete certificates).

Creating a New Server Certificate

To generate a new server certificate, proceed as follows:

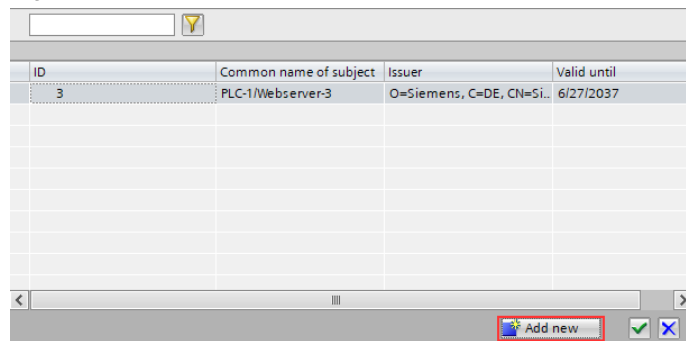
1. In the area navigation, select Web Server > Security.
2. To select another server certificate or to generate a new server certificate, click on the button integrated in the "Server certificate" drop-down list.

Figure 3-3



3. A dialog appears and lists all available server certificates. To create a new server certificate, click the "Add new" button.

Figure 3-4



3 Safe Web server connection

4. The dialog "Create new certificate" appears. You have the following options in this dialog:
 - You can choose between a self-signed certificate and a certificate signed by a certification authority.
 - If necessary, you can select the CA certificate of the certification authority.
 - You can determine the certificate parameters.

Figure 3-5

CA

Choose how the new certificate is to be signed:

Self signed

Signed by certificate authority

CA name: 2: Siemens TIA Project(5K0oVH59IU-D91-KL)

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1/Webserver-6

Signature: sha256RSA

Valid from: June 28, 2019 02:25:53 AM

Valid until: June 28, 2037 12:00:00 AM

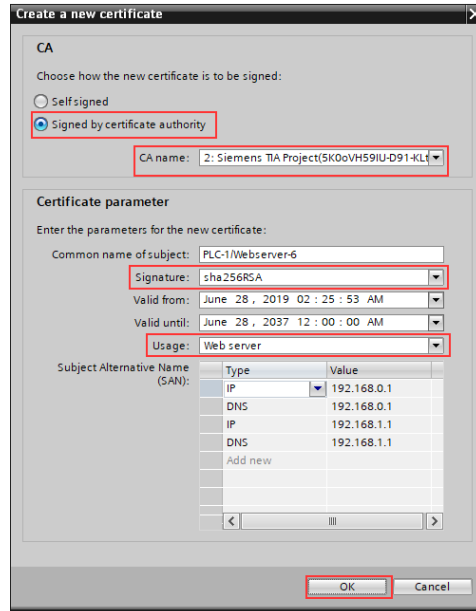
Usage: Web server

Type	Value
IP	192.168.0.1
DNS	192.168.0.1
IP	192.168.1.1
DNS	192.168.1.1
Add new	

OK Cancel

- This example creates a server certificate with strong encryption "SHA256" signed by a certification authority. The CA certificate provided by TIA Portal with the "ID: 2". Set the parameters. Use the screenshot as a guide. To generate the new certificate, click on the "OK" button.

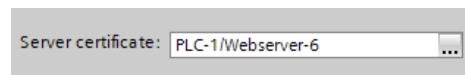
Figure 3-6



Note Coordinate the validity of the certificate with the plant operator.

- You can now use the newly created device certificate as the web server's server certificate.

Figure 3-7

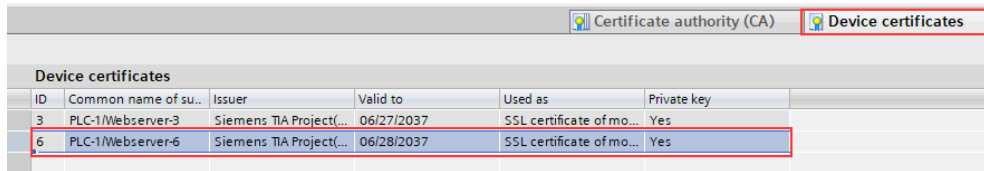


- Translate your TIA Portal project and load the CPU. During the load process, the device certificate, the CA certificate, and the authorization for Web server access, among other things, are loaded into the CPU.

Result

The new device certificate is added to the existing device certificates in the "Device certificates" tab of the certificate manager.

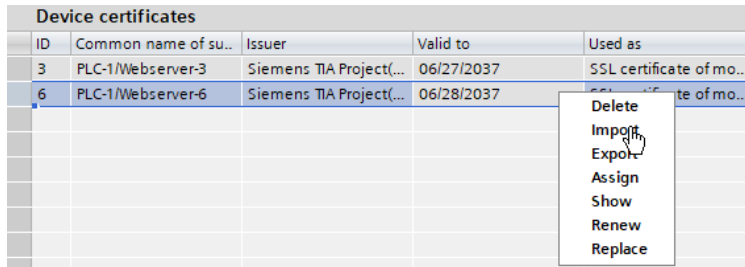
Figure 3-8



ID	Common name of su...	Issuer	Valid to	Used as	Private key
3	PLC-1/Webserver-3	Siemens TIA Project(...	06/27/2037	SSL certificate of mo...	Yes
6	PLC-1/Webserver-6	Siemens TIA Project(...	06/28/2037	SSL certificate of mo...	Yes

At this point, you can view, export, delete or renew the new device certificate, for example.

Figure 3-9



ID	Common name of su...	Issuer	Valid to	Used as
3	PLC-1/Webserver-3	Siemens TIA Project(...	06/27/2037	SSL certificate of mo...
6	PLC-1/Webserver-6	Siemens TIA Project(...	06/28/2037	SSL certificate of mo...

- Delete
- Import
- Export
- Assign
- Show
- Renew
- Replace

3.2 Setting up and testing the browser

In the following instructions the following browsers are used:

- Internet Explorer
- Firefox
- Chrome

Description

With the addition "https" you achieve that the web server transfers its device certificate to the browser. If the CA certificate used to sign the Web server's device certificate is known to the browser, the Web page is considered trusted. Depending on your browser, a padlock may appear in the address bar, which you can click to get more information about the certificate and the issuing certificate company. However, if you try to open the HTTPS version of a page that does not have a valid certificate, a warning appears.

Note

An activated virus scanner with additional browser or mail protection functions can prevent the proper exchange of certificates. You may need to customize these applications or replace them with another product.

Requirement

To establish a secure connection to the Web server, the CA certificate must be present in the certificate store that the browser accesses.

To import the CA certificate into the certificate store, you have the following options:

1. You install the CA certificate directly from TIA Portal. (see [section 2.2](#)).
However, the CA certificate is only stored in the Windows certificate store.

Note

This procedure is not applicable for the Firefox browser, since Firefox uses its own certificate store.

2. You import and install the CA certificate directly into the browser's certificate store. To import and install the CA certificate, you must have saved the CA certificate on the local computer. You have the following options for this:
 - You export the CA certificate from TIA Portal in the format "*.der". ("Certificate-DER coded") (see [section 2.3](#)).
 - You download the CA certificate from the intro page of the web server.

Note

In the following instructions, the CA certificate is loaded, imported and installed from the intro page of the web server.

3.2.1 Internet Explorer or Edge

Note

If you have already imported the CA certificate in the Windows central certificate store (see [section 2.2](#)), then the website of the CPU is already classified as trustworthy and you do not need to make any further adjustments.

Version

The instructions and screenshots were created with Internet Explorer version 11.

Certificate memory

Windows has a central certificate store. Many Windows programs can access the central certificate store if they work with certificates. This has the advantage that the certificates do not have to be imported into the certificate store of each software separately, but only once centrally in the Windows system itself.

If you import and install the CA certificate using Internet Explorer, the CA certificate is stored in the central certificate store. You can view and manage the central certificate store with the management console "mmc".

Download CA Certificate from Web Server and Install Directly

The CA certificate issued by the certification authority can simply be downloaded via web browser and then installed directly.

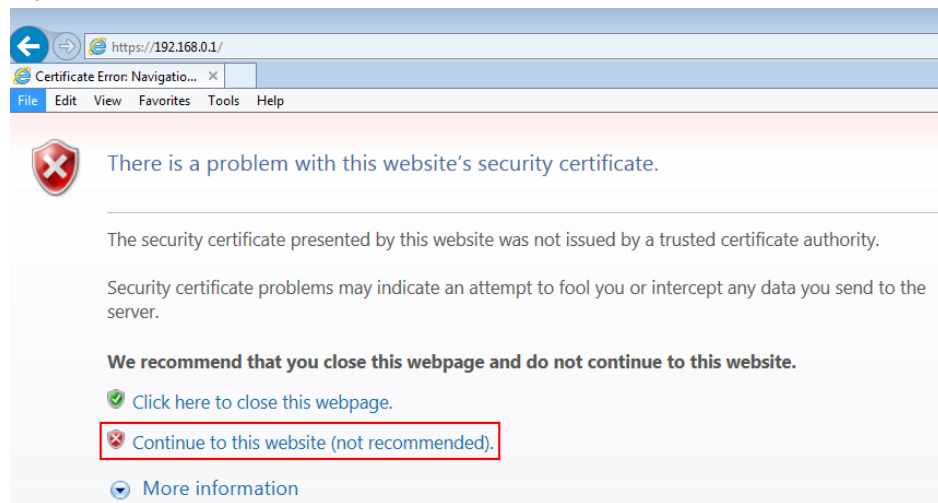
Follow these steps for this purpose:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".

The web page is loading. Since the device certificate of the CPU cannot yet be verified by the missing CA certificate, the web page is classified as insecure. The following message is displayed: "There is a problem with this website's security certificate".

If you know the operator of the web page and if you know that he has no bad intentions, you can access the web page by clicking on the link "Continue to this website (not recommended)" despite the warning.

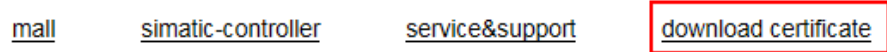
Figure 3-10



3 Safe Web server connection

- The intro page of the web server is opened as an insecure page. Internet Explorer colors the address bar red and reports the certificate error to the right of the address bar.
To download the CA certificate, click on the "Download certificate" menu.

Figure 3-11



- You can choose whether you want to open or save the CA certificate directly. To install the CA certificate directly, click "Open".

Figure 3-12

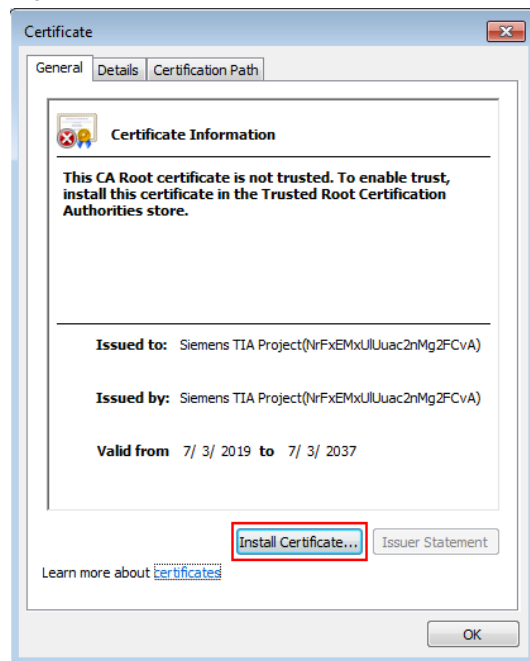


Note

If you want to save the CA certificate and install it later or on a different computer, follow the instructions in the next section.

- The certificate is open. Click on "Install Certificate".

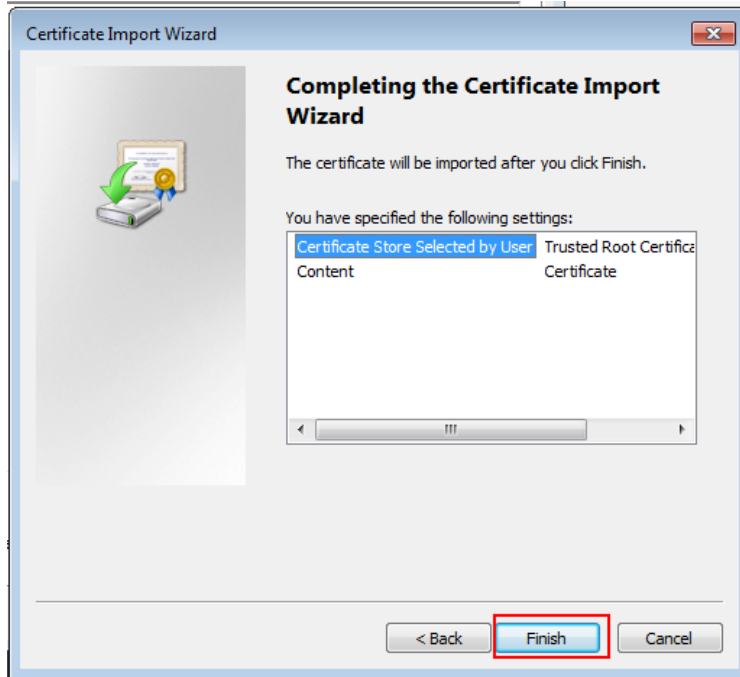
Figure 3-13



5. The wizard is started. Follow the instructions of the installation wizard.
 - Select the local storage as the storage location.
 - Select the certificate store yourself and locate the Trusted Root Certification Authorities folder.

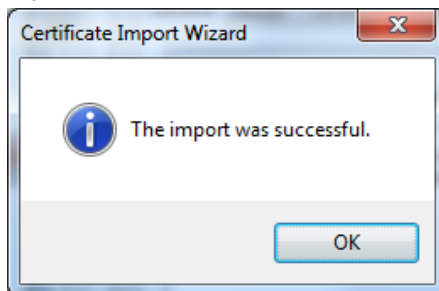
The "Finish" button imports the certificate into the selected folder. Before the wizard issues a security warning, which must be acknowledged with "Yes".

Figure 3-14



6. The wizard completes the successful import process with the following message, which you must confirm with "OK".

Figure 3-15

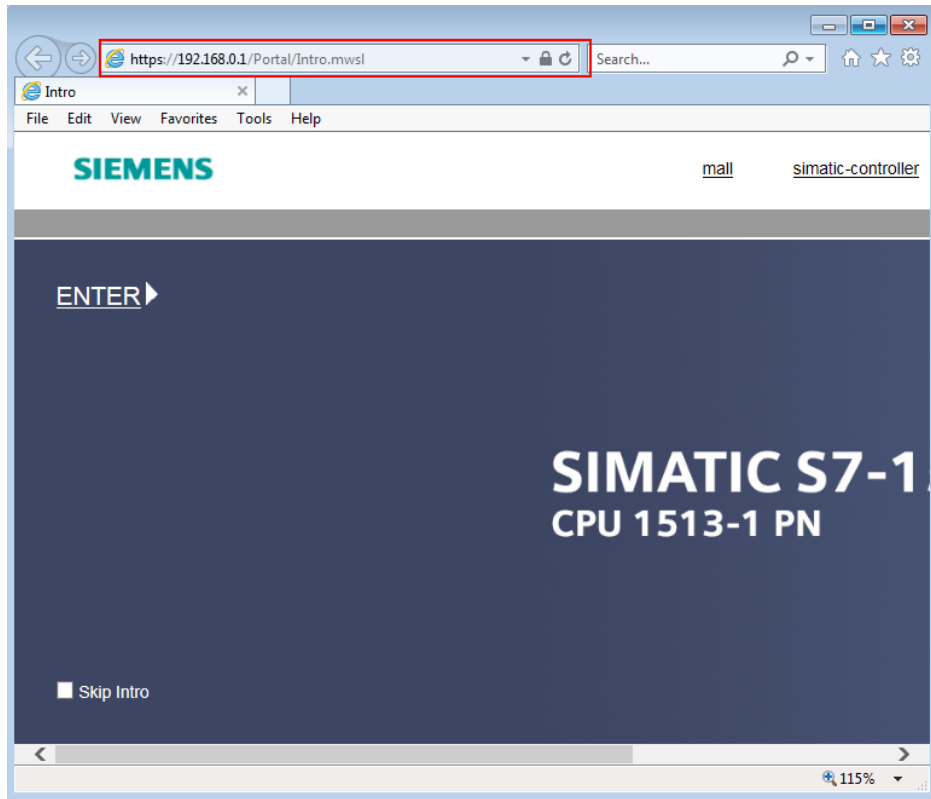


7. Close all instances of Internet Explorer, and then restart the program.

Result

You have imported the CA certificate into the Windows certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-16

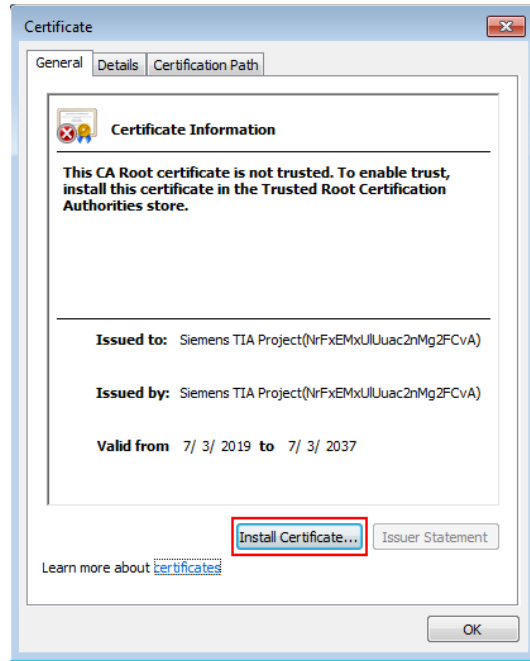


Importing and Installing a CA Certificate

If you have saved the CA certificate on the local computer, for example, by exporting it from TIA Portal or downloading it and then saving it, you can import the CA certificate into the central certificate store as follows:

1. On your computer, navigate to the directory with the CA certificate. Open the CA certificate with a double-click and click on "Install Certificate".

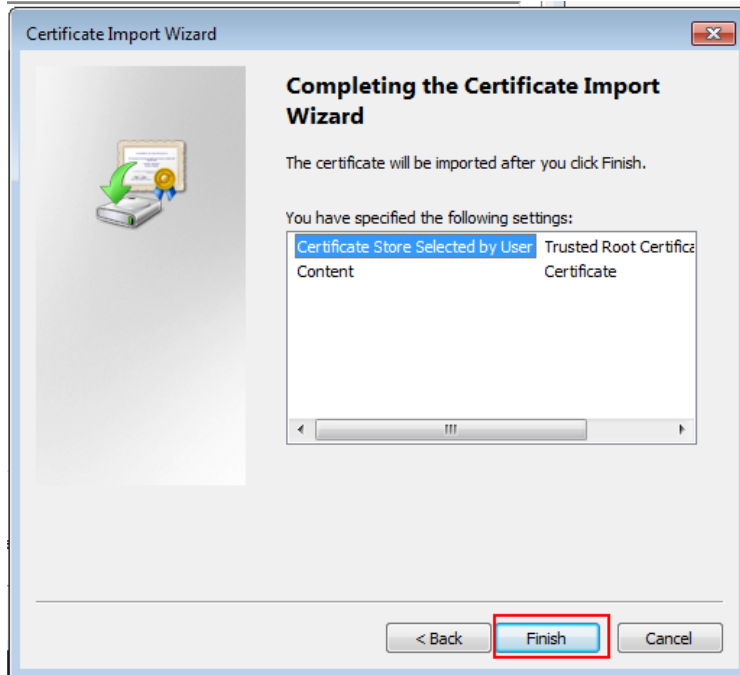
Figure 3-17



2. Follow the instructions of the Wizard.
 - Select the local storage as the storage location.
 - Select the certificate store yourself and locate the Trusted Root Certification Authorities folder.

