SIEMENS

Using Certificates with TIA Portal

SIMATIC / TIA Portal

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

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 under https://www.siemens.com/cert.

Table of contents

1 Introduction

1.1 Overview

This document addresses the key aspects of certificate management in OT environments, a topic gaining special significance as industries shift to the digital era. In this new industrial landscape, OT systems face the same challenges and risks as the IT domain, underscoring the need to secure communications and ensure proper understanding and utilization of certificates.

Therefore, this application example provides guidelines to establish secure communications in the context of OPC UA, OUC (Open User Communication) and HTTPS, offering an overview of the tools and possibilities available within TIA Portal.

1.2 Public Key Infrastructure

Integrity, confidentiality, and endpoint authentication

The Public Key Infrastructure (PKI) stands as a robust framework in the field of cybersecurity, safeguarding digital communications by ensuring the integrity and confidentiality of messages transmitted over networks, as well as providing endpoint authentication.

- Integrity: Data must remain unchanged and unaltered during transmission.
- Confidentiality: Sensitive information must be kept private and inaccessible to unauthorized parties.
- Authentication: The communication partner is who it claims to be and the party who is to be reached.

Basic principles

To grasp how the Public Key Infrastructure manages to secure communications, it is necessary to understand signing and encryption.

- Encryption is the process of transforming plain text into ciphertext, making it solely understandable to authorized users. By employing an "encryption key", a unique cipher is generated, effectively locking the message. Only entities possessing the correct key can decrypt and unlock this data, guaranteeing its confidentiality.

  There are two main types of encryptions: symmetric and asymmetric encryption.

  1. Symmetric encryption employs a single key for both encryption and decryption of the cipher, rendering it an efficient, simple, and high-performance procedure. The main challenge of this approach lies in securely distributing the shared key between the sender and the receiver, without it being intercepted by unauthorized parties.
  2. On the other hand, asymmetric encryption involves a pair of keys: a private key and a public key. Data encrypted with one key can only be decrypted with the other. While the public key is shared openly, the private key must always remain secret.

     Each communication partner has its own private and public keys, solving the key distribution problem present in symmetric cryptography. Nonetheless, it is computationally intensive and therefore not suitable for large data transfers.

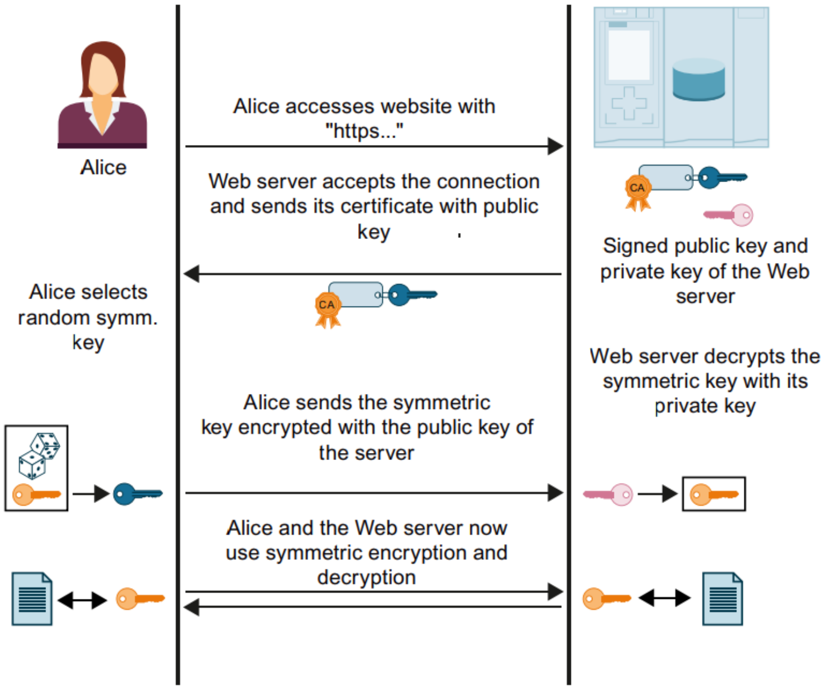
  To tackle the disadvantages associated with each individual encryption method, the PKI adopts a hybrid approach. Initially, communication partners employ asymmetric encryption to establish a secure channel, facilitating the exchange of a symmetric key between them. Once the shared key has been exchanged, communication transitions to symmetric encryption that can handle extensive sets of data.

- Digital signing is used to verify authenticity and integrity. The sender passes the message through a hashing algorithm, generating a unique code known as “hash”. This code is encrypted with the sender’s private key, forming a digital signature. Both the signature and the original message are transmitted.

Upon receiving the message, the recipient uses the sender's public key to decrypt the signature and extract the original hash. Then, the receiver performs the hashing process with the received message and compares it with the original. If both hashes match, the integrity and authenticity of the message can be confirmed.

Course of the secure communication

The figure below shows, in simplified terms, how communication is established ("handshake") focusing on the negotiation of keys used for data exchange. This process can be generalized to all communication options that are based on the usage of TLS, i.e., Secure Open User Communication.


Alice
Alice accesses website with "https..."
Web server accepts the connection and sends its certificate with public key
CA
Signed public key and private key of the Web server
Alice selects random symm. key
Web server decrypts the symmetric key with its private key
Alice sends the symmetric key encrypted with the public key of the server
Alice and the Web server now use symmetric encryption and decryption

Key components of the PKI

The Public Key Infrastructure main components are:

- Public and private keys, to perform the initial asymmetric encryption.
- Digital certificates, which serve as electronic credentials that bind public keys to the identity of the certificate holder.
- Certificate Authorities (CAs), used to validate the identity of certificate holders and issue new certificates.
- Servers, often referred to as subjects, are network entities that need to prove their identity.
- Clients, or relying parties, must trust servers to establish a secure connection with them.

NOTE

In certain protocols, such as HTTPS, clients only validate the server's identity. In contrast, some industrial protocols such as OPC UA require mutual authentication, establishing a two-way trust relationship between clients and servers.

NOTE

Clients and servers can be configured to allow connections from any communication partner without requiring authentication. It is essential, however, to restrict this configuration to the testing or commissioning stages. Transitioning to a production environment mandates special emphasis on security. Thus, access must be limited to authorized entities and communication safeguarded through signing and encryption.

1.3 Digital certificates

Certificate basics

A certificate is a digital/electronic credential used to assert the online identities of individuals, computers, and other entities on a network. They are similar to ID cards, and they bind the identity of the owner with a public key.

X-509 is one of the most common standards used to define the format of certificates. To ensure the authenticity of the entities and enable signing and encryption, these certificates include the following fields:

- Public key.
- Serial number of the certificate.
- Version number of the certificate.
- Validity period (starting and expiring dates).
- Owner (certificate subject).
- Issuer (CA or self-signed).
- Supported encryption and signing algorithms.
- Extensions – Subject Alternative Name (since X-509 Version 3)

NOTE Certificates do not contain the private key of the subject, as it must be kept secret.

Certificate types

Different types of certificates can be found depending on the entity of the issuer, as they can be generated by their own (self-signed) or issued by a Certificate Authority (CA).

- **Self-signed certificates:** Each device creates its own certificate; therefore, they are both certificate holder and issuer. To establish trust relations between devices, it is necessary to import all partner certificates.
- **Certificates issued by a Certificate Authority (CA):** Device certificates are signed by a Certificate Authority. Therefore, if the CA is trusted, all communication devices whose certificates are issued by this CA are instantly trusted and thus authorized to establish a connection.

  To invalidate certificates that are no longer deemed valid or trusted, Certificate Authorities employ Certificate Revocation Lists (CRL).

Decision making for different scenarios

- **Self-signed approach:** It can be useful in small and static systems where the number of devices is low. However, given that devices have a maximum limit of keys that can be stored (64 in the case of SIMATIC PLCs), this approach can lead to resource bottlenecks.

  Additionally, introducing new devices to the system can be challenging, as new certificates must be distributed to all communication partners. Therefore, industrial systems with these certificates can be difficult to maintain (renew certificates) and expand.
- **Issued by Certificate Authorities:** This second approach offers more flexibility when managing medium to big systems, and it consumes less storage resources, as only CA certificates need to be loaded to the CPUs.

  The primary drawback of this approach is the need for a centralized administrative instance equipped with security measures for private keys. However, this concern can be effectively addressed using TIA's Certificate Manager.

1.4 Certificate Management

Key Handling

Proper handling of certificates is critical to maintain integrity, confidentiality, and availability within industrial systems. As highlighted earlier, in the Public Key Infrastructure, entities make use of both a public and a private key to establish secure communications. Therefore, understanding the distinctions between these keys and how they must be handled is of utmost importance.