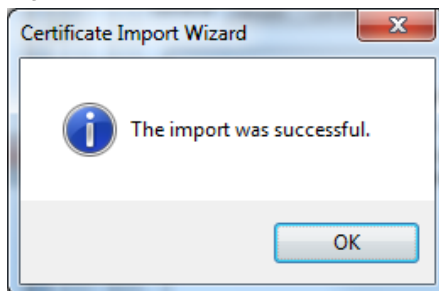
The "Finish" button imports the certificate into the selected folder. Before the wizard issues a security warning, which must be acknowledged with "Yes".

Figure 3-18



3. The wizard completes the successful import process with the following message, which you must confirm with "OK".

Figure 3-19

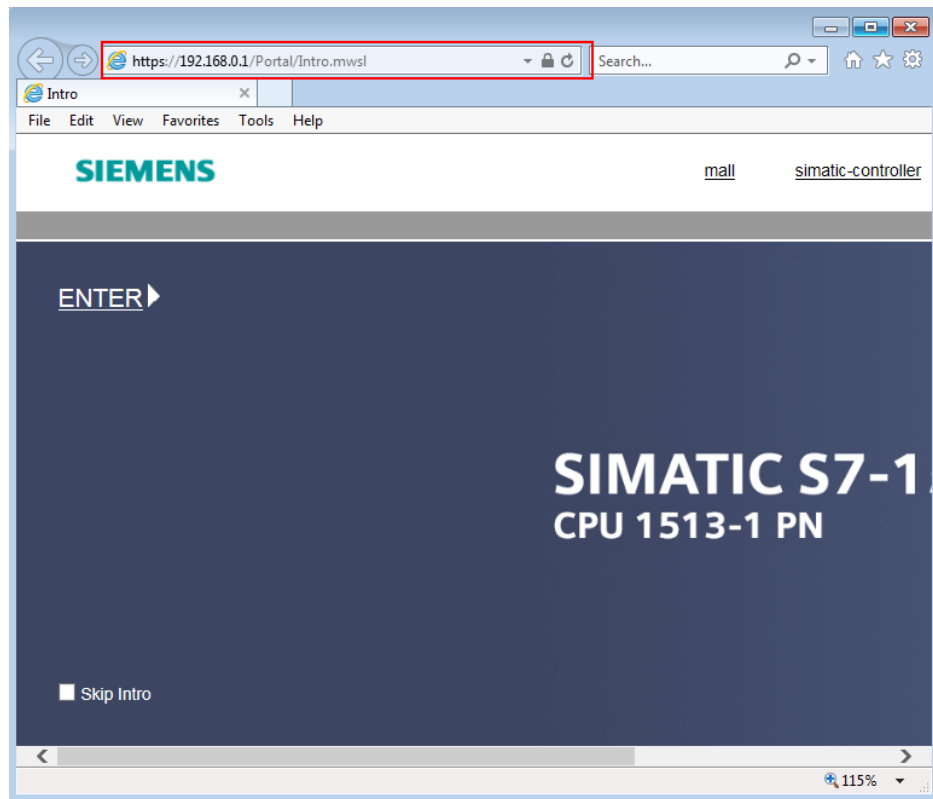


4. Close all instances of Internet Explorer, and then restart the program.

Result

You have imported the CA certificate into the Windows certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-20



3.2.2 Google Chrome

Note

If you have already imported the CA certificate in the central certificate store of Windows (e.g. through [section 2.2](#) or [section 3.2.1](#)), then the web page of the CPU is already classified as trustworthy and you do not need to make any further adjustments.

Version

The manual and the screenshots were created with Google Chrome Version 75.0.3770.100.

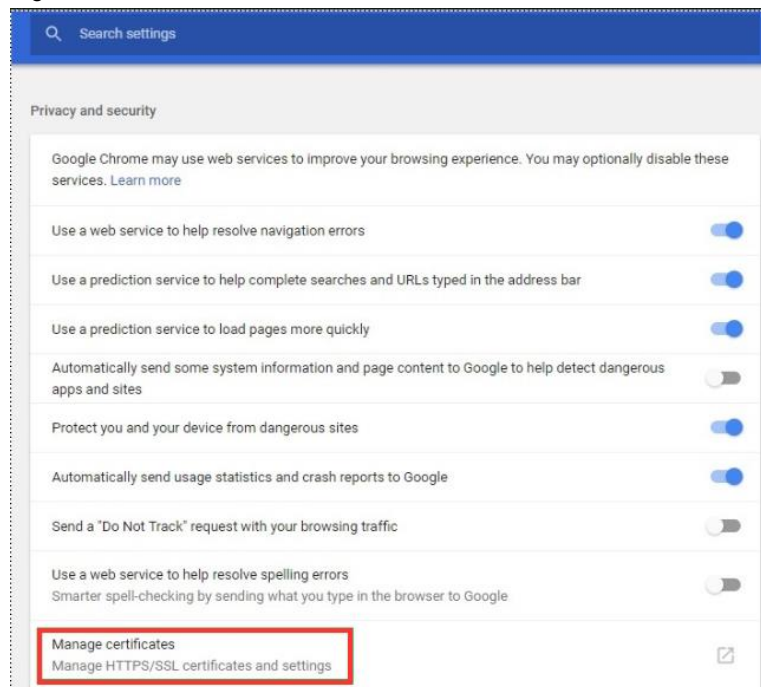
Certificate memory

The Google Chrome browser manages the certificates itself, but accesses the central Windows certificate store.

To check whether the CA certificate is known to the browser, proceed as follows:

1. Open the settings in Chrome. Under "Advanced > Privacy and Security" you will find the entry "Manage certificates". Click on the entry:

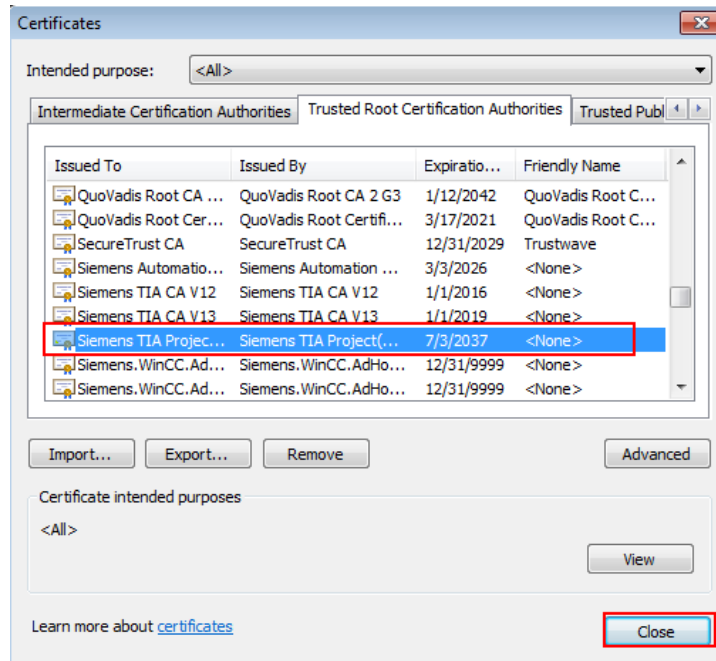
Figure 3-21



3 Safe Web server connection

2. The "Certificates" window opens. Switch to the "Trusted Root Certification Authorities" tab. If you have already installed the CA certificate, it is displayed in the list. Close the dialog with "Close".

Figure 3-22



Download CA Certificate from Web Server and Install Directly

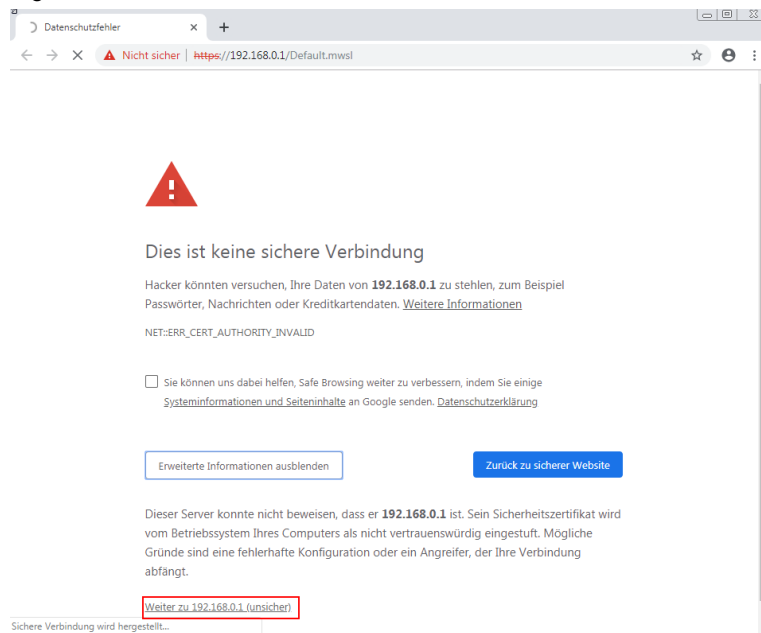
The CA certificate issued by the certification authority can simply be downloaded via web browser and then installed directly.

Follow these steps for this purpose:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".

The web page is loading. Since the device certificate of the CPU cannot yet be verified by the missing CA certificate, the web page is classified as insecure. If you know the operator of the web page and if you know that he has no bad intentions, you can access the web page by clicking on the link ("Go to <IP address of CPU>(unsecure)") despite the warning. You can find the link by clicking on the "Advanced" button.

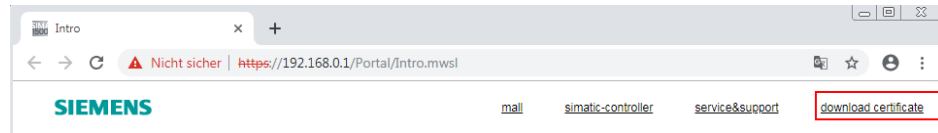
Figure 3-23



3 Safe Web server connection

- The intro page of the web server is opened as an insecure page. Chrome colors the "https" of the address red and reports the certificate error at the right edge of the address bar. To download the CA certificate, click on the "Download certificate" menu. Confirm the safety instruction with "Keep".

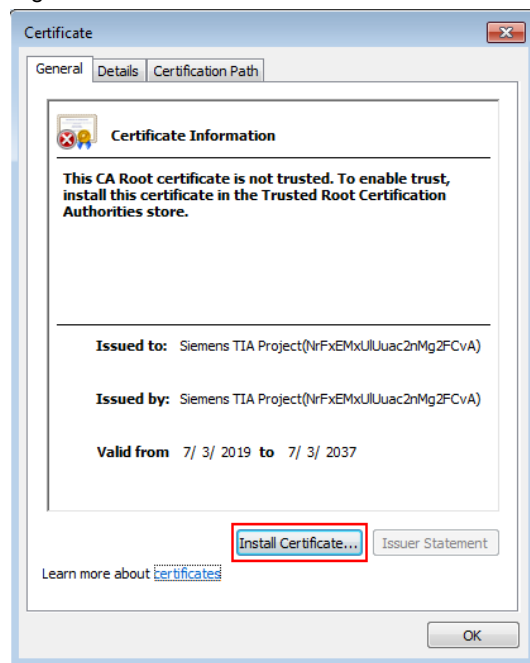
Figure 3-24



- The file will be saved in the preferred download folder. The file is also displayed in the lower left corner of the screen. Here you can choose whether you want to open the CA certificate directly or open the storage folder. To install the CA certificate directly, click on the displayed file and select "Open". Confirm the Windows security note with "Open".

- The certificate is open. Click on "Install Certificate".

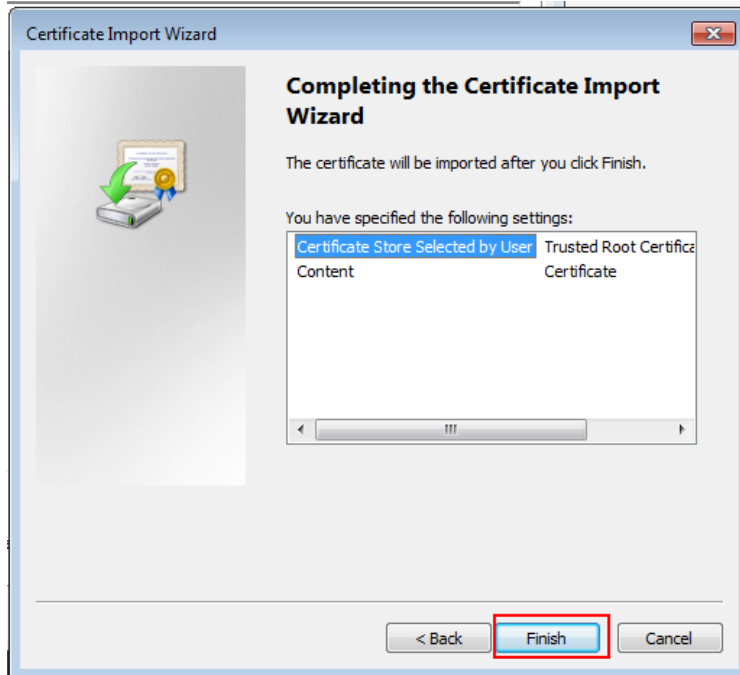
Fig. 3-25



5. The wizard is started. Follow the instructions of the installation wizard.
 - Select the local storage as the storage location.
 - Select the certificate store yourself and locate the Trusted Root Certification Authorities folder.

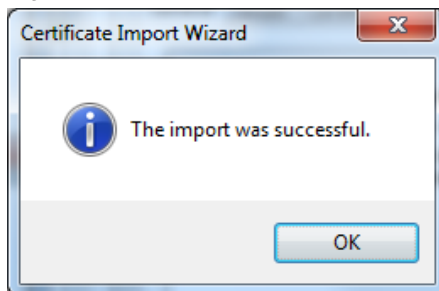
The "Finish" button imports the certificate into the selected folder. Before the wizard issues a security warning, which must be acknowledged with "Yes".

Figure 3-26



6. The wizard completes the successful import process with the following message, which you must confirm with "OK".

Figure 3-27



7. Close all instances of Chrome and then restart the program.

3 Safe Web server connection

Result

You have imported the CA certificate into the Windows certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-28

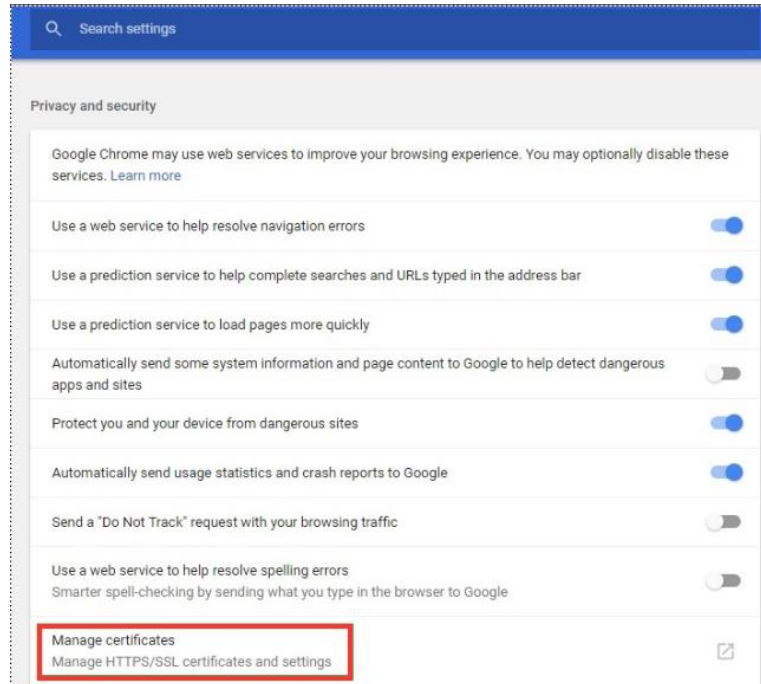


Importing and Installing a CA Certificate

If you have saved the CA certificate on the local computer, for example, by exporting it from TIA Portal or downloading it and then saving it, you can import the CA certificate into the central certificate store as follows:

1. Open the settings in Chrome. Under "Advanced > Privacy and Security" you will find the entry "Manage certificates". Click on the entry:

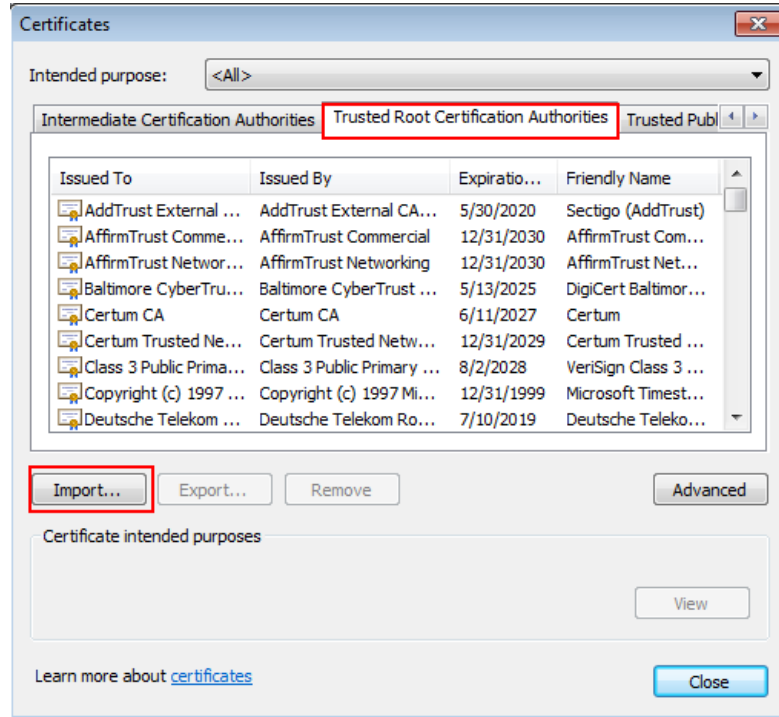
Figure 3-29



3 Safe Web server connection

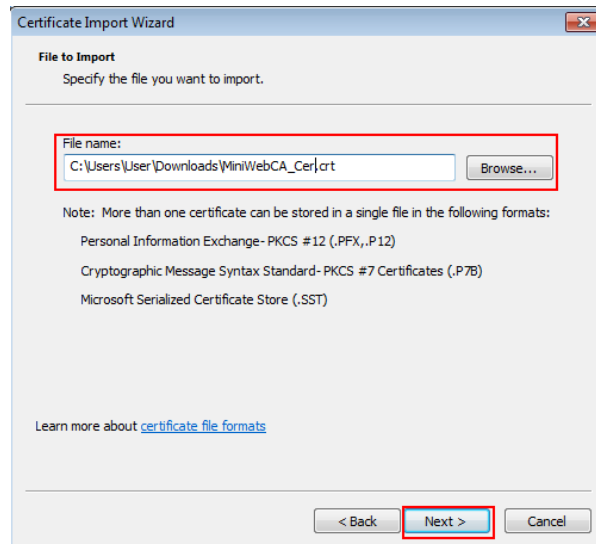
2. The "Certificates" window opens. Select the "Trusted Root Certification Authorities" tab and click the "Import" button.