Public Key: The public key is intentionally created for widespread use, and it can be shared freely to any entity without compromising the security of the system. Its responsibilities include:

- Encryption of messages: to ensure that only the owner of the matching private key can decrypt and access the information.
- Verification of digital signatures: providing assurance that a message is indeed originated from the rightful owner of the private key.

Private Key: On the other hand, the private key is strictly confidential and must be kept secret. Its roles include:

- Decryption of messages: that are sent and encrypted by communication partners, using the corresponding public key.
- Signing: so other devices can verify the authenticity and integrity of messages.

Consequently, protection of private keys is imperative to prevent unauthorized access, decryption, and forging of digital signatures. Sections 2.4.6 and 2.5.5 include diagrams to showcase how certificates and private keys must be handled in different scenarios.

Certificate renewal

In Operational Technology (OT), the recommended certificate validity is regulated by the specific needs and security practices of the organization. There are, however, some general guidelines.

1. **Shorter validity periods:** Due to the criticality of industrial systems and the ever-evolving security threats, certificates in OT environments often have shorter validity periods compared to traditional IT systems. This typical validity might range from a few months to a few years.
2. **Regular renewal:** Renewing certificates regularly helps to maintain a higher level of security by ensuring that older certificates, which might become compromised or less secure over time due to newly emerging technologies, are replaced with newer ones.
3. **Balance security and operational impact:** While shorter validity periods enhance security, frequent certificate changes could potentially impact operational continuity. Therefore, it is essential to find a balance between security needs and operational impact.

   Refer to chapter 3.1, “GDS Push for dynamic certificate management”, to gain insights on how to handle certificates with minimal disruptions to production.
4. **Compliance to industry standards:** Some industries or regulatory frameworks might require specific conditions regarding certificate validity periods.

Thus, OT environments tend to follow a more conservative approach than some IT environments when it comes to certificate validity. This stems from the critical nature of industrial control systems and the need to mitigate risks associated with cyber threats while considering the continuous operation of these systems.

1.5 Components used

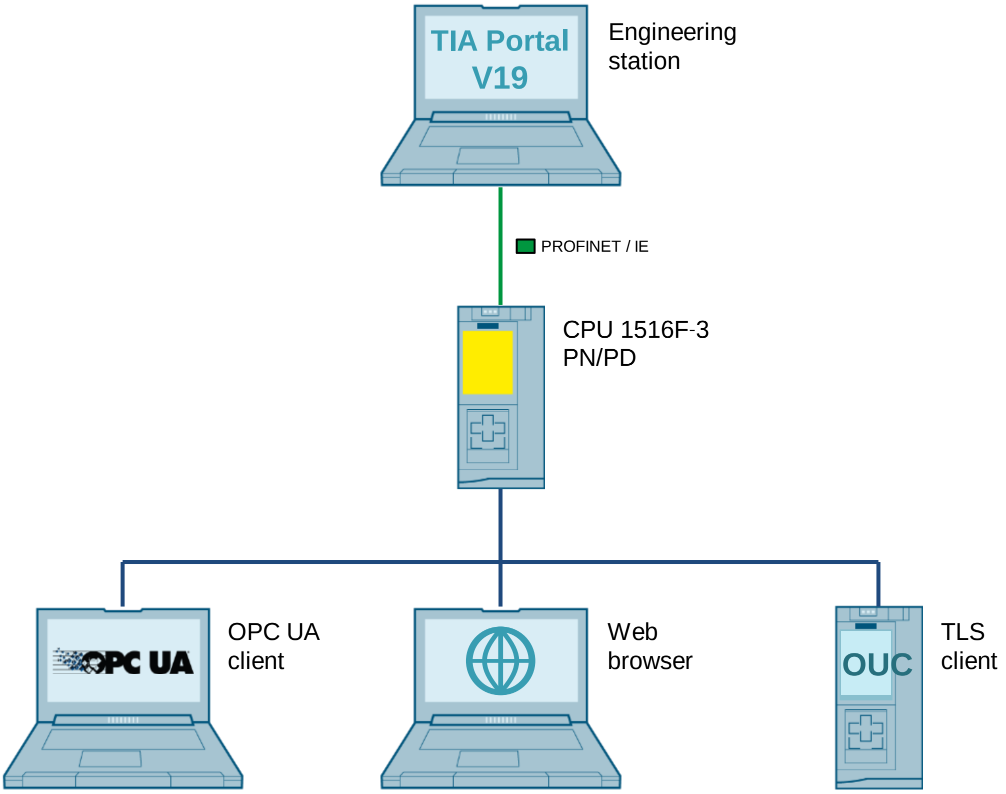
This application example consists of the following components:

Component	Article number	Note
TIA Portal V19	6ES7822-1AA23-0YA5	-
CPU 1516F-3 PN/PD	6ES7516-3FP03-0AB0	FW 3.1 – With previous firmware versions, step-by-step procedures can differ from those outlined in this document.
CPU 1516-3 PN/PD	6ES7516-3AP03-0AB0	FW 3.1

2 Engineering

2.1 Hardware setup

A PG with TIA Portal V19 is used to create and manage certificates, as well as configuring the S7-1500 CPU. The CPU will run an OPC UA server, a Web server, and a TLS server for Secure OUC. To test these protocols, UaExpert operates as the OPC UA client, Edge functions as the web browser for connecting to the web server, and a second PLC runs the TLS client.



2.2 Planning

This application example is structured into distinct sections, each focusing on a specific topic. It starts with an assessment on how to manage certificates within TIA Portal, offering a comprehensive overview of the possibilities that TIA Portal currently offers. Following this point, the document provides guidelines and examples on how to handle certificates for each communication protocol. Finally, a brief introduction to dynamic management of certificates via GDS Push is carried out.

2.3 TIA Portal for certificate management

2.3.1 Overview

Certificate management options in TIA Portal

Since TIA Portal version V14 and CPU firmware version V2.0, certificate management for S7-1500 CPUs has been available. The table below outlines all certificate management options based on the service used, TIA Portal version, and firmware version of S7-1500 PLCs.

Service	Certificate management with TIA Portal (TIA Portal version / S7-1500 CPU FW-version)	Certificate management with OPC UA GDS push methods (TIA Portal version / S7-1500 CPU FW-version)
Web server	as of V14 / as of V2.0	as of V18 / as of V3.0
Secure OUC	as of V14 / as of V2.0	-
OPC UA server	as of V14 / as of V2.0	as of V17 / as of V2.9
OPC UA client	as of V15.1 / as of V2.6	-
Secure PG/HMI communication	as of V17 / as of V2.9	-
Syslog client	as of V19 / as of V3.1	-

Additionally, as of firmware version V4.4, S7-1200 CPUs also support secure communication.

Local and global certificate managers

TIA Portal offers different options to manage certificates via the local and global certificate managers.

- Local certificate manager: Each device has its own local certificate manager, where certificates are generated and managed for each individual device. These certificates can be used for the OPC UA server and Web server running on the device, as well as for additional system features that require certificates, such as Secure OUC.
- Global certificate manager: Contains an overview of all the certificates used in a project, including Certification Authorities, certificates issued by CAs, and self-signed certificates.

NOTE

Certificates must always be included in the local certificate manager of a device to be part of the HW configuration. Referencing the certificate’s ID in the global certificate manager is not sufficient to assign the certificate to a device.

Global security settings

Devices in TIA Portal can be configured to operate exclusively with the local certificate manager or utilize both the local and global certificate managers through the global security settings.

If the global security settings are disabled in a device, it will only have access to the CPU-specific certificate manager. Consequently, its functionality will be limited, as it won't have access to root CAs or other certificates imported into the project.

Activating the global security settings allows the local certificate manager to access the global certificate manager and vice versa. Thus, the device is granted access to the certificate store of the project and to additional functionalities covered in section 2.3.3.

NOTE

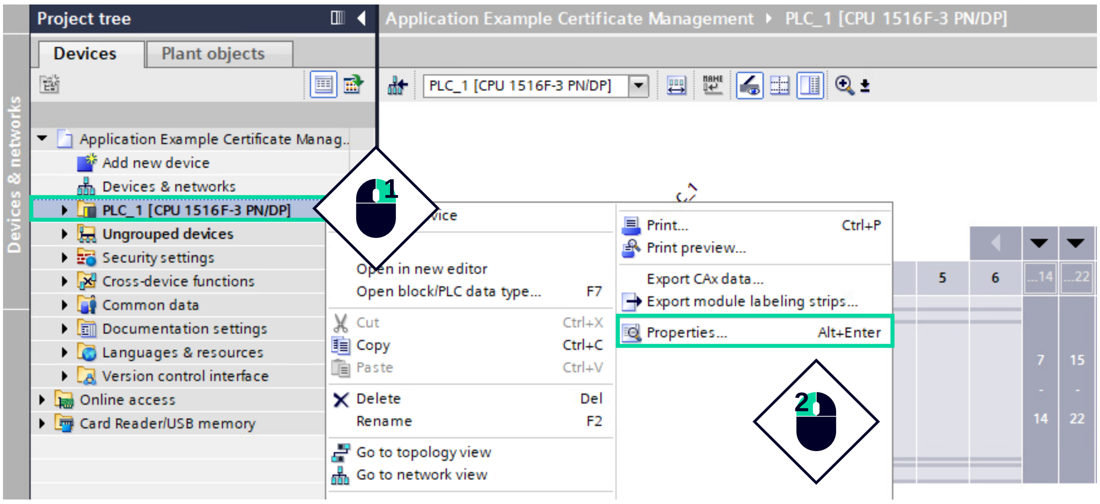
To access the global certificate manager, the project must be protected, and the user must be logged in as administrator.

2.3.2 Using the local certificate manager

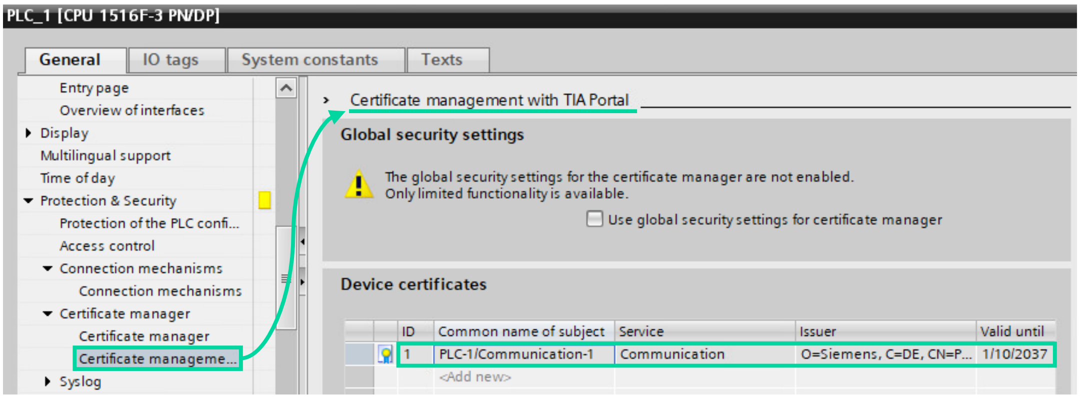
Access to the local certificate manager

The local certificate manager is located within each device.

1. To access the local CPU-specific certificate manager, select the CPU in the project tree and navigate to the “Properties” tab.



2. Select “Protection & Security > Certificate Manager > Certificate Management with TIA Portal”. If a device supports “secure PG/PC and HMI communication”, a certificate is automatically generated to enable this type of communication.



Global security settings

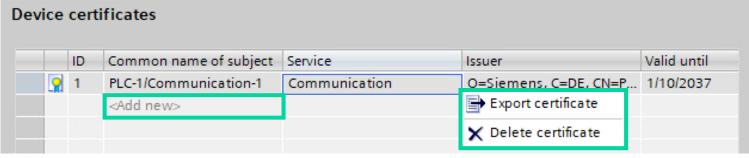
The global security settings for the certificate manager are not enabled.
Only limited functionality is available.

□ Use global security settings for certificate manager

Device certificates

ID	Common name of subject	Service	Issuer	Valid until
1	PLC-1/Communication-1	Communication	O=Siemens, C=DE, CN=P...	1/10/2037
	<Add new>			

Note: Due to the limited functionality in the local certificate manager, certificates can only be created, exported (without the private key) or deleted.

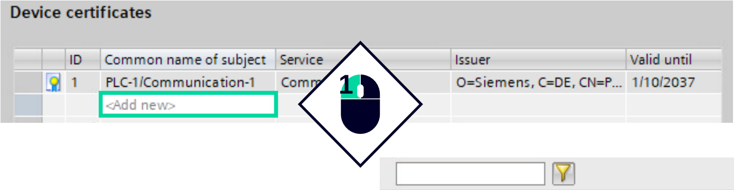

Device certificates

ID	Common name of subject	Service	Issuer	Valid until
1	PLC-1/Communication-1	Communication	O=Siemens, C=DE, CN=P...	1/10/2037
	<Add new>			

Creating new certificates

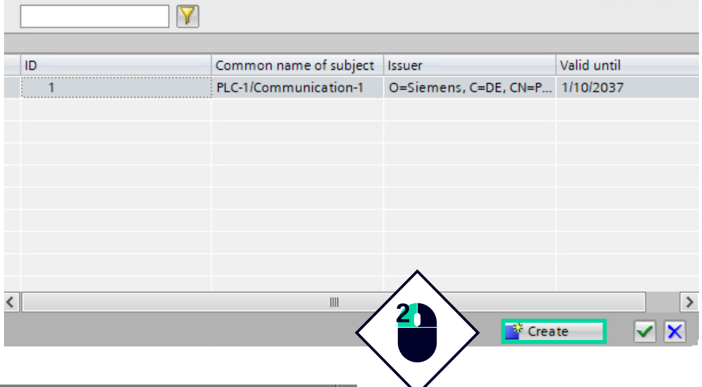
New certificates can be created in various ways within the local certificate manager.

1. To add new certificates, click on “<Add new>” and “Create”. Enter all certificate parameters in the corresponding input fields. As highlighted in the snapshot, certificates can only be self-signed, as the local certificate manager has no access to Certification Authorities.

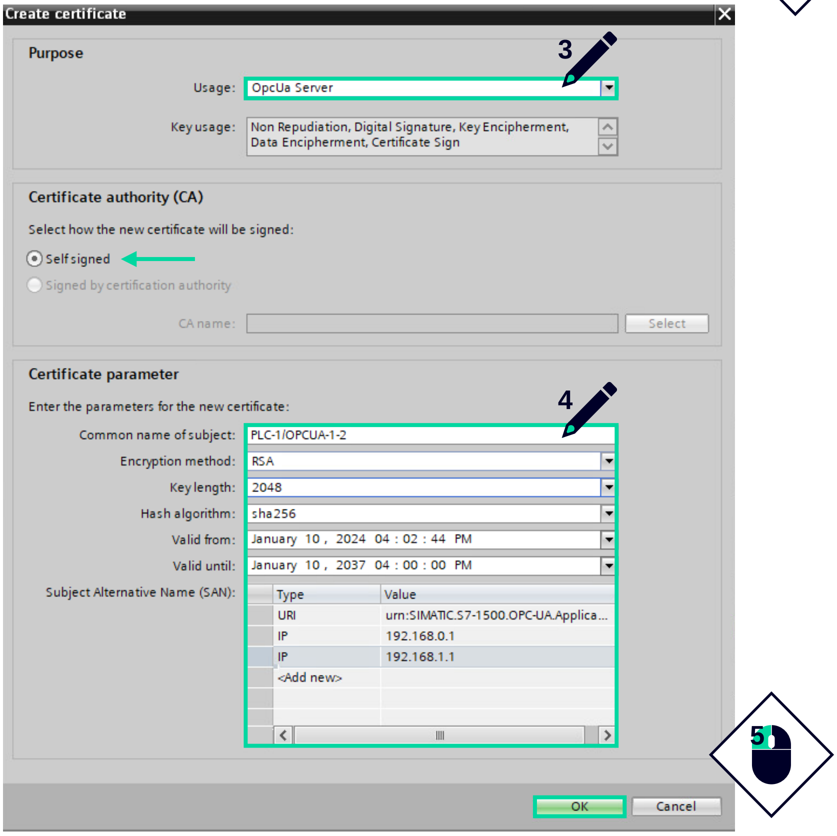


Device certificates

	ID	Common name of subject	Service	Issuer	Valid until
	1	PLC-1/Communication-1	Comm	O=Siemens, C=DE, CN=P...	1/10/2037
		<Add new>			



ID	Common name of subject	Issuer	Valid until
1	PLC-1/Communication-1	O=Siemens, C=DE, CN=P...	1/10/2037



Create certificate

Purpose

Usage: OpcUa Server

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Data Encipherment, Certificate Sign

Certificate authority (CA)

Select how the new certificate will be signed:

● Self signed

○ Signed by certification authority

CA name:

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1/OPCUA-1-2

Encryption method: RSA

Key length: 2048

Hash algorithm: sha256

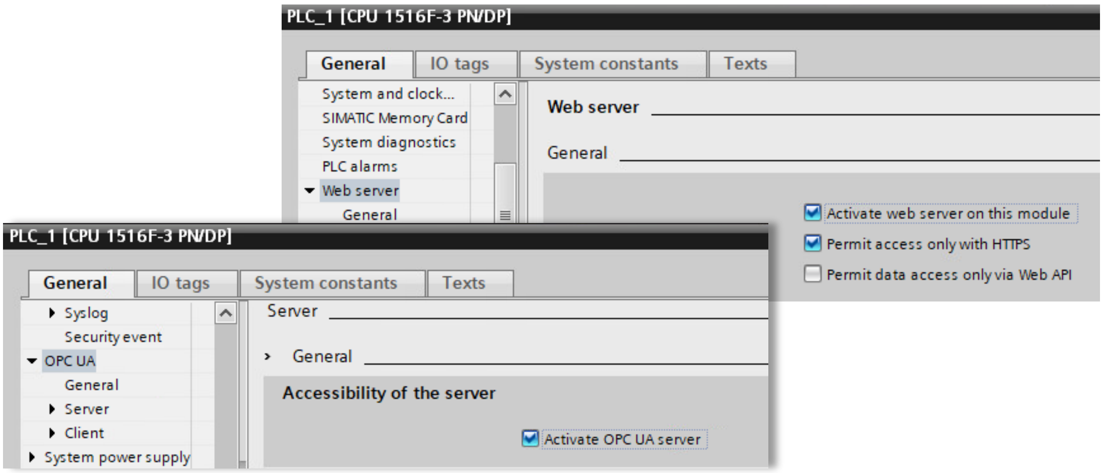
Valid from: January 10 , 2024 04 : 02 : 44 PM

Valid until: January 10 , 2037 04 : 00 : 00 PM

Subject Alternative Name (SAN):

Type	Value
URI	urn:SIMATIC.S7-1500.OPC-UA.Applica...
IP	192.168.0.1
IP	192.168.1.1
<Add new>	

2. In addition, certificates are automatically added into the CPU during the activation of both the web and OPC UA servers. Full detailed instructions on how to configure these servers is provided in sections 2.4.3 and 2.5.2.

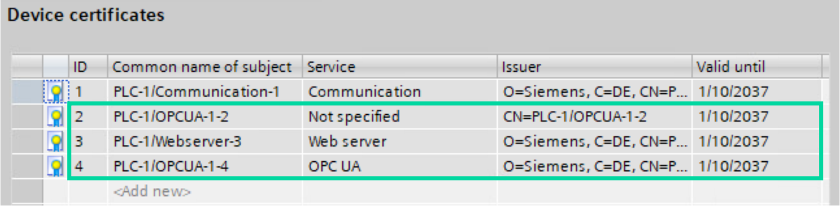


☑ Activate web server on this module

☑ Permit access only with HTTPS

□ Permit data access only via Web API

☑ Activate OPC UA server



Device certificates

ID	Common name of subject	Service	Issuer	Valid until
1	PLC-1/Communication-1	Communication	O=Siemens, C=DE, CN=P...	1/10/2037
2	PLC-1/OPCUA-1-2	Not specified	CN=PLC-1/OPCUA-1-2	1/10/2037
3	PLC-1/Webserver-3	Web server	O=Siemens, C=DE, CN=P...	1/10/2037
4	PLC-1/OPCUA-1-4	OPC UA	O=Siemens, C=DE, CN=P...	1/10/2037
	<Add new>			

NOTE

When the global security settings are activated, the contents of the local certificate manager are deleted, and the private keys cannot be restored.

2.3.3 Using the global certificate manager

Description

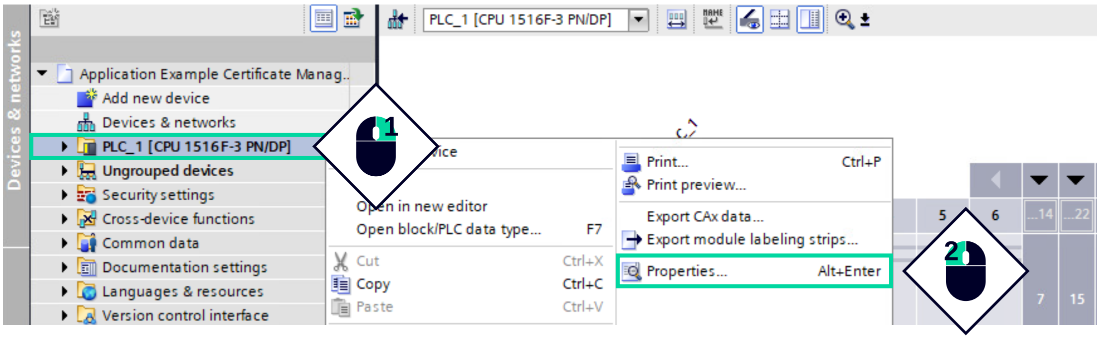
To access the global certificate manager the project must be protected from unauthorized access, which is done from the project's "Security settings".

In TIA Portal version V14, these settings become visible only after activating the global security settings on at least one device. Since TIA Portal version V15, such activation is no longer required, and the project's security settings are always visible.

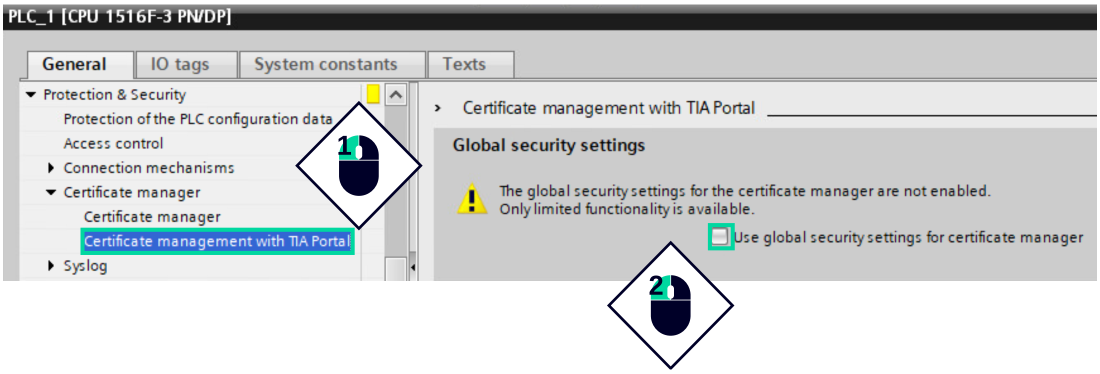
Access to the security settings of the project (only for TIA Portal version V14)

To access the security settings of a project in TIA Portal V14, these steps must be followed:

1. Select a CPU in the project tree and navigate to the "Properties" tab.



2. Select "Protection & Security > Certificate Manager > Certificate management with TIA Portal". Activate the function "Use global security settings for certificate manager".



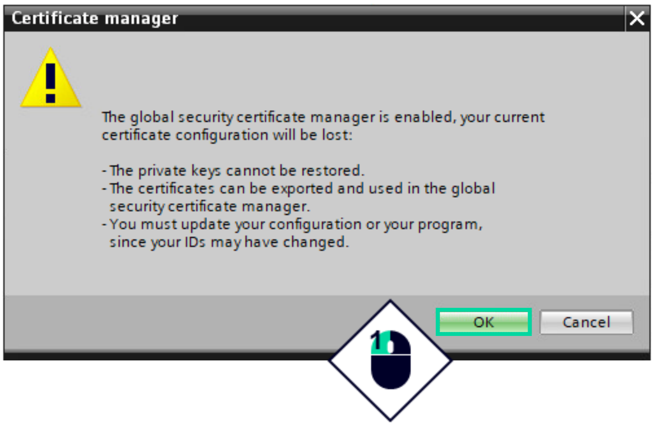
Certificate management with TIA Portal

Global security settings

The global security settings for the certificate manager are not enabled.
Only limited functionality is available.