Figure 3-30



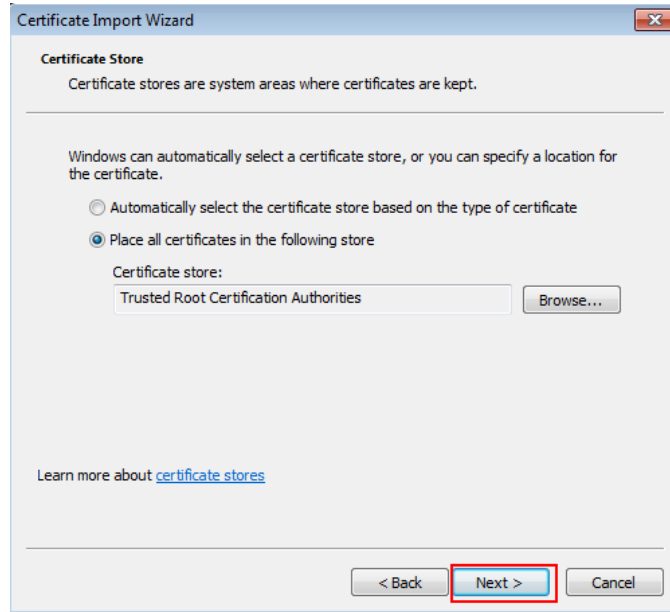
3. The wizard for importing the certificate is started. Use "Browse" to select the storage location of the certificate. Then click on the "Next" button.

Figure 3-31



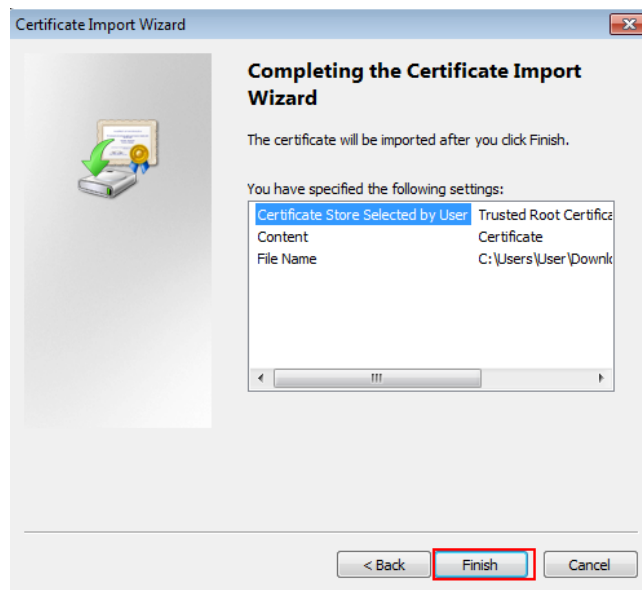
- The wizard selects the correct location using the register preselection in step 2. Click on "Next".

Figure 3-32



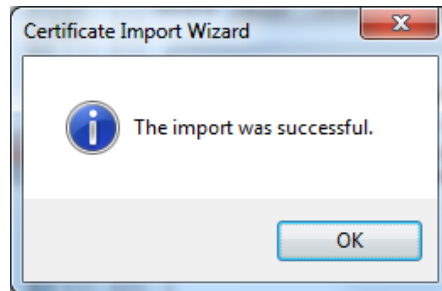
- The "Finish" button imports the certificate into the selected folder. Before the wizard issues a security warning, which must be acknowledged with "Yes".

Figure 3-33



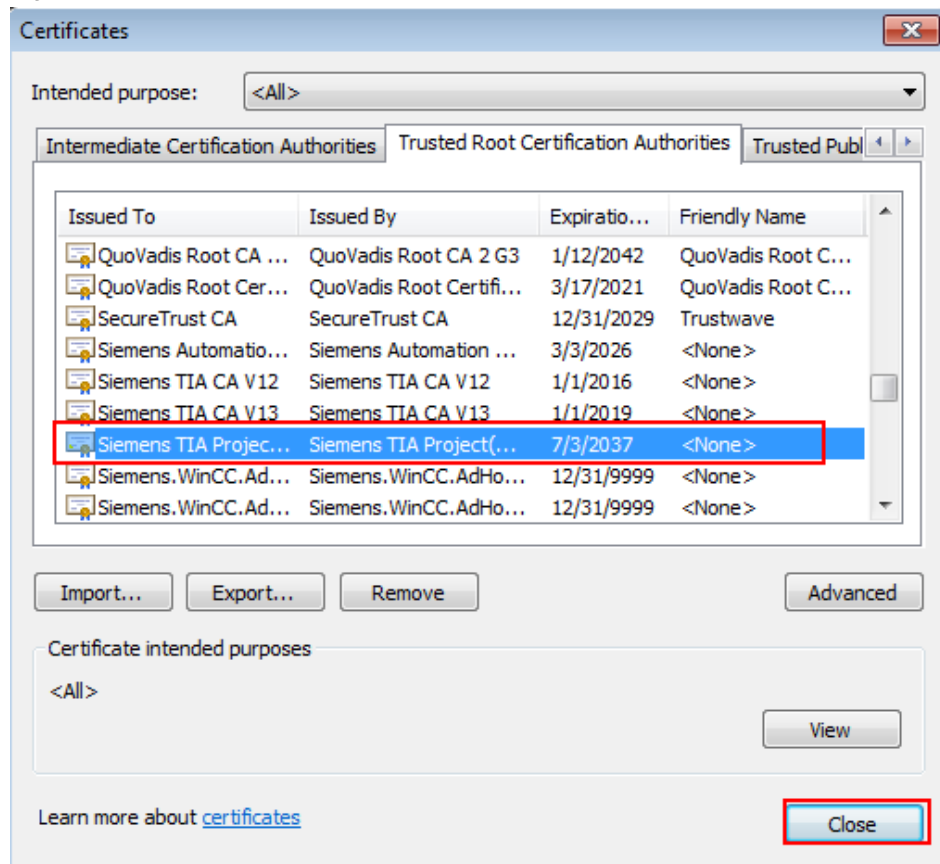
- The wizard completes the successful import process with the following message, which you must confirm with "OK".

Figure 3-34



- The CA certificate has been imported and can be viewed in the "Trusted Root Certification Authorities" tab. Close the dialog with "Close".

Figure 3-35



- Close all instances of Chrome and then restart the program.

Result

You have imported the CA certificate into the Windows certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-36



3.2.3 Firefox

Version

The instructions and screenshots were created with Firefox Quantum version 60.7.2.

Certificate memory

Unlike Internet Explorer or Google Chrome, Firefox uses its own certificate store by default.

Loading a CA Certificate from the Web Server

The CA certificate issued by the certification authority can easily be downloaded via web browser.

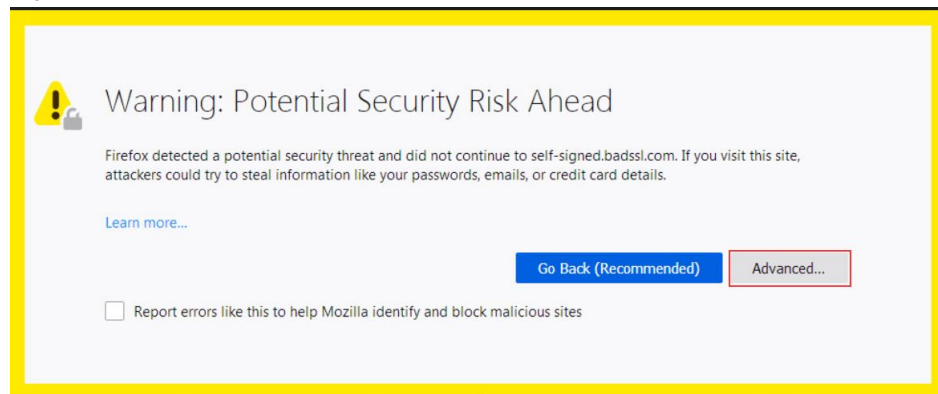
Follow these steps for this purpose:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".

On web pages that are actually considered secure, Firefox checks the validity of the certificate issued by the web page. If the certificate cannot be verified, Firefox rejects the connection to the web page and instead displays a page with the error message "Warning: Potential Security Risk Ahead".

If the web page operator is known and if you know that he has no bad intentions, you can add the web page as an exception by clicking on the "Advanced" button and open it despite the warning.

Figure 3-37



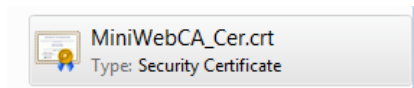
3 Safe Web server connection

2. The intro page of the web server is opened as an insecure page. Firefox reports the certificate error at the right edge of the address bar. To download the CA certificate, click on the "Download certificate" menu.

Figure 3-38



3. Save the CA certificate on the local computer.



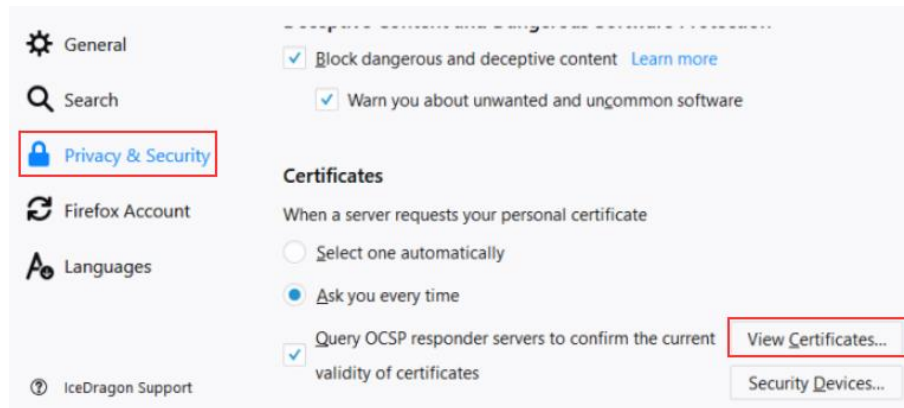
Importing and Installing a CA Certificate

If you have saved the CA certificate on the local machine, for example, by exporting it from TIA Portal or downloading it and then saving it, you can import the CA certificate into the Firefox certificate store as follows

Proceed as follows:

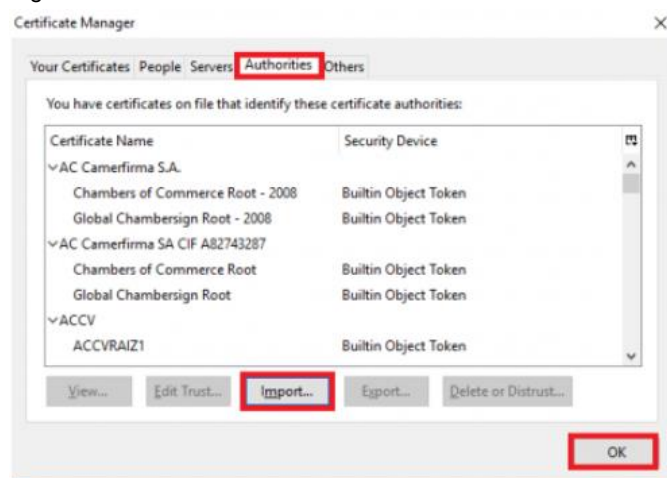
1. Open the settings in Firefox. Under "Privacy & Security" you will find the "Certificates" tab. Click on the button "View Certificates...".

Figure 3-40



2. The certificate administration of Firefox is opened. Go to the tab "Authorities" and click on the button "Import...". ("Import...").

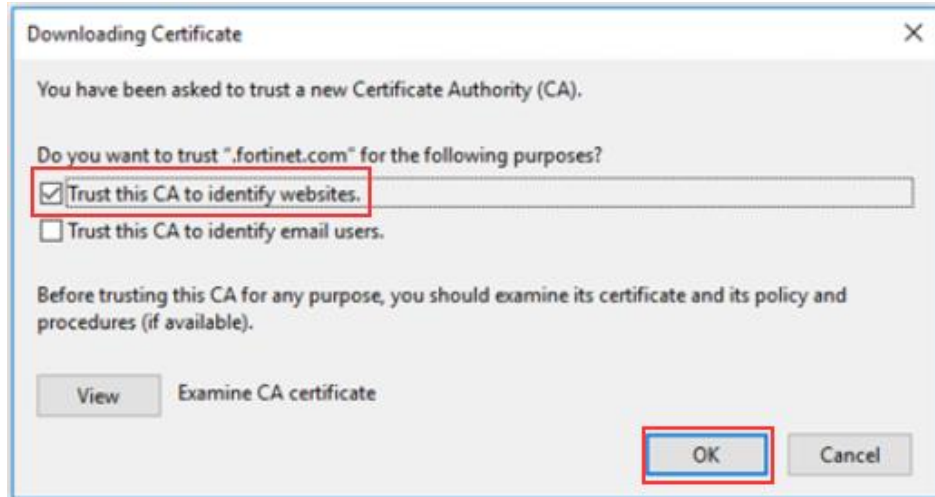
Figure 3-41



3 Safe Web server connection

3. The wizard is started. Follow the instructions of the installation wizard.
 - Select the local storage as the storage location.
 - In the "Download this certificate" dialog, select the entry "Trust this CA to identify websites".
Confirm the dialog with "OK".

Figure 3-42

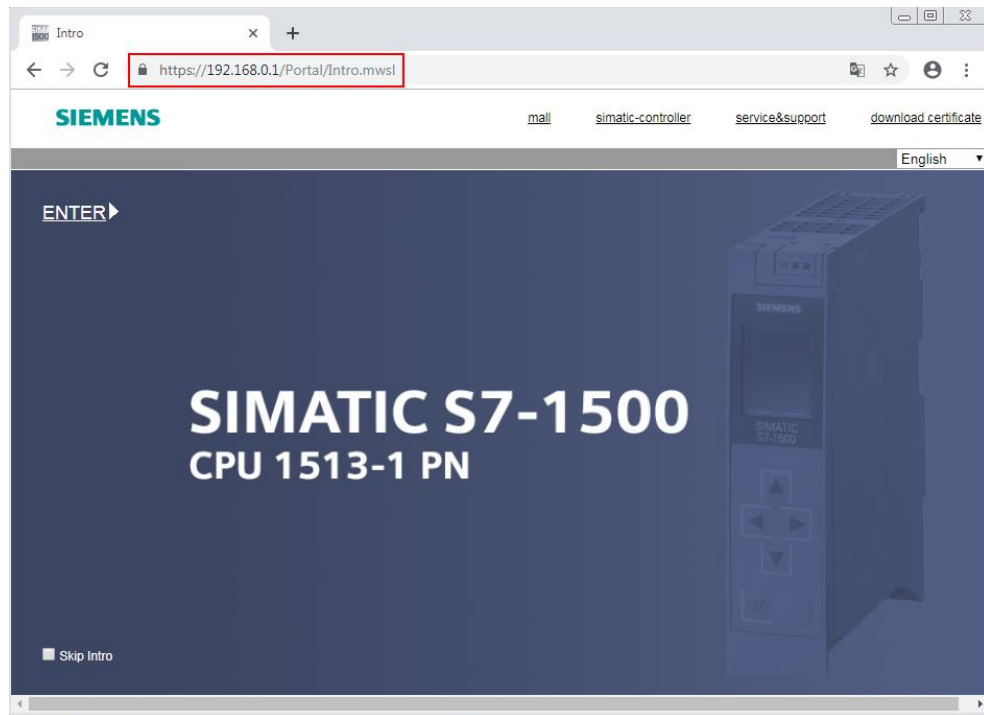


4. If the import process was successful, the CA certificate is listed in the Certificate Manager in the "Authorities" tab. Close the dialog by clicking "OK".
5. Close all instances of Firefox and then restart the program.

Result

You have imported the CA certificate into the Firefox certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-43



3.2.4 Operating system Android

Version

The manual and screenshots were tested with a Samsung Tablet 2016 with Android version 8.1.0. A lock screen type is not set up. Google Chrome version 75.0 was used.

Download CA Certificate from Web Server and Install Directly

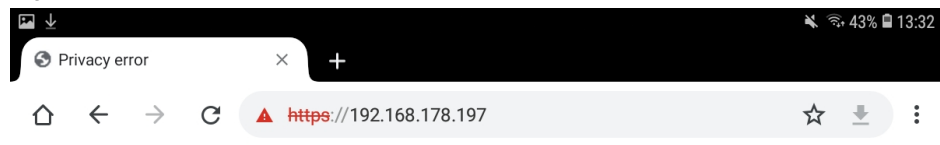
The CA certificate issued by the certification authority can simply be downloaded via web browser and then installed directly.

Follow these steps for this purpose:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".

The web page is loading. Since the device certificate of the CPU cannot yet be verified by the missing CA certificate, the web page is classified as insecure. If the operator of the web page is known and if you know that he has no bad intentions, you can access the web page by clicking on the link "Proceed to <IP address of CPU>(unsafe)". You can find the link by clicking on the "Advanced" button.

Figure 3-44



Your connection is not private

Attackers might be trying to steal your information from **192.168.178.197** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Safe Browsing by sending some [system information and page content](#) to Google.
[Privacy policy](#)

Hide advanced

Back to safety

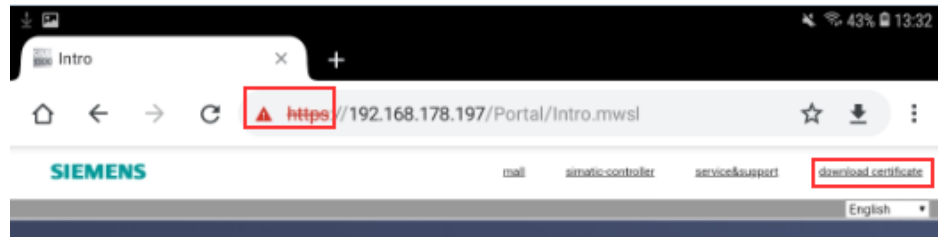
This server could not prove that it is **192.168.178.197**; its security certificate is not trusted by your device's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.178.197 \(unsafe\)](#)

3 Safe Web server connection

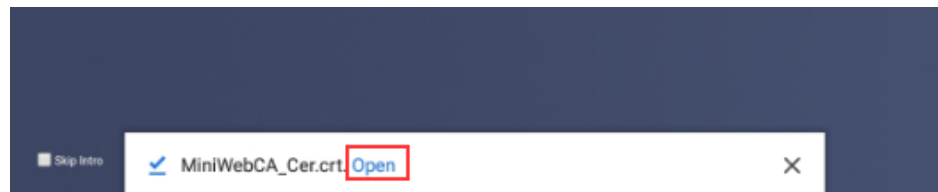
- The intro page of the web server is opened as an insecure page. Chrome colors the "https" of the address red and reports the certificate error at the right edge of the address bar. To download the CA certificate, click on the "Download certificate" menu.

Figure 3-45



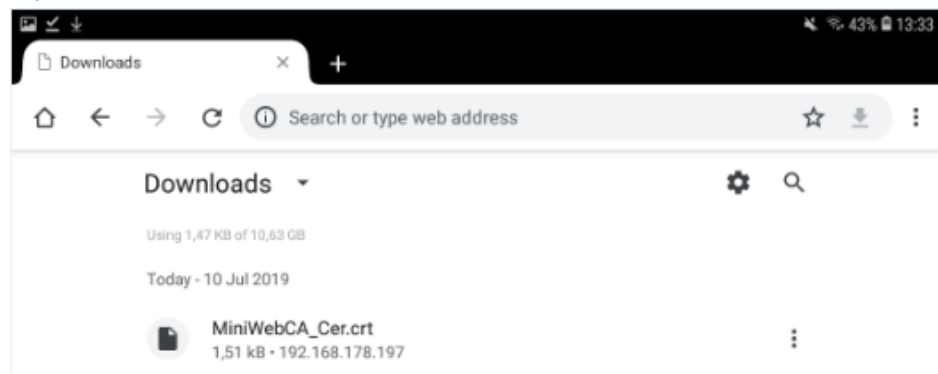
- The file will be saved in the preferred download folder. The file is also displayed in the lower left corner of the screen. Click on the link "Open".

Figure 3-46



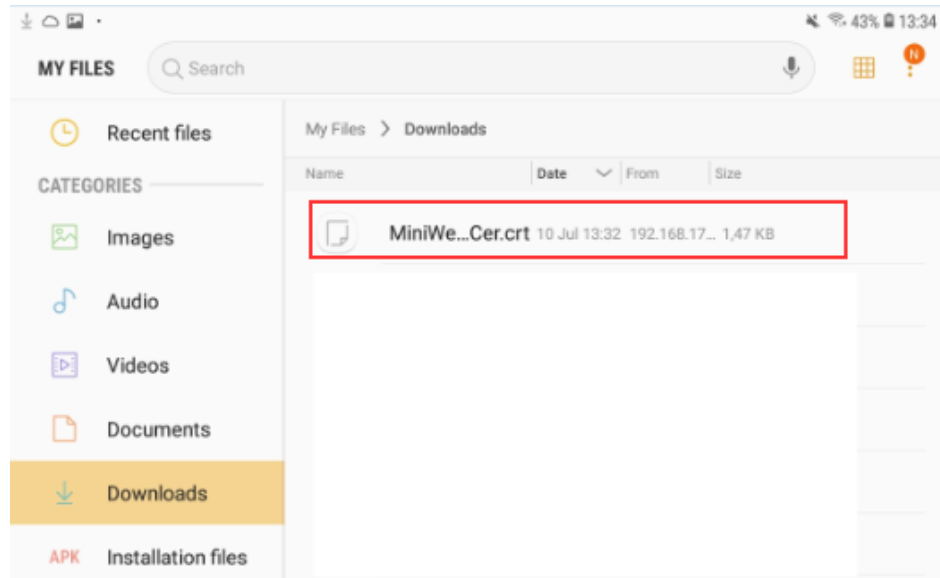
- The CA certificate is stored in the download folder and can be viewed.

Figure 3-47



5. You cannot open the certificate directly in the download folder. Open the file manager on your tablet. Under "Downloads" you will find the CA certificate.

Figure 3-48



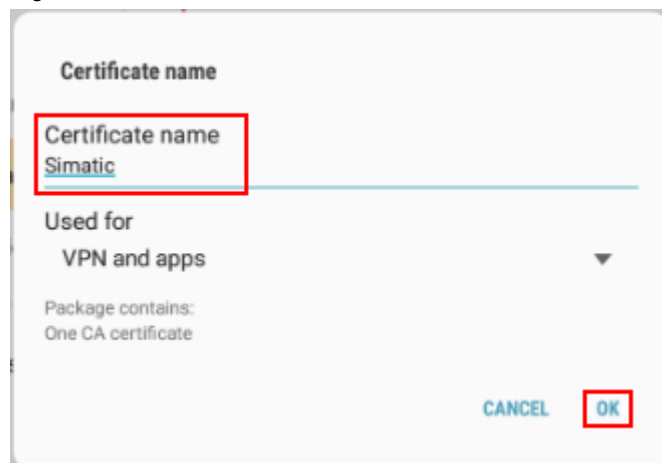
6. To install the CA certificate, press the "MiniWebCA_Cer" file. You must define a certificate name (in this example "Simatic"). The name can be chosen arbitrarily. For purpose of use, leave the default setting "VPN and apps" ("VPN and apps").

Note

If you have already stored a lock screen type in the tablet, such as a password or security pattern, you are prompted to enter it now.

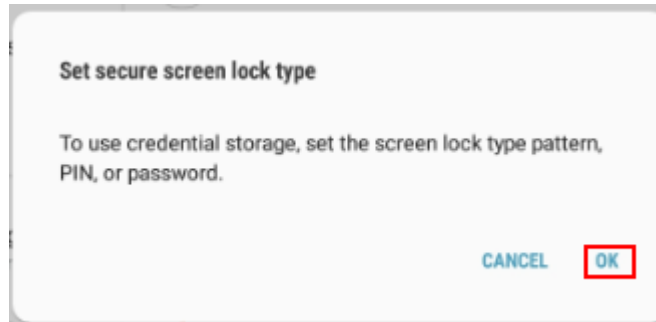
Activate this setting with "OK".

Figure 3-49



7. When you install certificates, you must set up a lock screen type. Confirm the message with "OK".

Figure 3-50



8. Select the lock screen type. In this example, a PIN query is set up.

Note

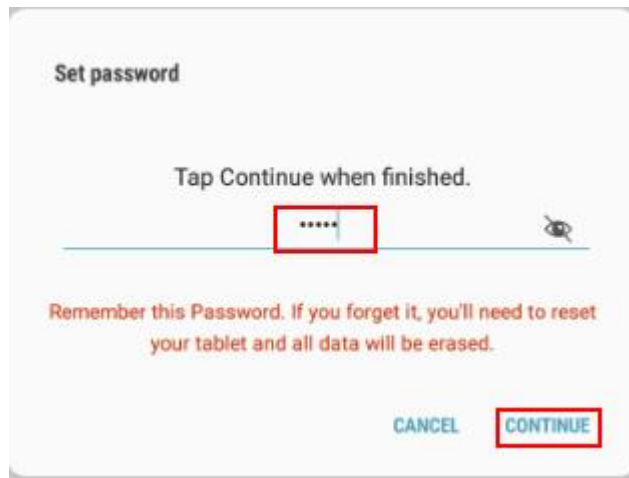
From now on, the security prompt will always be prompted when you activate and switch on the tablet.

Figure 3-51



9. Assign a PIN and then click on "Continue".

Figure 3-52



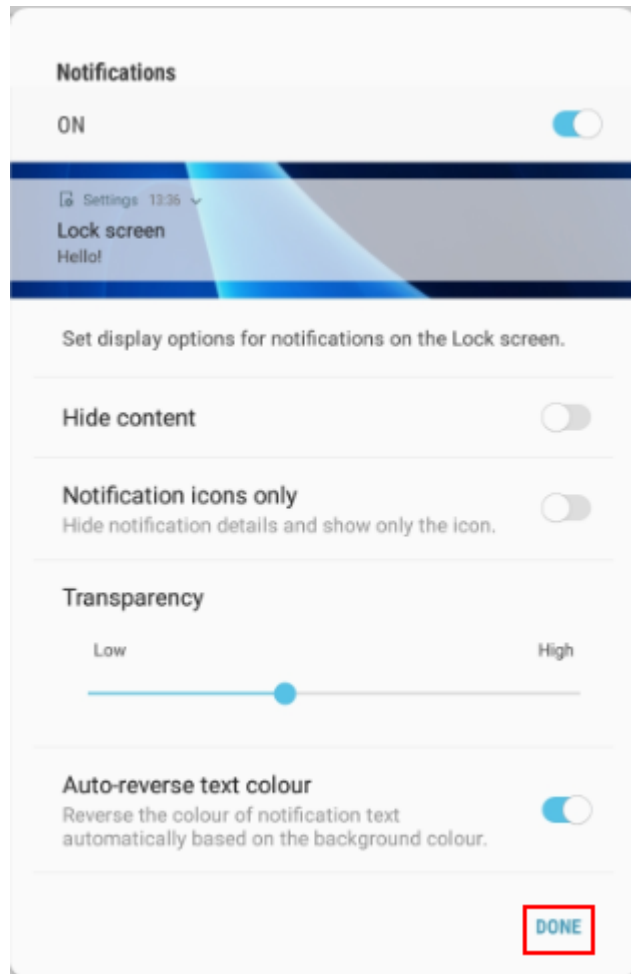
10. Confirm the PIN and then click on the "OK" button.

Figure 3-53



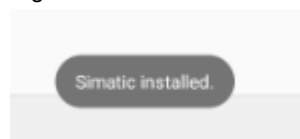
11. Specify the type of notifications on your lock screen. Finish the installation process with "Done".

Figure 3-54



12. The CA certificate has been installed.

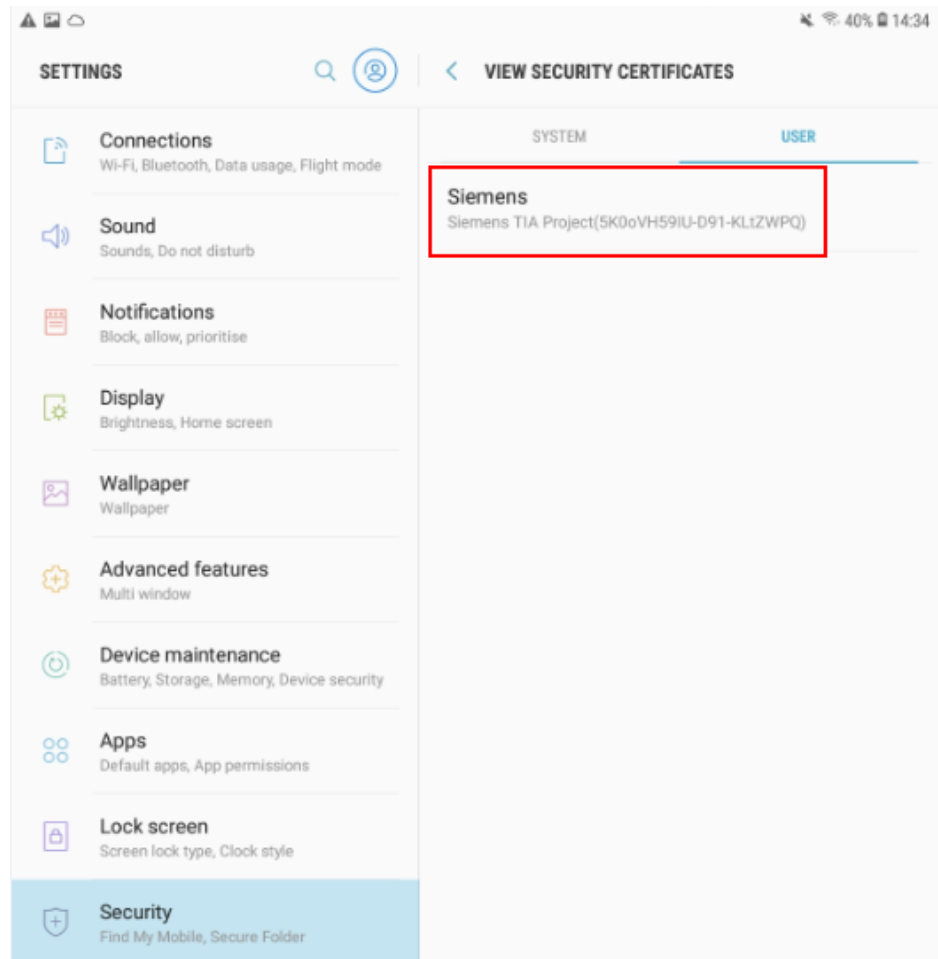
Figure 3-55



3 Safe Web server connection

13. The certificate can then be viewed under "Security > Other security settings > View security certificates" in the "Users" tab.

Figure 3-56

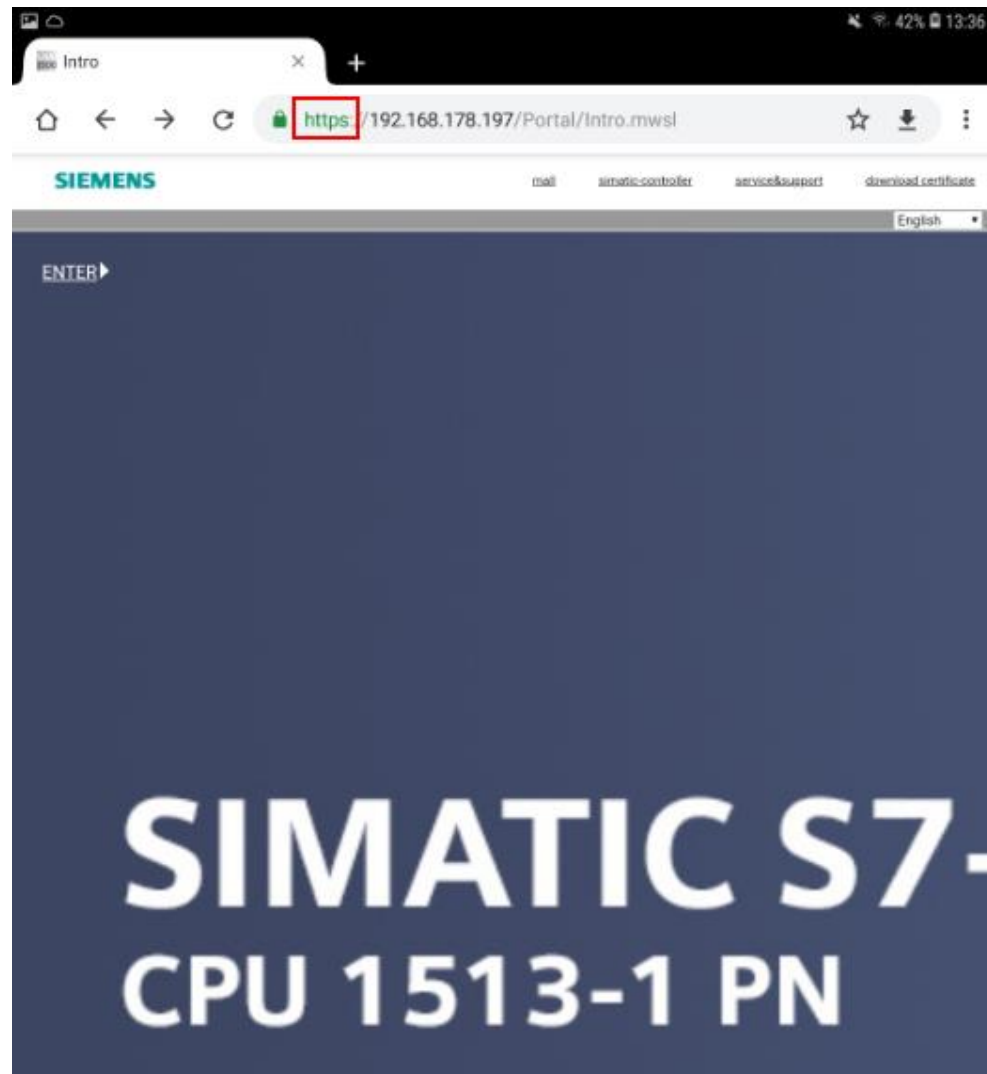


14. Close all instances of Chrome and then restart the program.

Result

You have imported the CA certificate into the Android certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-57



3.2.5 Operating system iOS

Version

The manual and the screenshots were tested with an iPad with iOS version 12.1.4. A lock screen is configured with PIN entry. Safari was used.

Download CA Certificate from Web Server and Install Directly

The CA certificate issued by the certification authority can simply be downloaded via web browser and then installed directly.

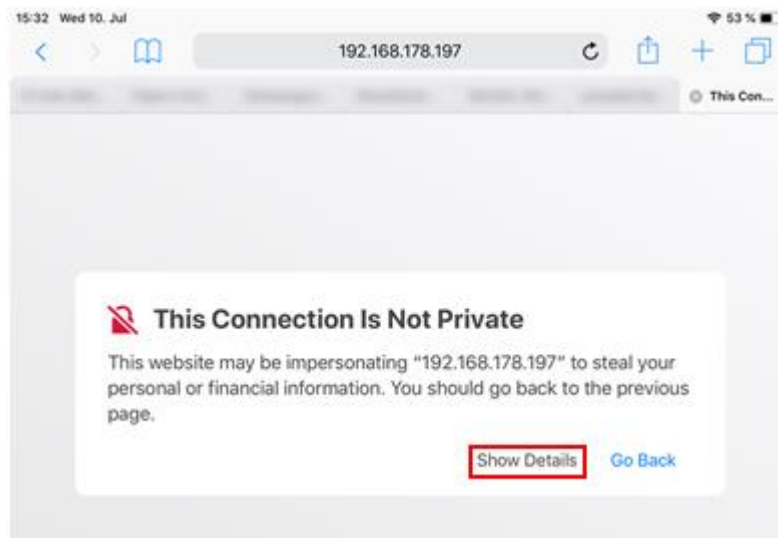
Follow these steps for this purpose:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".

The web page is loading. Since the device certificate of the CPU cannot yet be verified by the missing CA certificate, the Web page is classified as insecure and the message "This Connection Is Not Private" is displayed.

By clicking on the button "Show details" you can get further information.

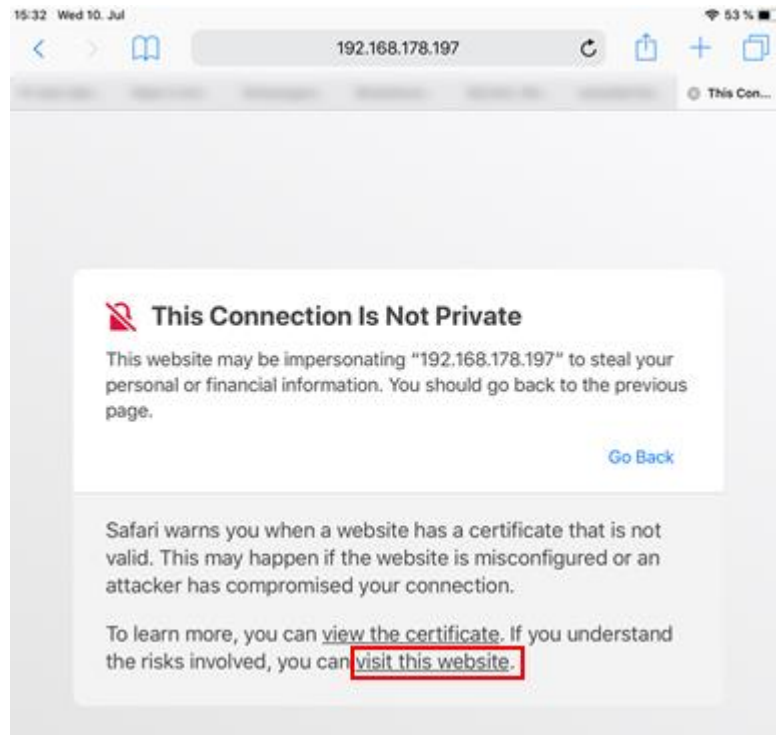
Figure 3-58



3 Safe Web server connection

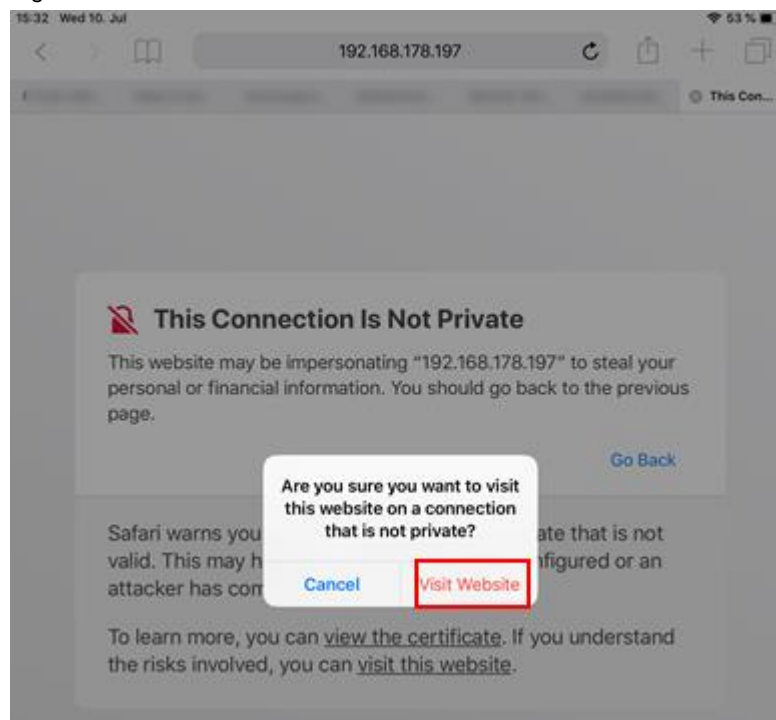
2. If the web page operator is known and you know that he has no bad intentions, you can use the link "visit this website" to access the website despite the warning.