□ Use global security settings for certificate manager

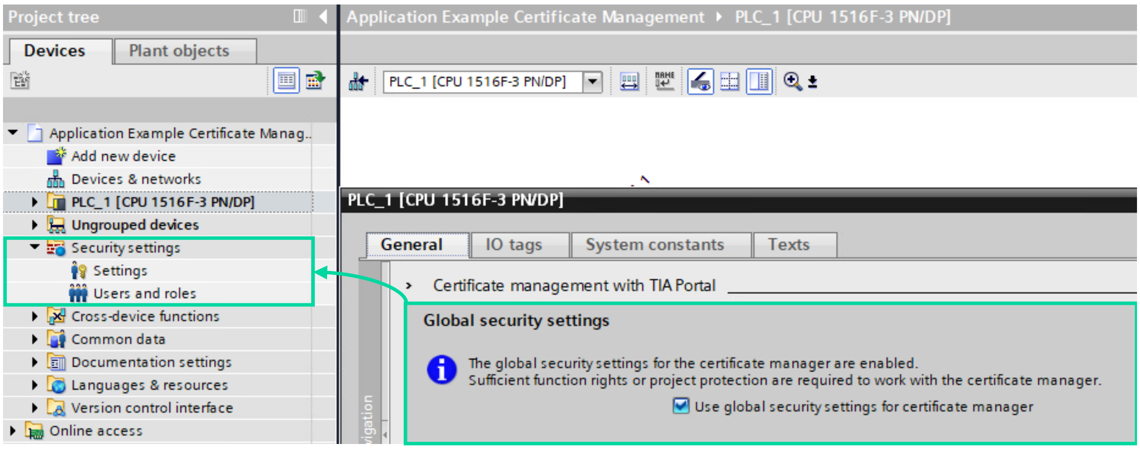
3. Confirm the following message with the "OK" button.



The global security certificate manager is enabled, your current certificate configuration will be lost:

- The private keys cannot be restored.
- The certificates can be exported and used in the global security certificate manager.
- You must update your configuration or your program, since your IDs may have changed.

As a result, the security settings of the project become visible.



The global security settings for the certificate manager are enabled.
Sufficient function rights or project protection are required to work with the certificate manager.

☑ Use global security settings for certificate manager

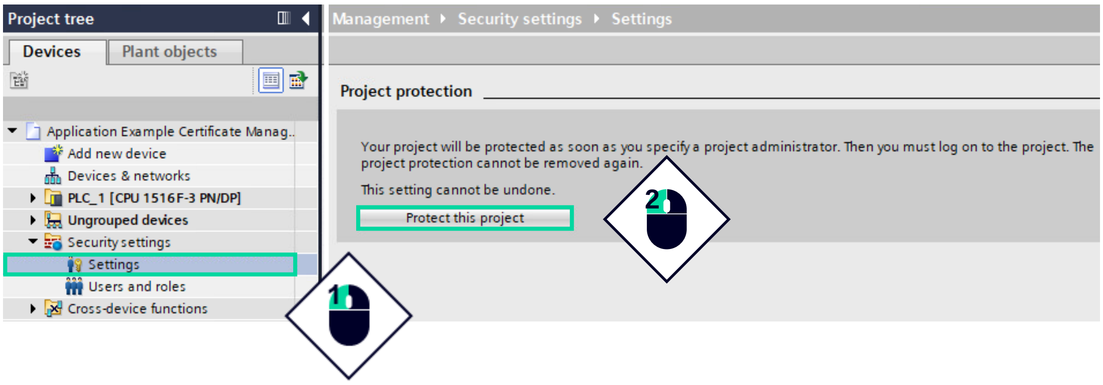
NOTE

Enabling the global security settings deletes the contents of the local certificate manager. Therefore, if any secure communications are being used, such as “Secure PG/PC and HMI Communication”, HTTPS, Secure OUC or OPC UA, new certificates need to be created.

Access to the global certificate manager

To access the global certificate manager, the project must be protected from unauthorized access. To create a project administrator:

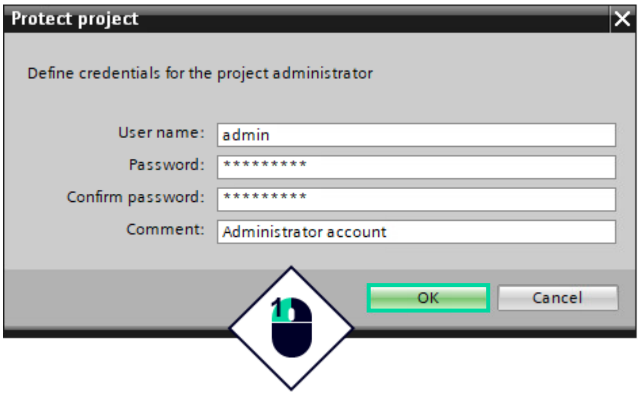
1. Double-click on the entry "Settings" in the project tree under "Security settings". Click the "Protect this project" button.



Your project will be protected as soon as you specify a project administrator. Then you must log on to the project. The project protection cannot be removed again.

This setting cannot be undone.

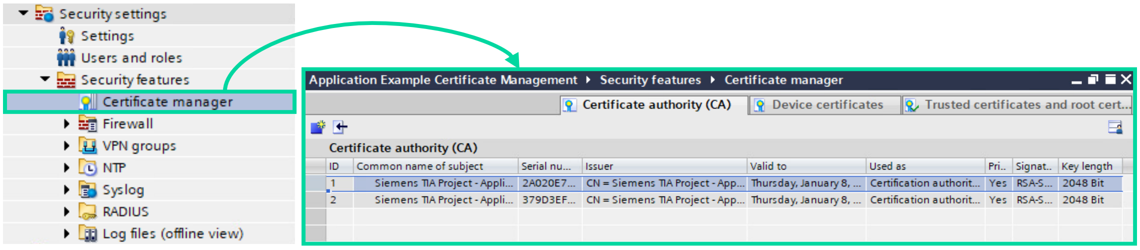
2. Define a username and password. Confirm the password and click on "OK".



Define credentials for the project administrator

User name: admin
Password: *********
Confirm password: *********
Comment: Administrator account

The “Certificate manager” will appear under the project’s “Security settings > Security features”.



Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signat..	Key length
1	Siemens TIA Project - Appli...	2A020E7...	CN = Siemens TIA Project - App...	Thursday, January 8, ...	Certification authorit...	Yes	RSA-S...	2048 Bit
2	Siemens TIA Project - Appli...	379D3EF...	CN = Siemens TIA Project - App...	Thursday, January 8, ...	Certification authorit...	Yes	RSA-S...	2048 Bit

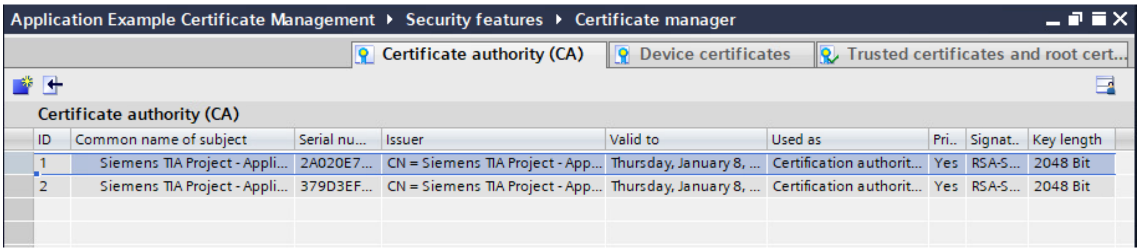
NOTE

> Following this step, the project can only be opened after logging in with admin credentials.

Default Certification Authorities

By default, two root certificates (Certification Authorities) are provided in each project:

- The first root certificate with ID=1 employs SHA1 as the hashing algorithm.
- The second Certification Authority with ID=2 is based on SHA-256.


Application Example Certificate Management ▸ Security features ▸ Certificate manager
Certificate authority (CA)
Device certificates
Trusted certificates and root cert...

Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signat..	Key length
1	Siemens TIA Project - Appli...	2A020E7...	CN = Siemens TIA Project - App...	Thursday, January 8, ...	Certification authorit...	Yes	RSA-S...	2048 Bit
2	Siemens TIA Project - Appli...	379D3EF...	CN = Siemens TIA Project - App...	Thursday, January 8, ...	Certification authorit...	Yes	RSA-S...	2048 Bit

NOTE

> SHA1 is deprecated and it is no longer considered secure, therefore the first CA should only be used in legacy systems that do not support SHA-256.

Certificate fields in the global certificate manager

Some of the most relevant fields shown in the global certificate manager are:

Field	Description
ID	Every certificate in the certificate manager receives a unique ID that cannot be changed. The certificate ID is assigned by the certificate manager when a certificate is created or imported.
Common name of subject	Device or certificate authority for which the certificate is valid.
Serial number	Unique serial number of the certificate.
Issuer	Shows the name, organization, and country of the certificate issuer.
Valid to	Indicates when the certificate expires.
Used as	Indicates for which application or service the certificate is used, e.g., as SSL certificate or certificate authority.
Private key	Indicates whether the private key exists in the project.
Signature algorithm	Indicates the cipher of the private key as well as the hash algorithm used.
Key length	Shows the key length of the certificate.