Figure 3-59



3. Confirm the security advice with "Visit Website".

Figure 3-60



3 Safe Web server connection

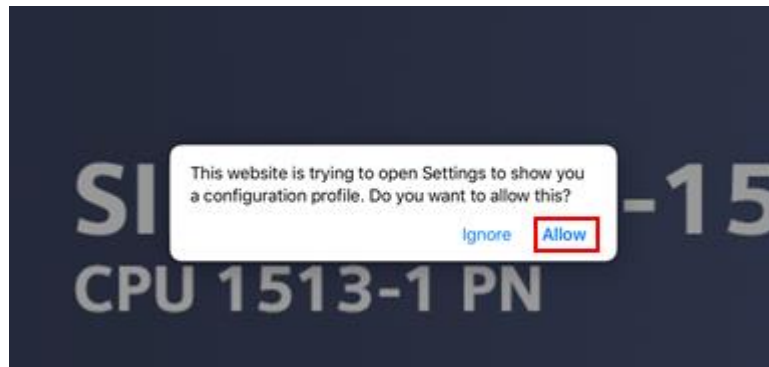
- The intro page of the web server opens.
To download the CA certificate, click on the "Download certificate" menu.

Figure 3-61



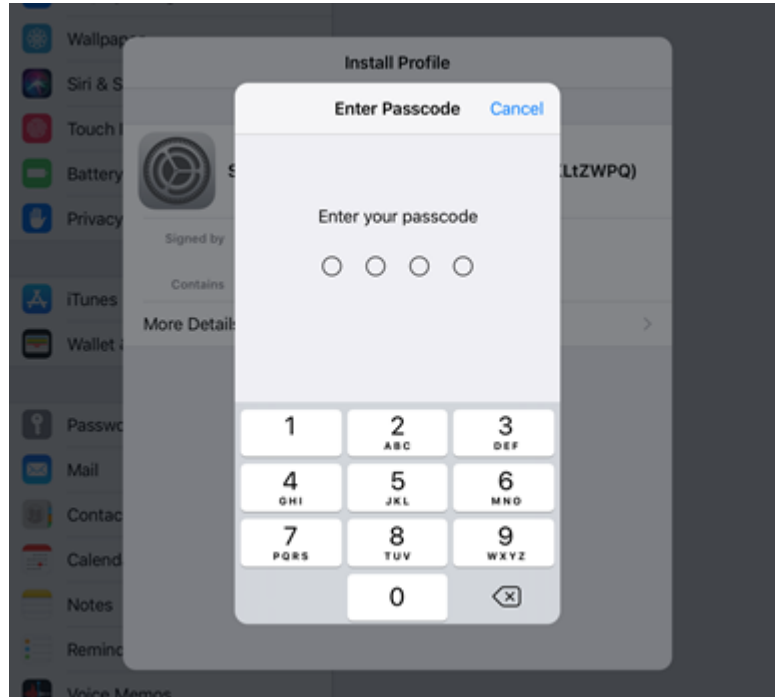
- The certificate is declared as a "Configuration profile" by iOS. To view the certificate (profile), the web page must have access to your settings in iPad. This requires your permission. Confirm the message with "Allow".

Figure 3-62



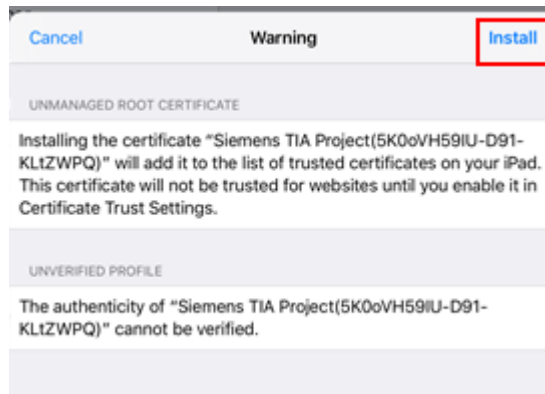
- To view the certificate (profile), you must enter the security ID that protects your iPad. In this example, the iPad is protected with a PIN entry.

Figure 3-63



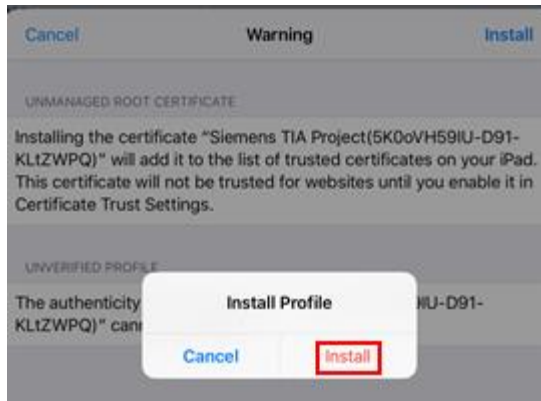
- A security warning is displayed indicating that you must manually enable trust for a certificate (profile) that you have downloaded from a Web page after installation. The certificate trust administration addressed in the warning can be found in the iPad settings under "General > About > Certificate Trust Settings". Click "Install".

Figure 3-64



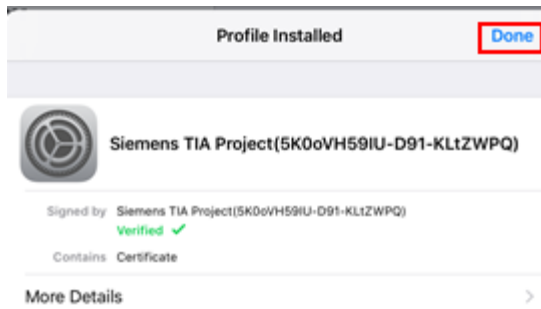
8. Confirm the installation request again with "Install".

Figure 3-65



9. The certificate has been installed and is trusted. Close the dialog by clicking "Done".

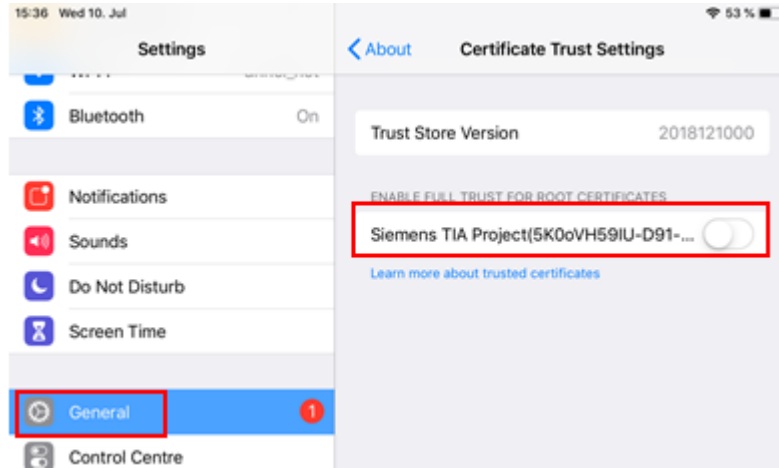
Figure 3-66



3 Safe Web server connection

10. If you install a certificate (profile) that you downloaded from a Web page, you must manually activate trust for the CA certificate. You were already informed of this in the warning in step 7.
To activate the certificate, go to the iPad settings and go to the menu "General > About > Certificate Trust Settings".

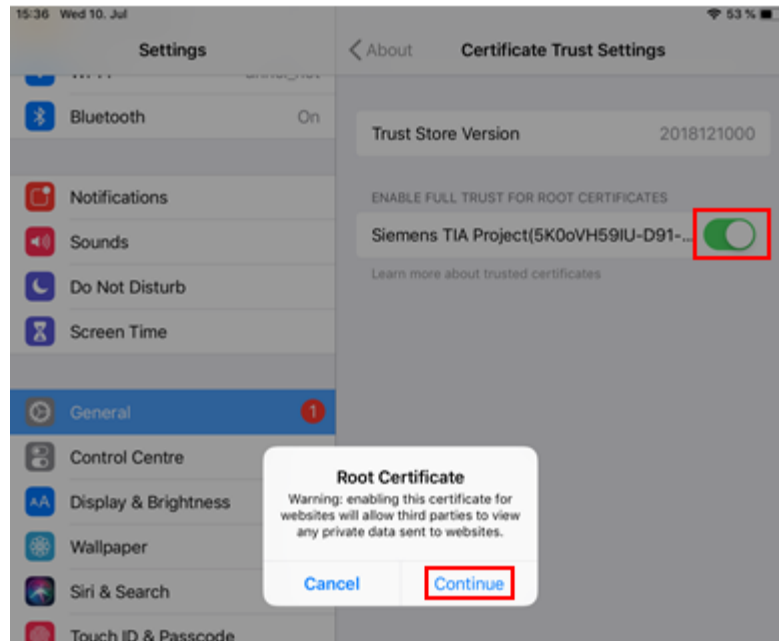
Figure 3-67



3 Safe Web server connection

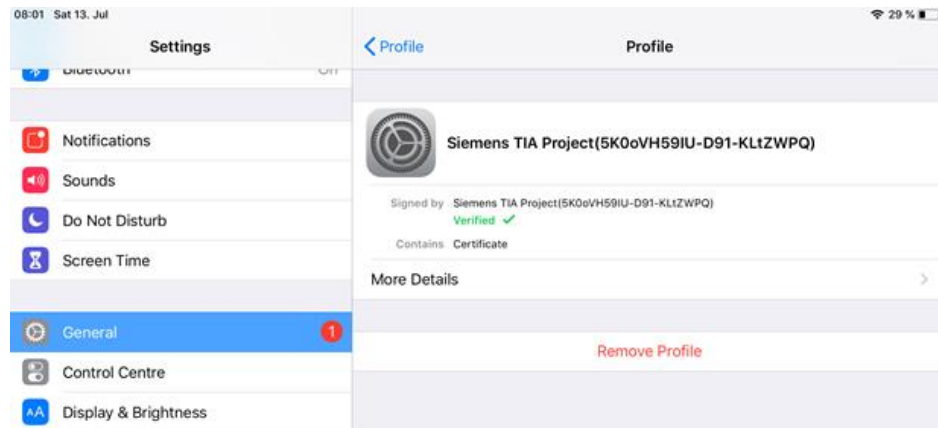
11. Under "Enable full trust for root certificates", enable the trust for the certificate. Confirm the safety note with "Continue".

Figure 3-68



12. You can view and delete the certificate in the iPad settings under "General > Profile".

Figure 3-69

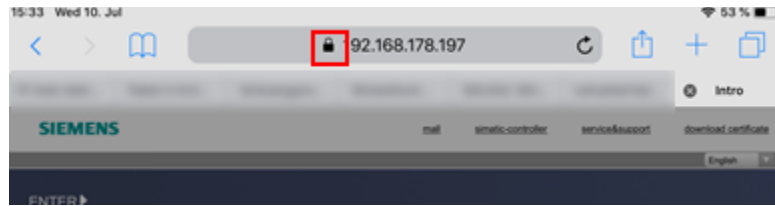


13. Close all instances of Safari and restart the application.

Result

You have imported the CA certificate into the iOS certificate store. The web page of the CPU is now classified as trustworthy.

Figure 3-70



Alternative procedure

If security policies are installed to prevent unsecure access to the web server, the certificate must be installed in another way to download the certificate. The easiest way is to send the certificate via an encrypted e-mail. In iOS, the attachment of the e-mail is then opened, the certificate is displayed and can be installed.

3.3 Checking certificates

Note The verification of the certificates is shown by the browser "Internet Explorer".

Requirement

To establish a secure connection to the Web server and compare the certificates, you must have imported and installed the CA certificate in the Windows certificate store.

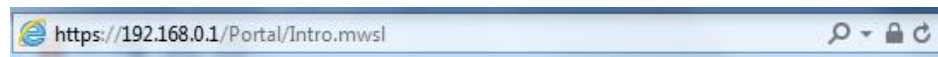
Testing certificates

Certificates are used to verify an identity or other security-critical applications. To determine that this certificate is genuine and has not been forged by an attacker, you should match the device certificate signature with the CA certificate signature.

To check the authenticity of the device certificate, proceed as follows:

1. Open the intro page of the web server of the CPU via the address "https://<IP address of the CPU>".
When you connect to the web server, the browser pulls the device certificate of the CPU and compares it with the CA certificate installed on the PC. If the certificates match in the signature, the intro page is classified as trustworthy and displayed without a security warning.

Figure 3-71



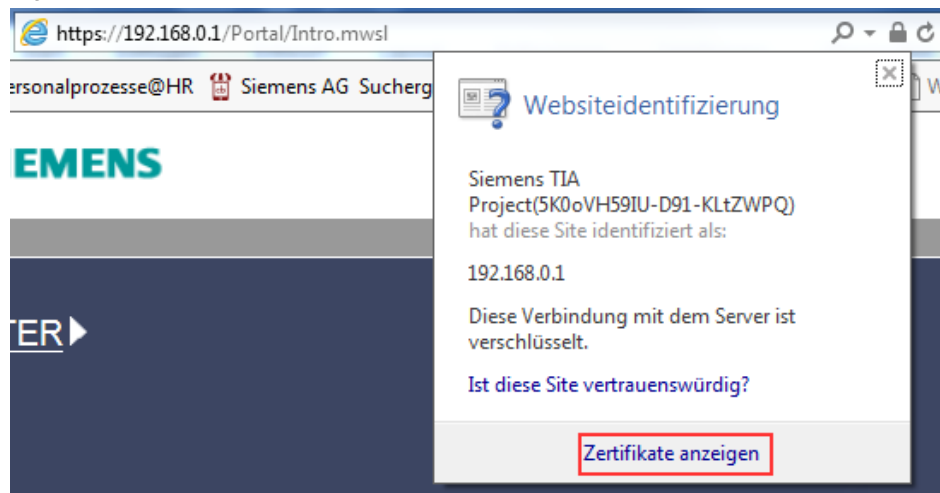
2. For information about the device certificate, click the lock icon in the address bar.

Figure 3-72



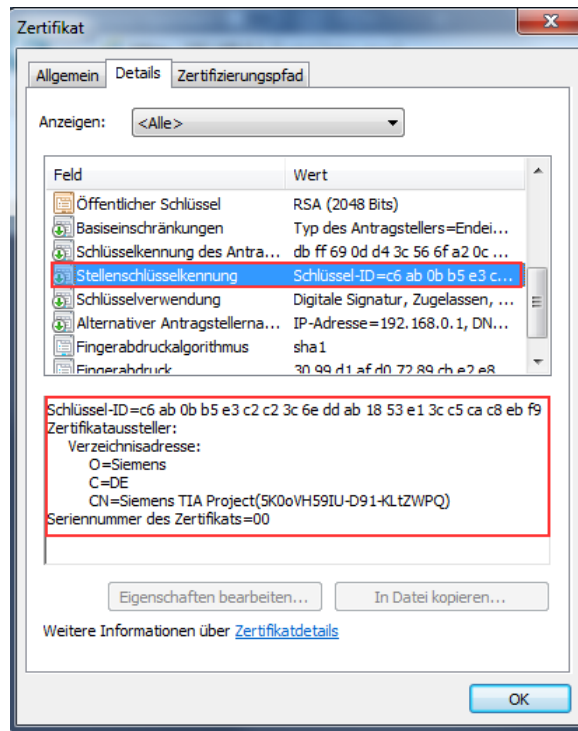
3. A window with Web page identification information appears. Click on the "Show certificates" link.

Figure 3-73



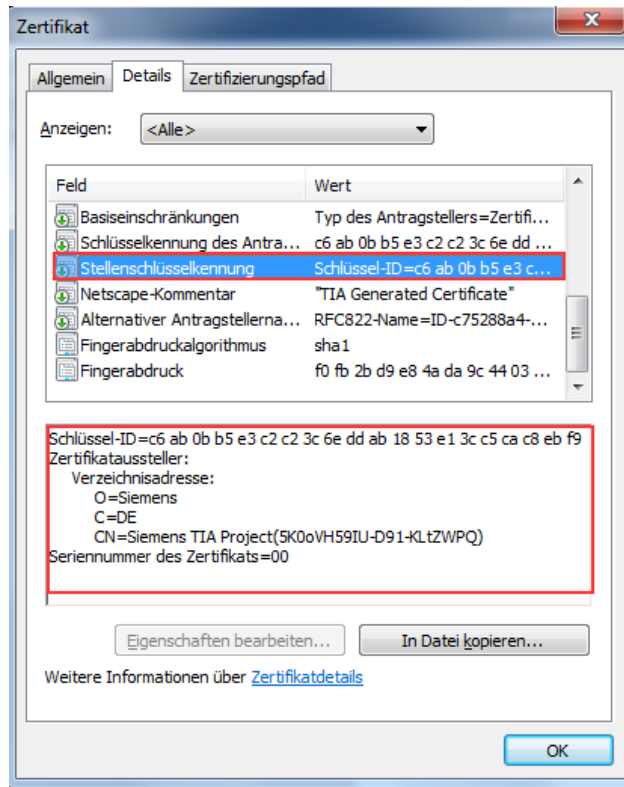
4. The device certificate is open. Switch to the "Details" tab and search for the entry "Authority Key Identifier". Select the entry to display the contents. To compare the key with the CA certificate, copy the key to a text file.

Figure 3-74



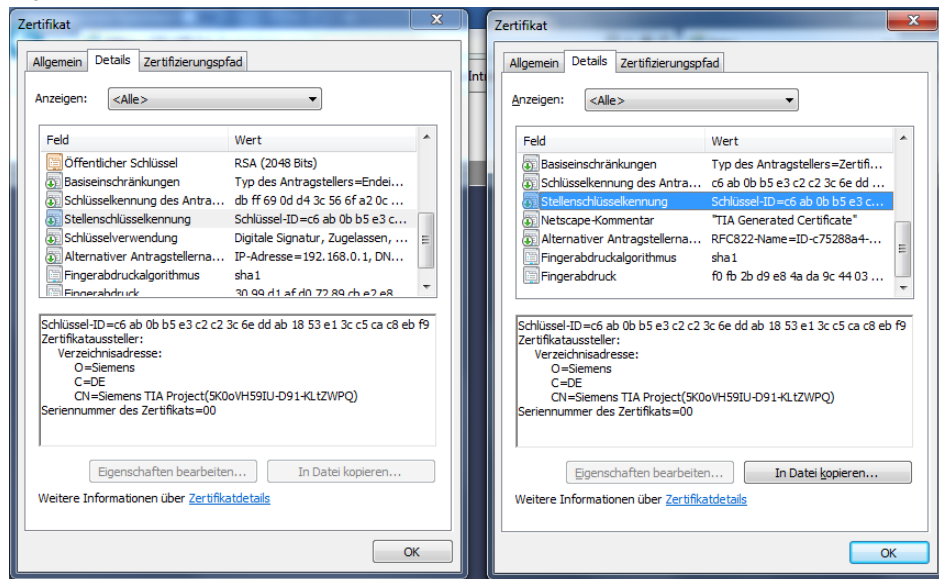
- Open the CA certificate. You can find the CA certificate from the management console, for example, or you have saved the CA certificate locally. Switch to the "Details" tab and search for the entry "Authority Key Identifier". Select the entry to display the contents.

Figure 3-75



- Now you can compare the keys with each other. If both are identical, then the certificates are genuine.

Figure 3-76



4 Secure OPC UA connection

Overview

With OPC UA, one system works as a server and makes the existing information available to other systems (clients).

OPC UA clients, for example, read and write data from an OPC UA server and call methods in the OPC UA server.

As of firmware V2.0, an S7-1500 CPU is equipped with an OPC UA server. As of firmware V2.6, an S7-1500 CPU also has an OPC UA client.

Security with OPC UA

OPC UA uses secure connections between client and server. OPC UA checks the identity of the communication partners. OPC UA uses certificates according to X.509-V3 of the ITU (International Telecommunication Union) for the authentication of client and server.

OPC UA uses the following security policies to protect messages:

- No security: All messages are unsecured.
- Signing: All messages are signed. This allows the integrity of received messages to be verified. Manipulations are detected.
- Sign & Encrypt: All messages are signed and encrypted. This allows the integrity of received messages to be verified. Manipulations are detected. In addition, no attacker can read the contents of the message (protection of confidentiality).