Functions of the global certificate manager

The global certificate manager contains an overview of all the certificates used in the project, and, in contrast to the local certificate manager, incorporates a wide variety of options to manage certificates, such as:

1. Import new certificates and certificate authorities.
2. Export certificates and certificate authorities used in the project.
3. Renewal of expired certificates and certificate authorities.
4. Replacement of existing certificates.
5. Adding trusted certificates and certification authorities.
6. Deleting manually imported certificates.

Exporting certificates

Certificates and private keys can be exported in various formats. Depending on the format, the following options are available during export.

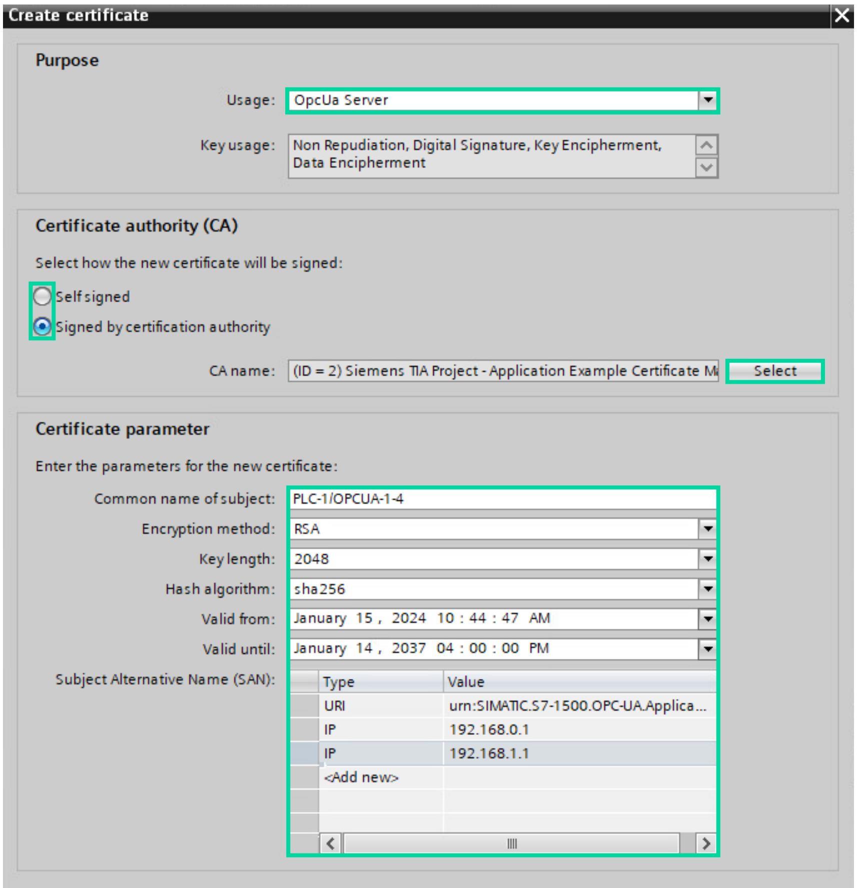
Available for selection during export	Format						Note
	.cer	.der	.crt	.pem	.crl	.p12	
Private key	x	x	x	x	-	x	For *.cer and *.der, an additional key file is exported for the certificate. The exported key file cannot be imported again. For *.crt and *.pem, the private key is stored together with the certificate in a file.
Encrypted private key	-	-	x	x	-	-	Selection of the encryption method and input of password possible. If no password is entered, the project name is used as the password.
Certificate chain	-	-	x	x	-	-	Only possible if the certificates of the certificate chain are stored in the certificate manager.
Password only	-	-	-	-	-	x	If no password is entered, the project name is used as password.
Revocation list	-	-	-	-	x	-	Certain programs, such as UaExpert, require revocation lists to establish trust relationships with root CAs. TIA Portal can only export empty revocation lists.

Creating and renewing certificates

Establishing new secure communication channels involves the creation of digital certificates. Once created, long-term maintenance is achieved through the renewal of these certificates, allowing users to update the validity period of expired certificates or adjust the encryption and hashing algorithms if they become deprecated.

The creation and renewal of certificates is done through the pop-up window depicted below. To configure new certificates, the following steps must be carried out.

1. Specify the intended purpose of the certificate by choosing a predefined template. Depending on the intended use, specific "KeyUsage" and "ExtendedKeyUsage" extensions will be incorporated into the certificate.
2. Select the issuer of the new certificate: self-signed or signed by a Certificate Authority.
3. If the certificate is issued by a Certificate Authority, select it with the "Select" button. Only certification authorities from the certificate store of the current project, equipped with a private key, can be selected.
4. Depending on the certificate, enter the following parameters in the corresponding input fields:
   - Common name of subject: name associated with the certificate holder.
   - Encryption method: cipher algorithm used to perform asymmetric encryption.
   - Key length: Depends on the cipher. For RSA, it represents the key length in bits, while for EC, it corresponds to the ECC curve (e.g., prime256v1, secp256r1, secp384r1).
   - Hash algorithm: algorithm used for signing the certificate.
   - Valid from/until: validity period of the certificate.
   - Subject alternative name (SAN): additional host names, IP addresses, email addresses, and other identifiers associated with the certificate subject beyond the common name.



Create certificate

Purpose

Usage: OpcUa Server

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Data Encipherment

Certificate authority (CA)

Select how the new certificate will be signed:

○ Self signed

● Signed by certification authority

CA name: (ID = 2) Siemens TIA Project - Application Example Certificate M

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1/OPCUA-1-4

Encryption method: RSA

Key length: 2048

Hash algorithm: sha256

Valid from: January 15 , 2024 10 : 44 : 47 AM

Valid until: January 14 , 2037 04 : 00 : 00 PM

Subject Alternative Name (SAN):

Type	Value
URI	urn:SIMATIC.S7-1500.OPC-UA.Applica...
IP	192.168.0.1
IP	192.168.1.1
<Add new>	

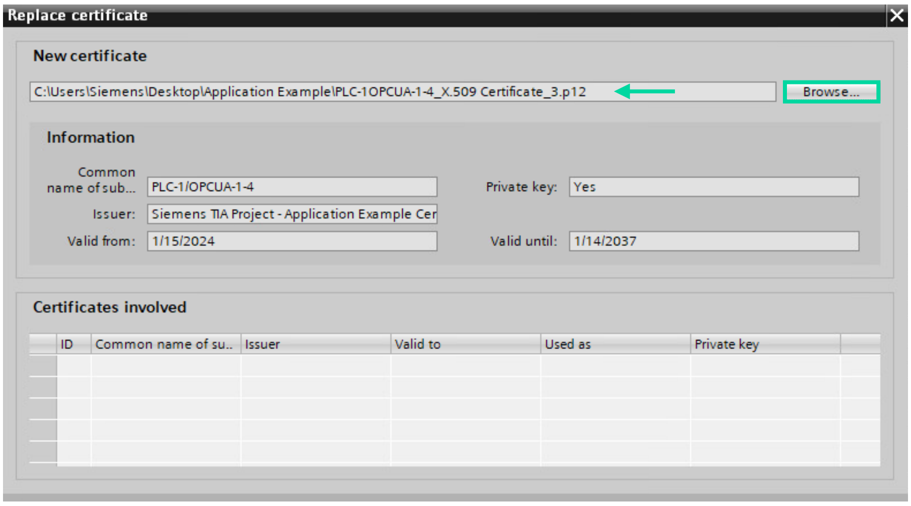
NOTE

When certificates are created from the global certificate manager, a blank canvas is provided. In contrast, generating certificates directly from the CPU offers templates that streamline the creation process.

Creating a certificate from the CPU does not restrict the certificate to the local certificate manager of the device. With the global security settings activated, these certificates can also be accessed and managed through the global certificate manager.

Replacing certificates

The process of replacing certificates enables the substitution of an existing certificate with a new .p12 certificate while preserving its unique ID within the global certificate manager. The benefits of replacing certificates instead of importing or creating new ones is explained in section 2.3.4.



Replace certificate

New certificate

C:\Users\Siemens\Desktop\Application Example\PLC-1OPCUA-1-4_X.509 Certificate_3.p12

Information

Common name of sub...	PLC-1/OPCUA-1-4	Private key:	Yes
Issuer:	Siemens TIA Project - Application Example Cer		
Valid from:	1/15/2024	Valid until:	1/14/2037

Certificates involved

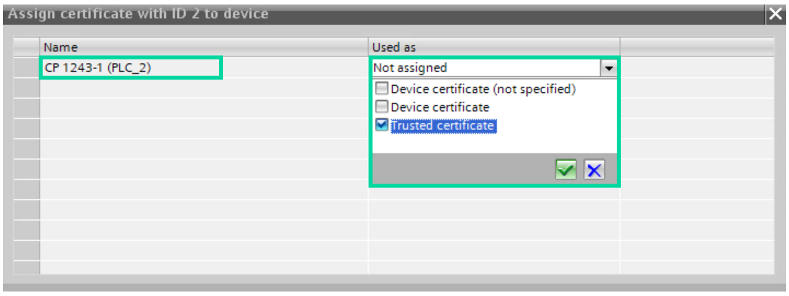
ID	Common name of su..	Issuer	Valid to	Used as	Private key

Assigning certificates

When integrating other devices, such as communication processors (CPs), certificates need to be assigned through the global certificate manager. The dialog "Assign certificate with ID x to device" provides the mechanism to transfer certificates to these processors.

As shown in the manual (https://support.industry.siemens.com/cs/document/103948898) of the CP 1243-1, to assign trusted partner certificates to the CP via the global certificate manager:

1. Right-click on the desired certificate.
2. Select "Assign" in the shortcut menu.
3. Mark the device/module in the subsequent dialog.
4. Define how the certificate is to be assigned in the "Used as" field:
   - Device certificate (not specified): e.g., for Secure OUC or blocks.
   - Device certificate: Web server certificate.
   - Trusted certificate: e.g., OPC UA.



Assign certificate with ID 2 to device

Name	Used as
CP 1243-1 (PLC_2)	Not assigned

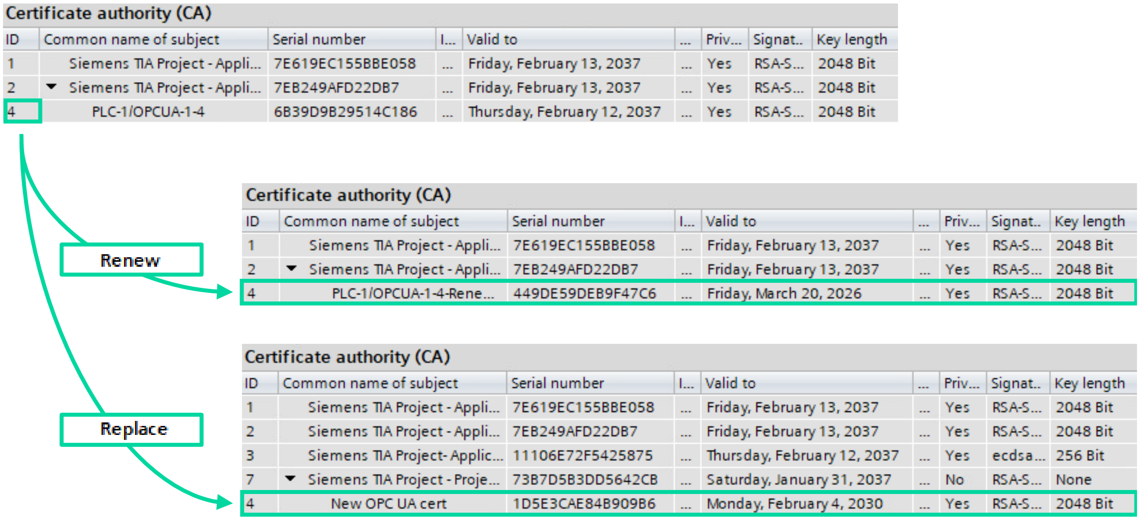
☐ Device certificate (not specified)
☐ Device certificate
☑ Trusted certificate

Only one certificate per device can be used as a “Device certificate”. Once assigned, the certificate appears in the "Certificates of the partner devices" table in the local certificate manager of the module.

2.3.4 Loading certificates to the CPU during runtime

Downloading certificates to the CPU is part of the hardware configuration. Traditionally, applying changes to the hardware configuration requires the CPU to be in STOP mode, which, in turn, halts production processes. However, with TIA V19 and FW 3.1, new certificates can be loaded to the CPU during runtime.

To do so, new certificates need to have the same certificate ID in the global certificate manager as the ones already loaded on the device. The only available means to generate new certificates with matching IDs are the "Renew" and "Replace” methods.



Certificate authority (CA)

ID	Common name of subject	Serial number	I...	Valid to	...	Priv...	Signat..	Key length
1	Siemens TIA Project - Appli...	7E619EC155BBE058	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
2	▼ Siemens TIA Project - Appli...	7EB249AFD22DB7	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
4	PLC-1/OPCUA-1-4	6B39D9B29514C186	...	Thursday, February 12, 2037	...	Yes	RSA-S...	2048 Bit

Certificate authority (CA)

ID	Common name of subject	Serial number	I...	Valid to	...	Priv...	Signat..	Key length
1	Siemens TIA Project - Appli...	7E619EC155BBE058	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
2	▼ Siemens TIA Project - Appli...	7EB249AFD22DB7	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
4	PLC-1/OPCUA-1-4-Rene...	449DE59DEB9F47C6	...	Friday, March 20, 2026	...	Yes	RSA-S...	2048 Bit

Certificate authority (CA)

ID	Common name of subject	Serial number	I...	Valid to	...	Priv...	Signat..	Key length
1	Siemens TIA Project - Appli...	7E619EC155BBE058	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
2	Siemens TIA Project - Appli...	7EB249AFD22DB7	...	Friday, February 13, 2037	...	Yes	RSA-S...	2048 Bit
3	Siemens TIA Project- Applic...	11106E72F5425875	...	Thursday, February 12, 2037	...	Yes	ecdsa...	256 Bit
7	▼ Siemens TIA Project - Proje...	73B7D5B3DD5642CB	...	Saturday, January 31, 2037	...	No	RSA-S...	None
4	New OPC UA cert	1D5E3CAE84B909B6	...	Monday, February 4, 2030	...	Yes	RSA-S...	2048 Bit

NOTE

To upload certificates, users must be logged in with an admin account. Newly created admin users need to sign out and log in again to be able to load certificates during runtime.

2.4 Certificates in the scope of OPC UA communication

2.4.1 Overview on OPC UA communication

Description

OPC UA communication in S7-1200/S7-1500 CPUs follows a client-server approach. In this model, servers provide services such as read, write, browse, subscribe, and more, enabling clients to access data stored in their AddressSpace.

For a secure connection to be established, the client must validate and accept the digital certificate presented by the server, deeming it trustworthy. Simultaneously, the server is required to verify the certificate provided by the client, ensuring mutual authentication.

Once the secure connection is established via the Public Key Infrastructure, a shared key is transmitted, and communication transitions to symmetric encryption.

OPC UA certificates

OPC UA certificates adhere to the format specified by X-509 Version 3 of the ITU (International Telecommunication Union) for the authentication of client and server.

When a connection is being established between both entities, the devices check all information from the certificate that is required to determine its integrity, such as signature, period of validity, application name (URI) and, in case of firmware version V2.5 (S7-1500 CPU), also the IP address of the client.

2.4.2 Security settings for the OPC UA server

Security policies and security modes

Server endpoints can be configured with different “SecurityModes” and “SecurityPolicies”.

SecurityMode	Description
None	No security is applied, and communication is in plaintext.
Sign	Sign security mode ensures message integrity by adding a digital signature to each message. The signature is generated using the private key of the sender and can be verified using the sender's public key. This ensures that the message has not been tampered with during transmission.
Sign & Encrypt	Sign&Encrypt security mode provides both message integrity and confidentiality. In addition to generating a digital signature, this mode encrypts the message to prevent unauthorized access or reading of the message content. The encryption is performed using a shared secret key that is negotiated between the sender and receiver during the communication process.

SecurityPolicy	Description
None	No security is applied, and communication is in plaintext.
Basic128Rsa15 (deprecated)	128-bit encryption keys and RSA 15 encryption algorithm.
Basic256 (deprecated)	256-bit encryption keys and AES encryption algorithm.
Basic256Sha256	256-bit encryption keys and SHA-256 hashing algorithm.
Aes128Sha256RsaOaep	Advanced Encryption Standard (AES) with 128-bit key size and SHA-256 hashing algorithm, and RSA with Optimal Asymmetric Encryption Padding (OAEP) for key exchange.
Aes256Sha256RsaPss	AES with 256-bit key size and SHA-256 hashing algorithm for message integrity, and RSA with Probabilistic Signature Scheme (PSS) for key exchange.

User authentication

In addition to transport layer security, OPC UA can use application-based security to control access to the server, known as authentication. This mechanism is performed each time a new session is activated.

During this process, the client is given a “userIdentityToken”, which allows the server to determine if the token is authorized to establish a connection. This introduces an additional layer of security, as not only the client certificate needs to be trusted, but also a valid token must be provided for user authentication.