4.1.1 Security settings in the Server

OPC UA server

In this example, an S7-1500 CPU is set up as an OPC UA server.

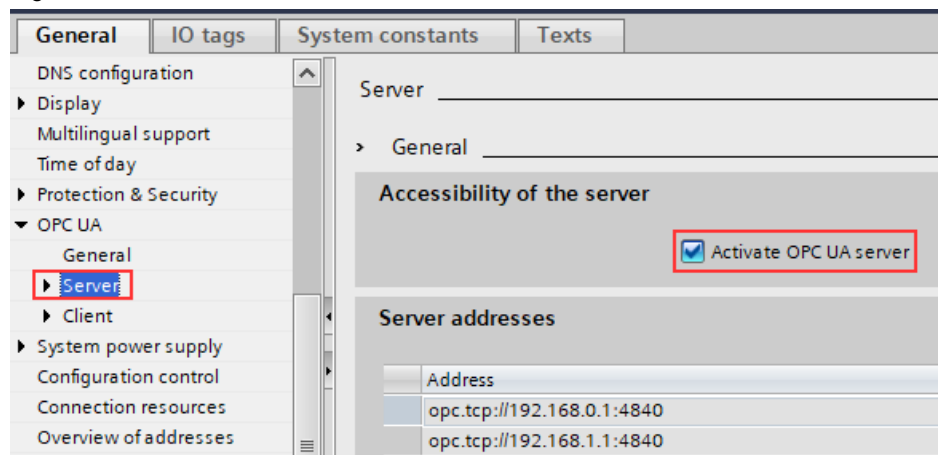
Commissioning OPC UA servers

In the basic setting the OPC UA server of the CPU is not released for security reasons. OPC UA clients can neither read nor write access to the S7-1500 CPU. The OPC UA server of the S7-1500 CPU is accessible via all internal PROFINET interfaces of the CPU (from firmware V2.0), but not via the PROFINET interfaces of CP/CM.

To activate the OPC UA-Server of the CPU, proceed as follows:

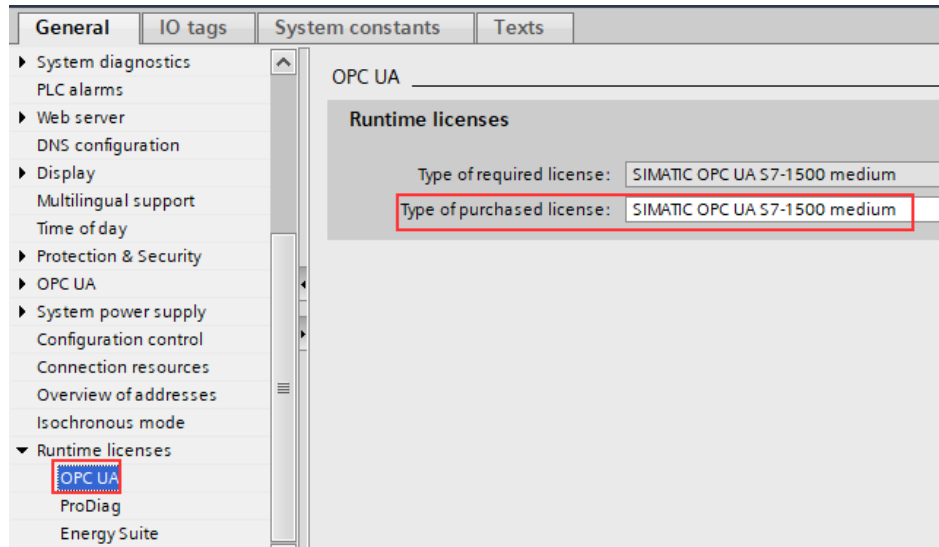
1. Mark the CPU in the device or network view. The properties of the CPU are displayed in the inspection window.
2. Select the entry "OPC UA > Server" ("OPC UA > Server") in the area navigation of the "Properties" tab. Activate the OPC UA server of the CPU and confirm the security message.

Figure 4-1



3. Select the area "Runtime licenses" in the CPU properties and set the purchased runtime license for the OPC UA server in the selection list "Type of purchased license".

Figure 4-2



4. Translate the project and load the project into the CPU.

Result

You have activated the OPC UA server of the CPU. In the section "Server addresses" you can see which URLs can be used to establish connections to the OPC UA server of the CPU.

Figure 4-3

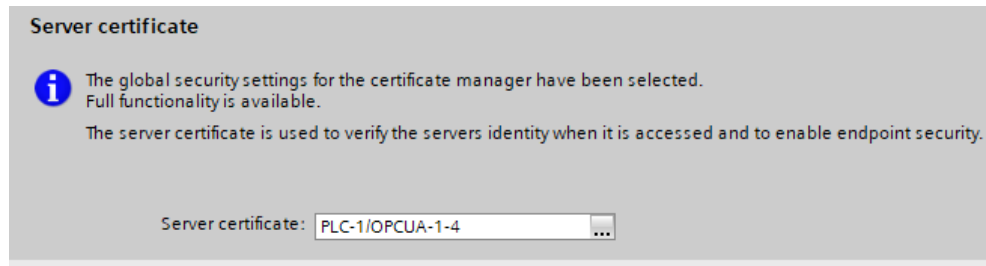
Address
opc.tcp://192.168.0.1:4840
opc.tcp://192.168.1.1:4840

View Server Certificate

If you have activated the OPC UA server and confirmed the security instructions, TIA Portal automatically generates the certificate for the server. You can find the server certificate in the properties of the OPC UA server.

Select the entry "OPC UA > Server > Security" in the area navigation. Under "Server certificate" you can see that TIA Portal has already created a device certificate assigned to the OPC UA server.

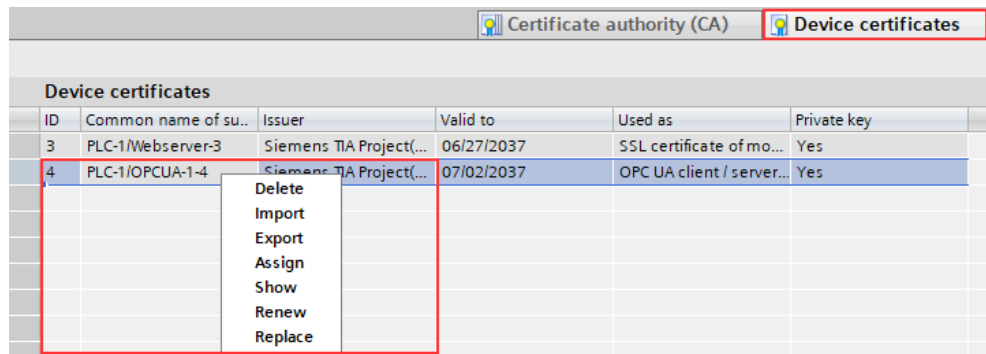
Figure 4-4



TIA Portal stores the server certificate in the local certificate directory of the CPU. You can view and manage this directory in the local certificate manager of the CPU and in the certificate manager of the global security settings (e.g. to export or delete certificates).

You can find the device certificate in the certificate manager of the global security settings in the "Device certificates" tab.

Fig. 4-5

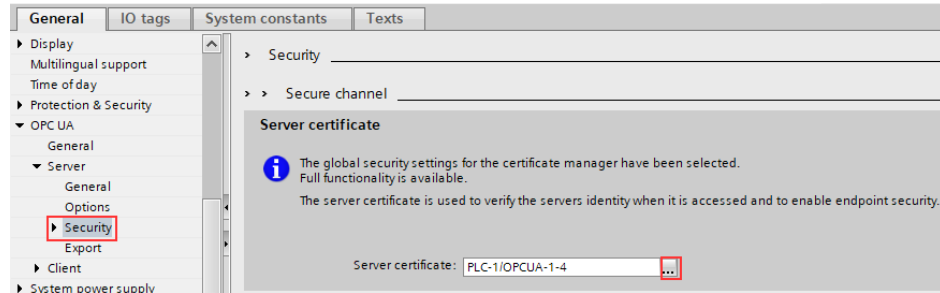


Creating a New Server Certificate

To generate a new server certificate, proceed as follows:

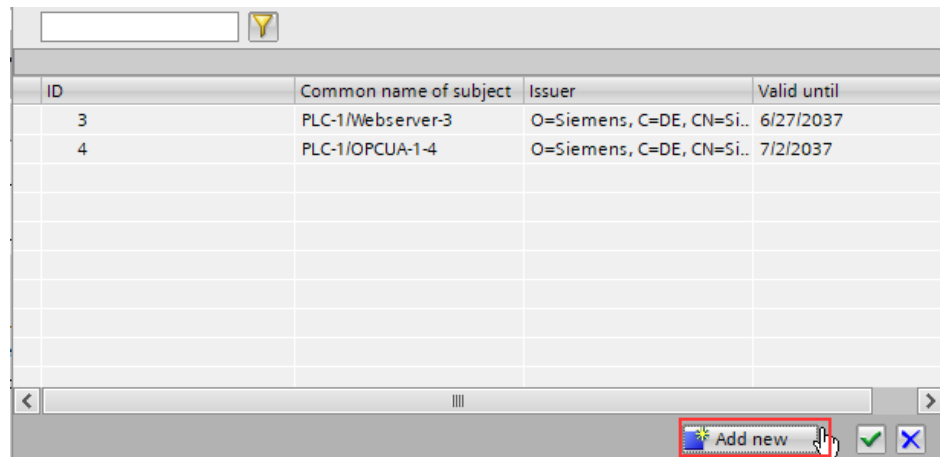
1. Select the entry "OPC UA > Server > Security" in the area navigation.
2. To select another server certificate or to generate a new server certificate, click on the button integrated in the "Server certificate" drop-down list.

Figure 4-6



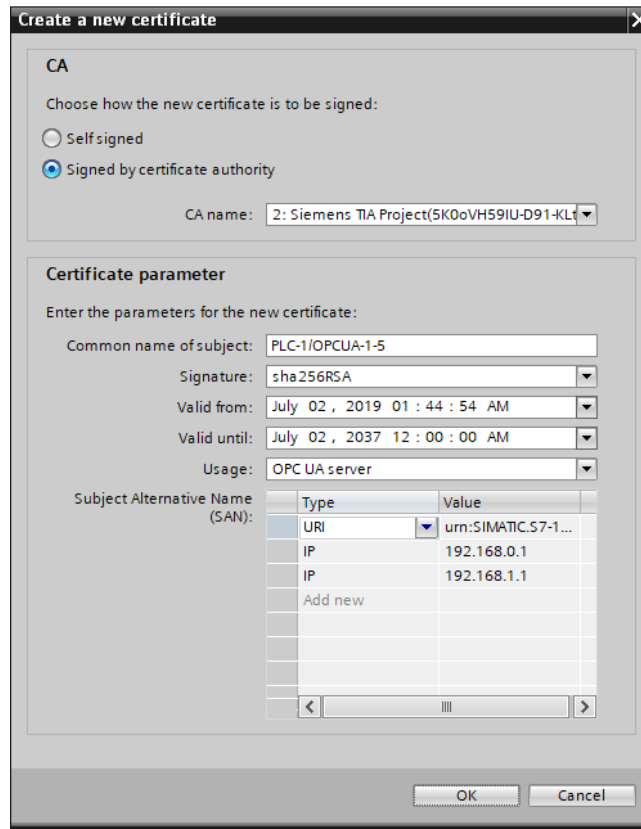
3. A dialog appears and lists all available server certificates. To create a new server certificate, click the "Add new" button.

Figure 4-7



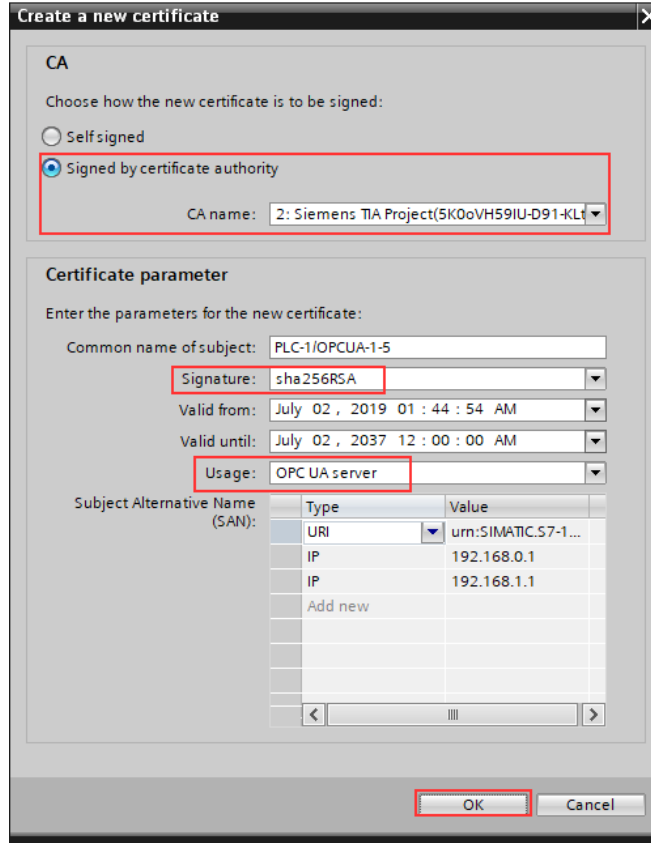
4. The dialog "Create new certificate" appears. You have the following options in this dialog:
 - You can choose between a self-signed certificate and a certificate signed by a certification authority.
 - If necessary, you can select the CA certificate of the certification authority.
 - You can determine the certificate parameters.

Figure 4-8



- This example creates a server certificate with strong encryption "SHA256" signed by a certification authority. The CA certificate provided by TIA Portal with the "ID: 2". Set the parameters. Use the screenshot as a guide. To generate the new certificate, click on the "OK" button.

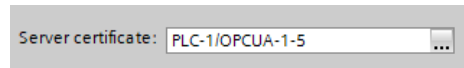
Figure 4-9



© Siemens AG 2019. All rights reserved

Note Coordinate the validity of the certificate with the plant operator.

- You can now use the newly created device certificate as the server certificate of the OPC UA server.



- Translate your TIA Portal project and load the CPU. During the loading process the device certificate, the CA certificate and the authorization for the OPC UA server access are loaded into the CPU.

Result

The new device certificate is added to the existing device certificates in the "Device certificates" tab of the certificate manager.

Figure 4-11

Device certificates					
ID	Common name of su..	Issuer	Valid to	Used as	Private key
3	PLC-1/Webserver-3	Siemens TIA Project(...	06/27/2037	SSL certificate of mo...	Yes
4	PLC-1/OPCUA-1-4	Siemens TIA Project(...	07/02/2037	OPC UA client / server...	Yes
5	PLC-1/OPCUA-1-5	Siemens TIA Project(...	07/02/2037	OPC UA client / server...	Yes

At this point, you can view, export, delete or renew the new device certificate, for example.

Figure 4-12

Device certificates				
ID	Common name of su..	Issuer	Valid to	Used as
3	PLC-1/Webserver-3	Siemens TIA Project(...	06/27/2037	SSL certificate of mo...
4	PLC-1/OPCUA-1-4	Siemens TIA Project(...	07/02/2037	OPC UA client / server...
5	PLC-1/OPCUA-1-5	Siemens TIA Project(...	07/02/2037	OPC UA client / server...

- Delete
- Import
- Export
- Assign
- Show
- Renew
- Replace

Configure server security settings

The OPC UA server of the S7-1500 CPU provides multiple server security settings for signing and encrypting messages. You can find the Security Policy at "OPC UA > Server > Security > Secure Channel" in the section "Security policies".

The following security policies are released:

Table 4-1

Policy	Description
None	Unsecured endpoint.
Basic128Rsa15 - Signing	Secure endpoint; supports a number of algorithms that use the RSA15 hash-algorithm and 128-bit encryption. This endpoint ensures the integrity of the data by signing it.
Basic128Rsa15 - Sign & Encrypt:	Secure endpoint; supports a number of algorithms that use the RSA15 hash-algorithm and 128-bit encryption. This endpoint ensures the integrity and confidentiality of the data by signing and encrypting it.
Basic256Rsa15 - Signing	Secure endpoint; supports a number of algorithms that use the RSA15 hash algorithm and 256-bit encryption. This endpoint ensures the integrity of the data by signing it.
Basic256Rsa15 - Sign & Encrypt:	Secure endpoint; supports a number of algorithms that use the RSA15 hash algorithm and 256-bit encryption. This endpoint ensures the integrity and confidentiality of the data by signing and encrypting it.
Basic256Sha256 - Signing	Secure endpoint supports a range of algorithms for 256-bit hashing and 256-bit encryption. This endpoint ensures the integrity of the data by signing it.
Basic256Sha256 - Sign & Encrypt:	Secure endpoint supports a range of algorithms for 256-bit hashing and 256-bit encryption. This endpoint ensures the integrity and confidentiality of the data by signing and encrypting it.

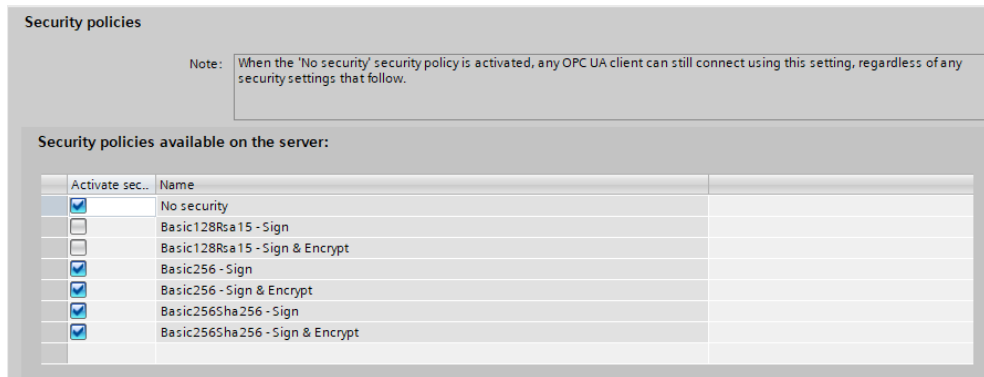
Note

If you use the settings "Basic256Sha256 Sign" and "Basic256Sha256 Sign & Encrypt", then the OPC UA server and the OPC UA clients must use signed certificates according to "SHA256".

In the Basic256Sha256 Signing and Basic256Sha256 Sign & Encrypt settings, TIA Portal's Certificate Authority automatically signs certificates with "SHA256".

The following security policies are set by default in TIA Portal:

Figure 4-13

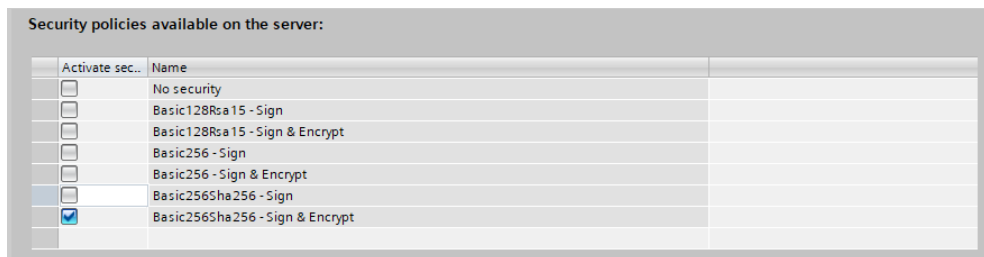


If you have activated all security policies in the secure channel settings of the S7-1500 OPC UA server (default, including the policy "No Security", then the data traffic between server and client is also possible unsecured (neither signed nor encrypted). The identity of the client remains unknown. Each OPC UA client can then connect to the server, regardless of any subsequent security settings.

When configuring the OPC UA server, make sure that only security policies that are compatible with the protection concept for your machine or system are activated. All other security policies must be deactivated.

To ensure a tap-proof connection, you should select "Basic256Sha256-Sign & Encrypt" ("Basic256Sha256-Sign & Encrypt") as the only possible access point.

Figure 4-14



Making the Client Certificate Known to the Server

A secure connection between the OPC UA server and an OPC UA client is only established if the server classifies the client's certificate as trustworthy.

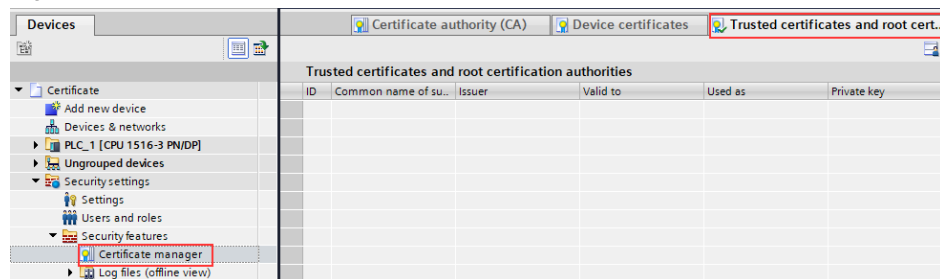
If you use OPC UA clients from manufacturers or the OPC Foundation, a client certificate is automatically generated during the installation or the first program call.

For a secure connection, you must make the client certificate known to the server and add it to the Trusted Clients list. To add the client certificate to the Trusted Clients list, the client certificate must be imported into the Certificate Manager of TIA Portal's global security settings.

To make the client certificate available to the server, proceed as follows:

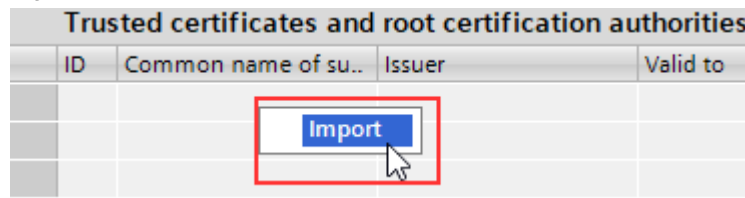
1. In the project navigation, open the "Security settings > Security features" menu. Double-click on the "Certificate manager" line.
2. The global certificate manager opens. Switch to the "Trusted certificates and root certification authorities" tab.

Figure 4-15



3. Right-click on an empty table row in the tab and select "Import" from the context menu.

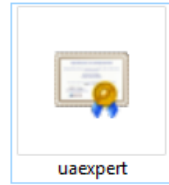
Figure 4-16



- The dialog for importing certificates is displayed. Select the client certificate that you want the server to trust. Click the "Open" button to import the certificate.

In this example, the certificate of UaExpert is added.

Figure 4-17



Note

Alternatively, you can import the CA certificate that was used to sign the client's device certificate.

By importing the CA certificate, all device certificates of the clients that were signed via this certification authority would be classified as trustworthy from now on.

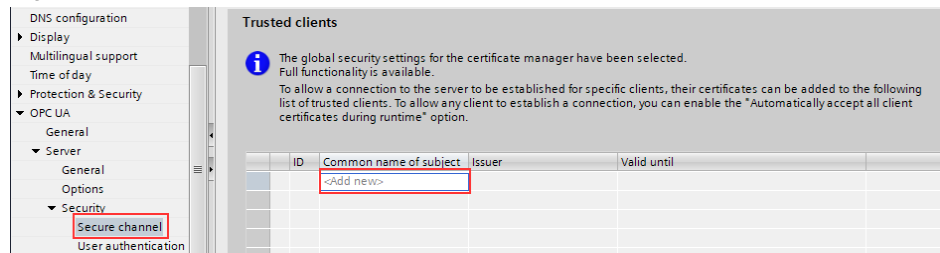
- The client's certificate is now included in the global security settings certificate manager. Note the ID of the currently imported client certificate.

Figure 4-18

Trusted certificates and root certification authorities					
ID	Common name of ...	Issuer	Valid to	Used as	Private key
8	UaExpert@myPC	UaExpert@myPC	07/07/2020	Certificate	No

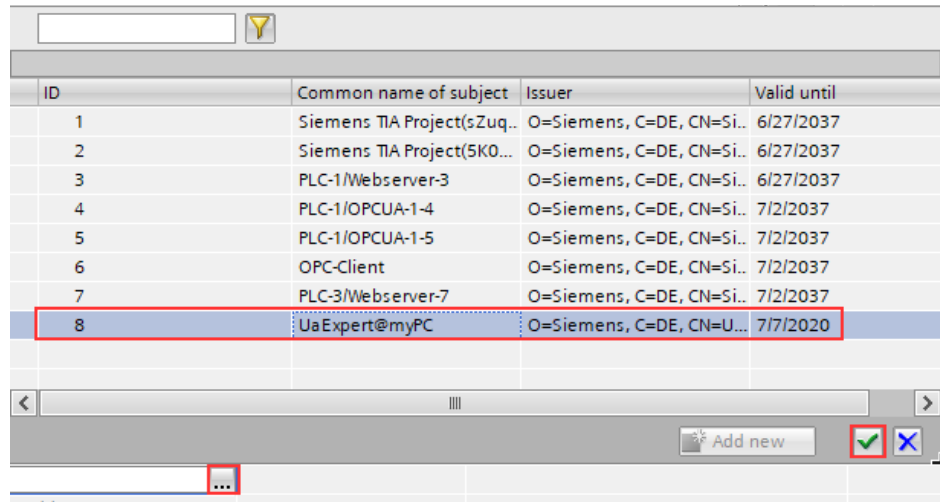
- In the device or network view, mark the CPU that serves as OPC server. The properties of the CPU are displayed in the inspection window.
- In the area navigation of the Properties tab, select "OPC UA > Server > Security > Secure channel". Here you will find the "Trusted Clients" section. In the table, double-click the empty row with "<Add new>".

Figure 4-19



8. A button with three dots is displayed in the line. Click this button. Select the client certificate that you imported. Click on the button with the green checkmark.

Figure 4-20

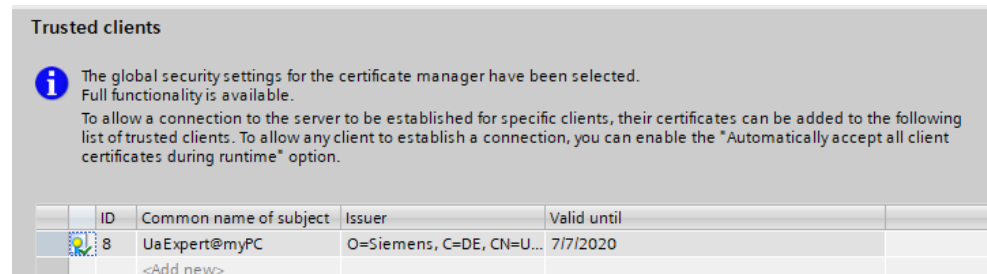


9. Translate the project and load the configuration into the S7-1500 CPU.

Result

You have classified the client certificate as trusted by the server. The server now trusts the client. If the client now also classifies the server certificate as trustworthy, then server and client can establish a secure connection (see also [section 4.1.2](#)).

Figure 4-21



Note

You can also configure the server to automatically accept the client certificates. If you enable the option "Automatically accept client certificates during runtime", the server will accept all client certificates. You will find this option below the "Trusted clients" list.

To avoid security risks, deactivate the option again after commissioning.

Automatically accept client certificates during runtime

User authentication

The security concept of the OPC UA connection is rounded off by user authentication.

With the OPC UA server of the S7-1500, you can set how a user of the OPC UA client must legitimize himself if he wants to access the server.

There are the following possibilities:

- **Guest authentication:**
The user does not have to prove his authorization (anonymous access). The OPC UA server does not check the authorization of the client user.
- **Authentication via user name and password:**
The user must prove his authorization (no anonymous access). The OPC UA server checks whether the client user is authorized to access the server. As proof the user name with the correct password is valid.
- **User management via the security settings of the project:**
If you activate this option, the user administration of the opened project is also used for the user authentication of the OPC UA server: With OPC UA, the same user names and passwords are valid as in the current project.

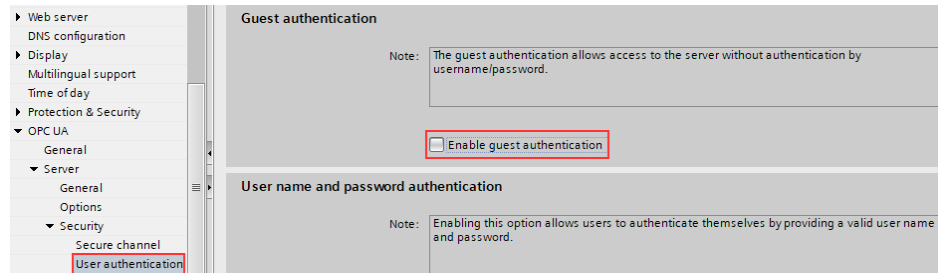
Note

To increase security, you should only allow access to the OPC UA server with user authentication.

To set up authentication using a user name and password, proceed as follows:

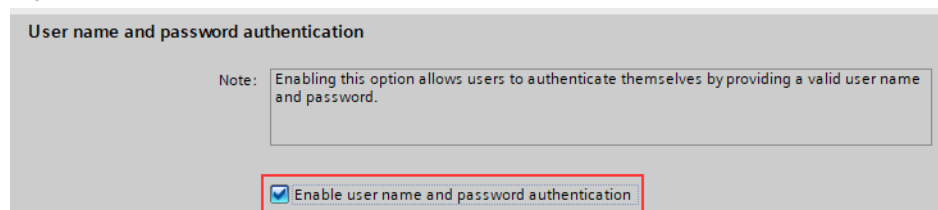
1. In the device or network view, mark the CPU that serves as OPC server. The properties of the CPU are displayed in the inspection window.
2. Select "OPC UA > Server > Security > User authentication" in the area navigation of the "Properties" tab. In the "Guest authentication" section, disable guest authentication.

Figure 4-22



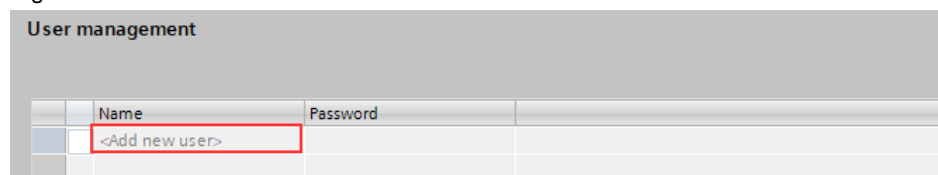
3. In the "User name and password authentication" section, enable the "Enable user name and password authentication" option.

Figure 4-23



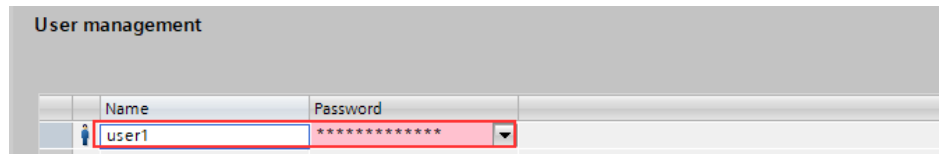
4. You can define users in the "User management" section. Enter the users in the table. To do this, click on the entry "<Add new user>".

Figure 4-24



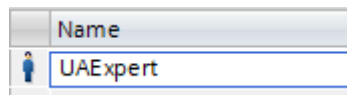
5. A new user with an automatically assigned name is created.

Figure 4-25



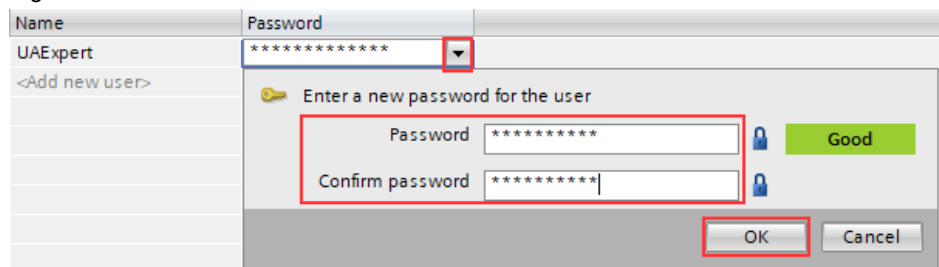
6. You can edit the user name and enter the password associated with the user name.
To change the name, double-click in the line "user1" and change the name according to your wishes.

Figure 4-26



7. To define the password, click on the integrated button in the cell under "Password" and set a password.
Close the dialog by clicking "OK".

Figure 4-27



Result

You have defined a user. If a client user wants to access the OPC UA server, the OPC UA server checks whether the client user is authorized to access the server. As proof, the user name just created with the correct password is valid. You can add a maximum of 21 users.

4.1.2 Security settings in the Client

OPC UA client

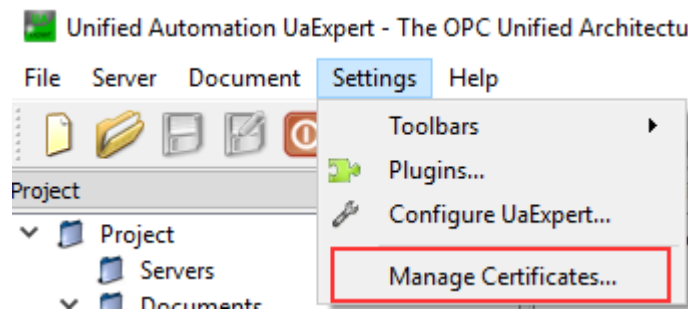
The following screenshots were taken with the free test client UaExpert Version 1.4.0 from UnifiedAutomation. The procedure for other clients may differ from the one shown.

Certificate management

If you use OPC UA clients from manufacturers or the OPC Foundation, the OPC UA clients have their own certificate manager. A client certificate is automatically generated during installation or when the program is called for the first time.

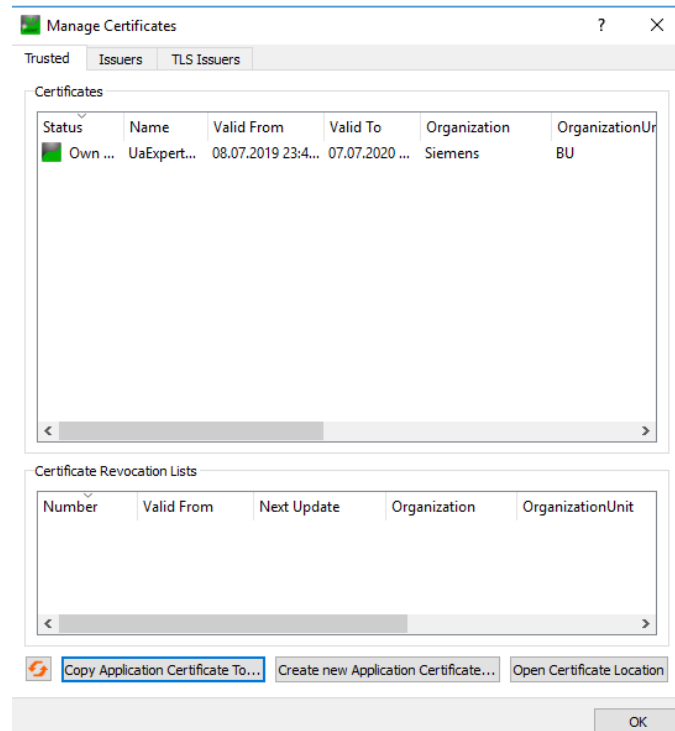
You can open UaExpert's certificate manager under "Settings > Manage Certificates".

Figure 4-28



The various certificates that are currently stored are displayed here.

Figure 4-29



Note Here you will also find the OPC UA client certificate that must be imported into the list of trusted clients in TIA Portal at the OPC UA server. (see [section 4.1.1](#)).

Making the Server Certificate Known to the Server

A secure connection between OPC UA server and an OPC UA client is only established if the client classifies the certificate of the server as trustworthy. To do this, you must import the server certificate into the certificate manager of the client. In this example, the CA certificate from TIA Portal is used as the server certificate.

Note When you import the CA certificate from TIA Portal, all server device certificates signed with this CA are automatically trusted.

Alternatively, you can import only the server's device certificate. You can find the device certificate in the global certificate manager of TIA Portal in the "Device certification" tab (see also the "View server certificate" section of [section 4.1.1](#))

To import the CA certificate, you must have saved the CA certificate on the local host in the following file formats:

- with the data type "*.der" ("Certificate-DER coded")

Figure 4-30

Dateityp: Certificate - DER coded (*.der)

- with the data type "*.crl" ("Certificate - Certificate Revocation List, DER coded")

Figure 4-31

Dateityp: Certificate - Certificate revocation list, DER coded (*.crl)

Export the CA certificate in the required formats from TIA Portal (see [section 2.3](#)).

Note You can export the certificates from TIA Portal in DER and CRL format. In addition to the certificate format "DER", UaExpert also requires the certificate revocation list (CRL-Certificate Revocation List), which can also be exported from the TIA portal via an export. For File type, select the "Certificate - Certificate Revocation List, DER coded" instead of "Certificate-DER coded".

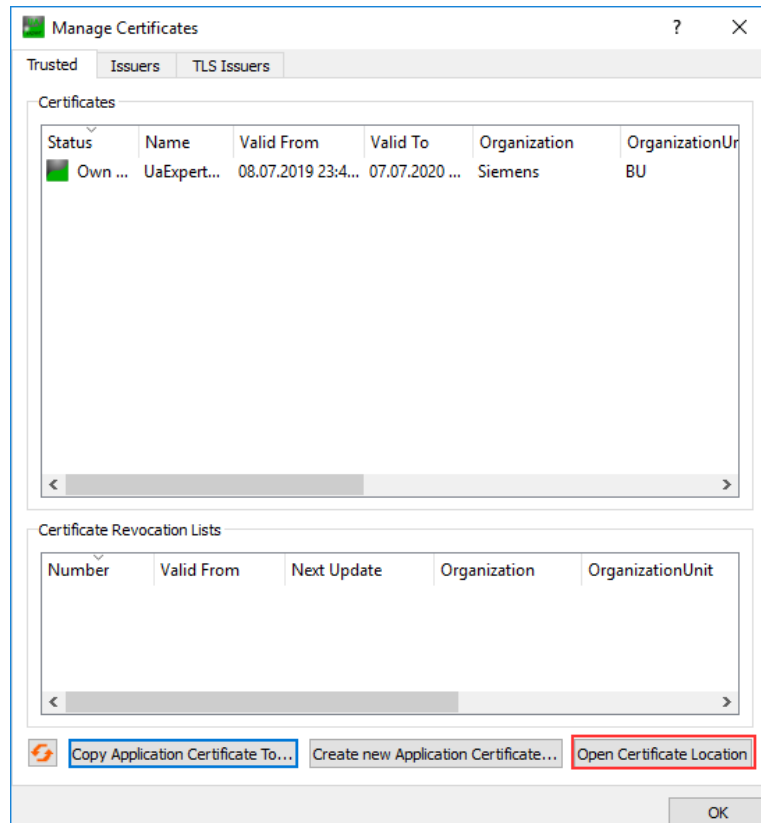
4 Secure OPC UA connection

To add CA certificates to the UaExpert Certificate Manager, they must be copied to the UaExpert storage location.

Proceed as follows:

1. Open the certificate manager of UaExpert via "Settings > Manage Certificates".
2. To access the certificate manager's storage location, click on the "Open Certificate Location" button.

Figure 4-32



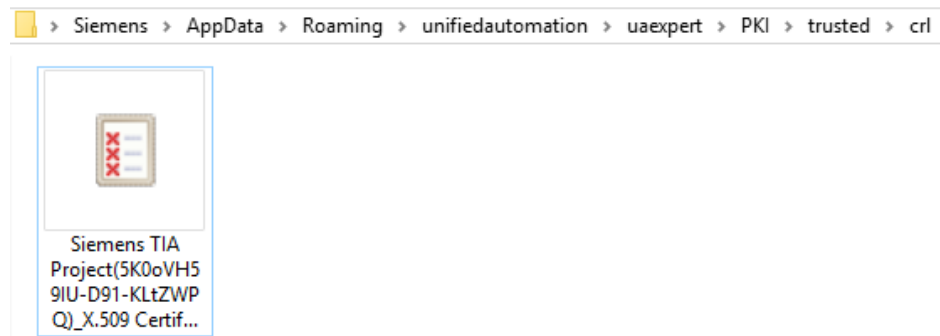
3. The directory "/unifiedautomation/uaexpert/PKI/trusted/certs" is opened. Copy the CA certificate of the server in the format "DER" into this folder. All server device certificates signed with this CA certificate are trusted by the client.

Figure 4-33



4. Change to the "/unifiedautomation/uaexpert/PKI/trusted/crl" directory. Copy the certificate revocation list in "CRL" format into this folder.

Figure 4-34

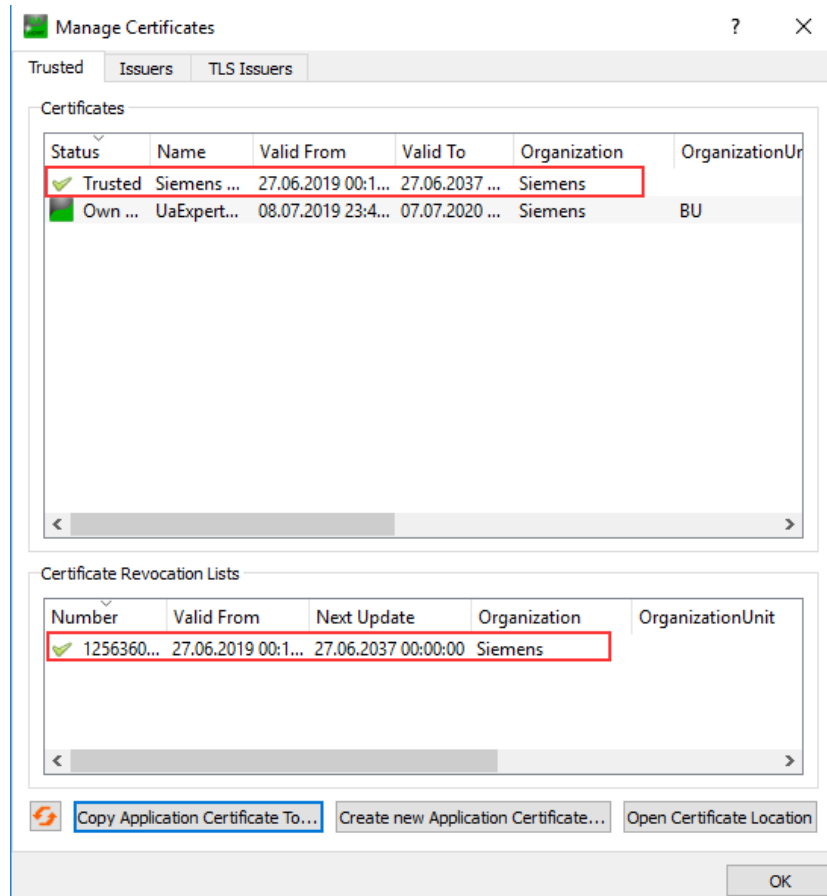


Result

You have imported the CA certificate and the certificate revocation list from TIA Portal into the certificate manager of UaExpert and have therefore classified it as trustworthy. Because this CA certificate signed the server's device certificate, the server's device certificate is also automatically trusted.

You can view the certificates via the UaExpert interface.

Figure 4-35

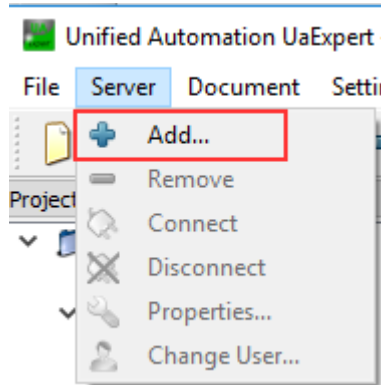


Add server in the client

Before you can establish a connection with UaExpert, you must add a server. Follow these steps for this purpose:

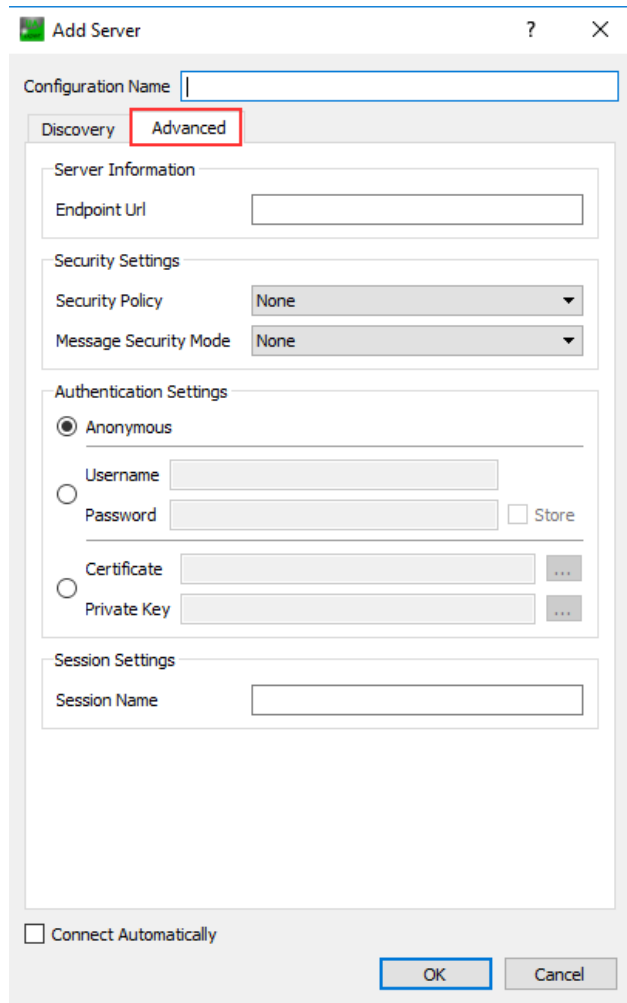
1. Go to the "Server > Add..." menu.

Figure 4-36



2. The "Add Server" window appears. Change to the "Advanced" tab.

Figure 4-37

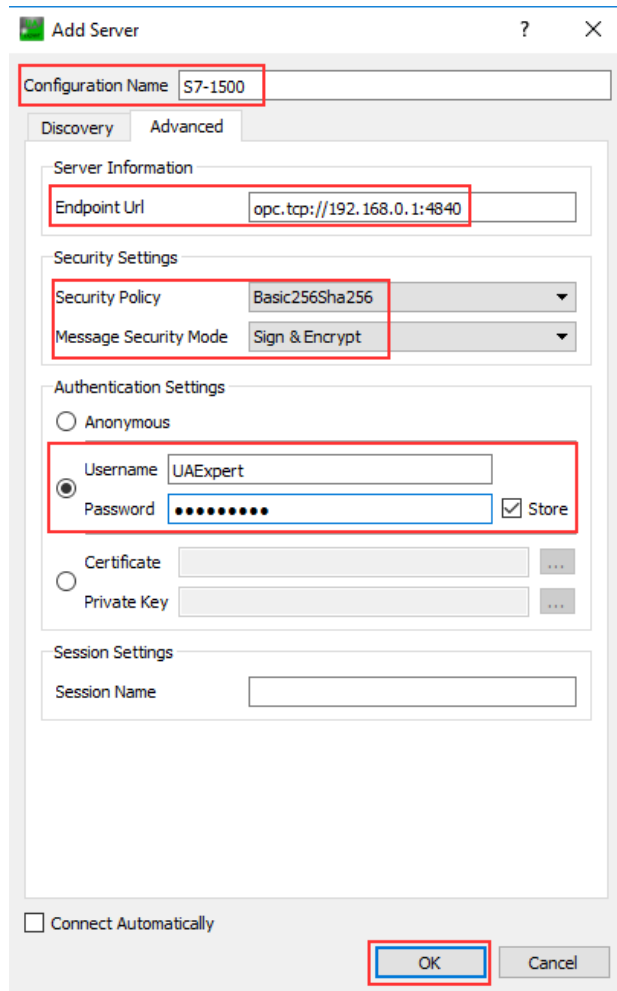


3. Make the following settings:

- In the "Configuration Name" section, define a display name for the server in UaExpert. In this example, the display name is "S7-1500".
- In the "Server Information" section, enter the URL of the OPC UA server. You can find the URL in TIA Portal when configuring the server. (see [section 4.1.1](#)).
- In the "Security Settings" section, select "Basic256Sha256" as the security policy.
- In the "Security Settings" section, select "Sign & Encrypt" as the Message Security Mode.
- In the "Authentication Settings" section, activate the "Username / Password" option and the "Store" option. Enter the user name and password set in TIA Portal. (see [section 4.1.1](#)).

Close the dialog by clicking "OK".

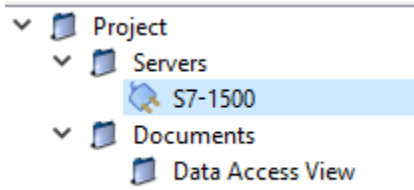
Figure 4-38



Result

You have added the S7-1500 CPU as an OPC UA server in UaExpert.

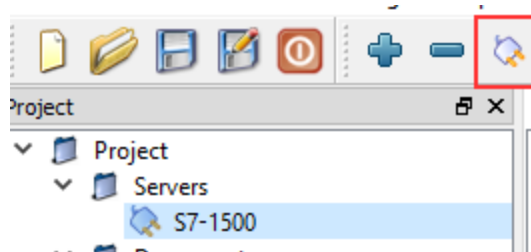
Figure 4-39



4.1.3 Test secure OPC UA connection

Once you have configured all security settings in the server and client, you can use UaExpert to establish a secure connection to the OPA UA server of the S7-1500 CPU.

Figure 4-40

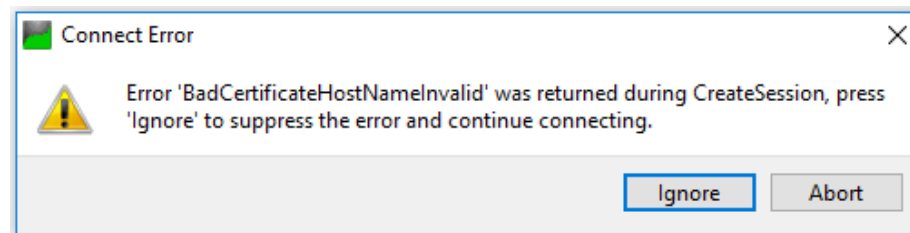


When establishing a connection, the certificates are exchanged and checked.

BadCertificateHostNameInvalid

When connecting to the server, you are confronted with the following error message:

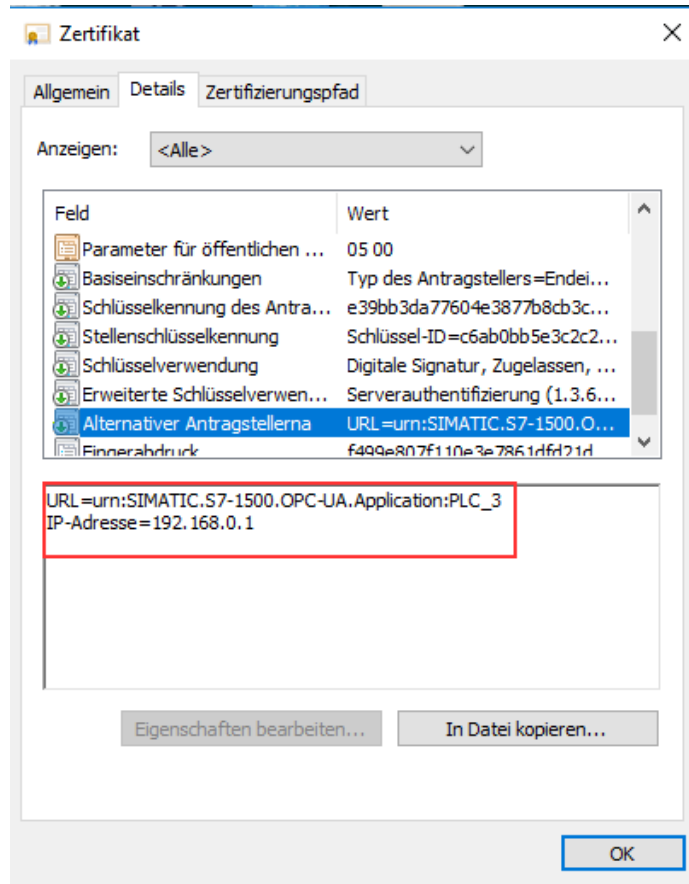
Figure 4-41



This error is due to the fact that UaExpert checks both an IP address and the DNS name of the server.

However, the S7-1500 does not return a DNS name or there is also no DNS name entered in the device certificate under "Subject Alternative Name".

Figure 4-42

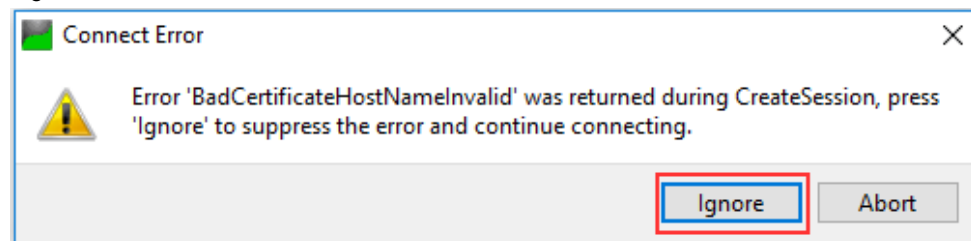


© Siemens AG 2019. All rights reserved

Ignore error

The error has no effect on the encryption functionality. You can ignore it by clicking on the "Ignore" button.

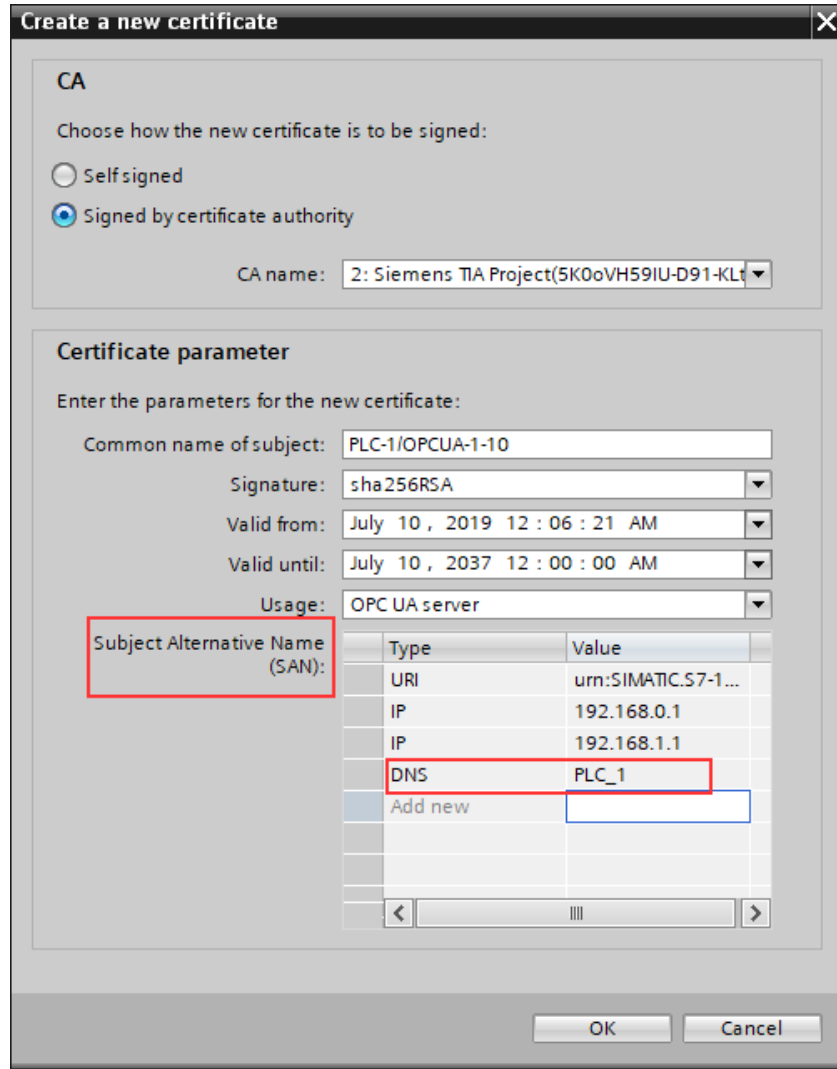
Figure 4-43



Eliminate errors

You can permanently fix the error by creating your own device certificate for the OPC UA server in TIA Portal and manually adding a DNS record (see section "Creating a new server certificate" in [section 4.1.1](#)).

Figure 4-44



On the OPC UA client computer you must then enter the IP address of the server. To do this, you must add an entry with IP address and DNS name to the "hosts" file. The Hosts file on Windows is an important Windows system file that is responsible for resolving IP addresses into hostnames.

You will find the file in the directory "%Windir%\System32\drivers\etc".

Note To edit this file, you need administrator rights.

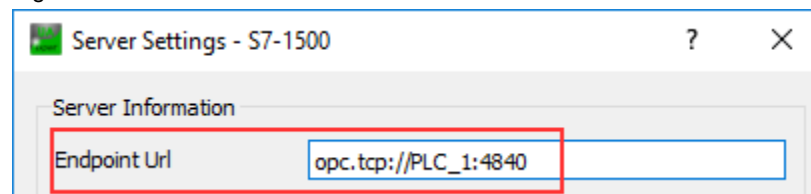
Figure 4-45

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com          # source server
#       38.25.63.10     x.acme.com             # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1          localhost
#   ::1                localhost
#   192.168.0.1       PLC_1
```

Then, in the UaExpert settings, you can use the DNS name as the endpoint URL instead of the IP address and the error will no longer be displayed.

Figure 4-46



Checking in on a connection

If the connection was successfully established, you can use a network analysis program, e.g. Wireshark, to check whether the security settings are working.

In the following screenshot, the connection between the server and client was monitored without encryption. The data is available in plain text.

Figure 4-47

The screenshot shows a Wireshark capture of network traffic. The top pane lists several packets (73-107) between 192.168.0.241 and 192.168.0.4, all using the OpcUa protocol. The middle pane shows the details of a selected packet (107), including the Security Sequence Number (102), Security RequestId (52), and OpUa Service (Encodeable Object). The bottom pane shows the raw packet bytes in hexadecimal and ASCII, which are clearly legible, indicating that the data is not encrypted.

In the following screenshot, the connection between the server and client was monitored using encryption. The data can no longer be viewed with the encrypted connection.

Figure 4-48

The screenshot shows a Wireshark capture of network traffic. The top pane lists several packets (4-20) between 192.168.0.241 and 192.168.0.4, all using the OpcUa protocol. The middle pane shows the details of a selected packet (18), including the Security Token Id (1), Security Sequence Number (39681260), Security RequestId (4206467001), and OpUa Service (Encodeable Object). The bottom pane shows the raw packet bytes in hexadecimal and ASCII, which are completely garbled, indicating that the data is encrypted.

5 Appendix

5.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

<https://support.industry.siemens.com>

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:

<https://support.industry.siemens.com/cs/ww/en/sc/2067>

5.2 Links and literature

Table 5-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109769068

5.3 Change documentation

Table 5-2

Version	Date	Change
V1.0	09/2019	First version