There are several types of user authentication methods in OPC UA, including:

Token	Description
Anonymous	Clients can connect to the server without providing any user identity.
Username and password	Clients provide a username and password, which are authenticated by the server.
X-509 Certificate	Clients provide a digital certificate that is validated by the server.

NOTE

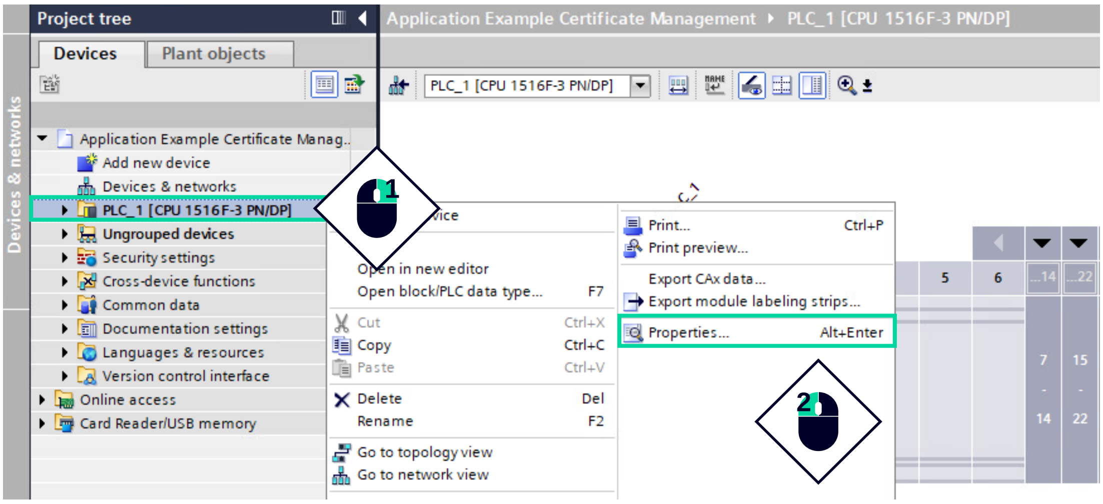
Since S7-1200/S7-1500 CPUs do not support user authentication through X-509 certificates, no additional information will be provided in this document.

2.4.3 Setting up the OPC UA server

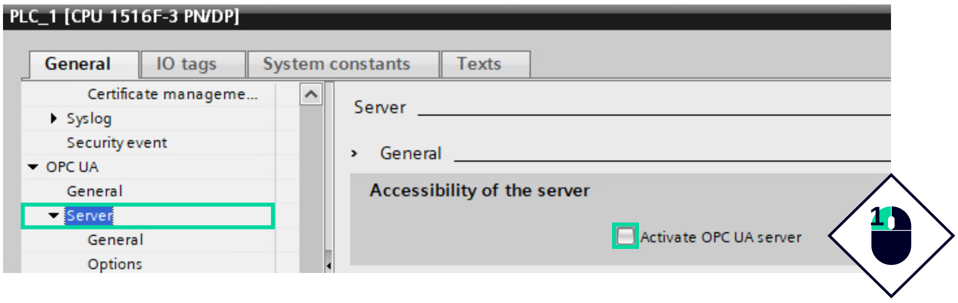
Commissioning an OPC UA server

For security reasons, the OPC UA server is not enabled by default. To activate the server of the CPU, proceed as follows:

1. Select the CPU in the project tree and navigate to the “Properties” tab.



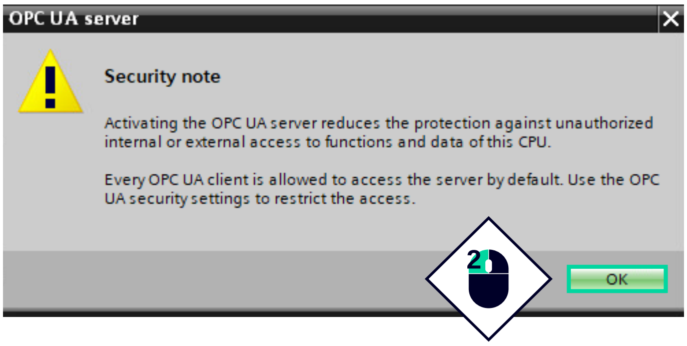
2. Navigate to the entry "OPC UA > Server". Activate the server and confirm the security message.



PLC_1 [CPU 1516F-3 PN/DP]

Accessibility of the server

□ Activate OPC UA server



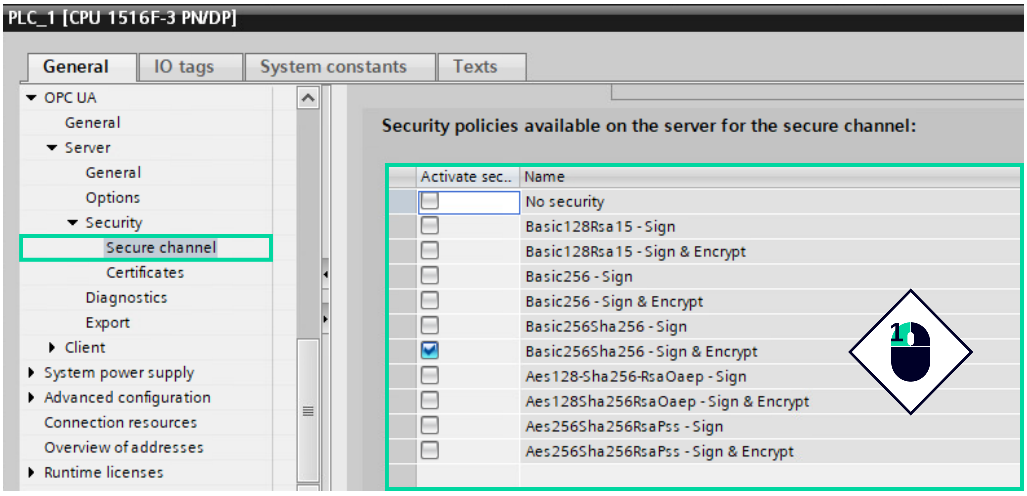
OPC UA server

Security note

Activating the OPC UA server reduces the protection against unauthorized internal or external access to functions and data of this CPU.

Every OPC UA client is allowed to access the server by default. Use the OPC UA security settings to restrict the access.

3. In “OPC UA > Server > Security > Secure channel”, select the server endpoints that will be available for OPC UA clients (security policies and modes).

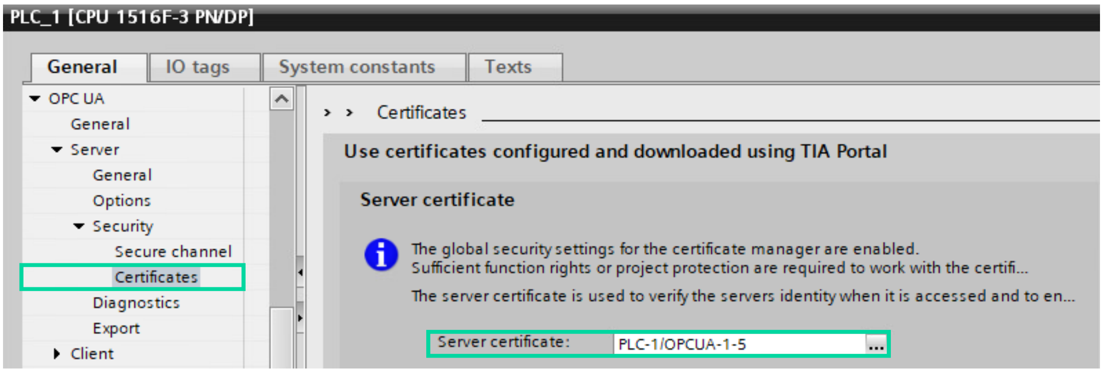


PLC_1 [CPU 1516F-3 PN/DP]

Security policies available on the server for the secure channel:

Activate sec..	Name
□	No security
□	Basic128Rsa15 - Sign
□	Basic128Rsa15 - Sign & Encrypt
□	Basic256 - Sign
□	Basic256 - Sign & Encrypt
□	Basic256Sha256 - Sign
☑	Basic256Sha256 - Sign & Encrypt
□	Aes128-Sha256-RsaOaep - Sign
□	Aes128Sha256RsaOaep - Sign & Encrypt
□	Aes256Sha256RsaPss - Sign
□	Aes256Sha256RsaPss - Sign & Encrypt

4. By default, a server certificate is automatically generated in the local certificate manager of the device. As can be seen here, the certificate shown below is issued by TIA's Certification Authority (ID=2).



Use certificates configured and downloaded using TIA Portal

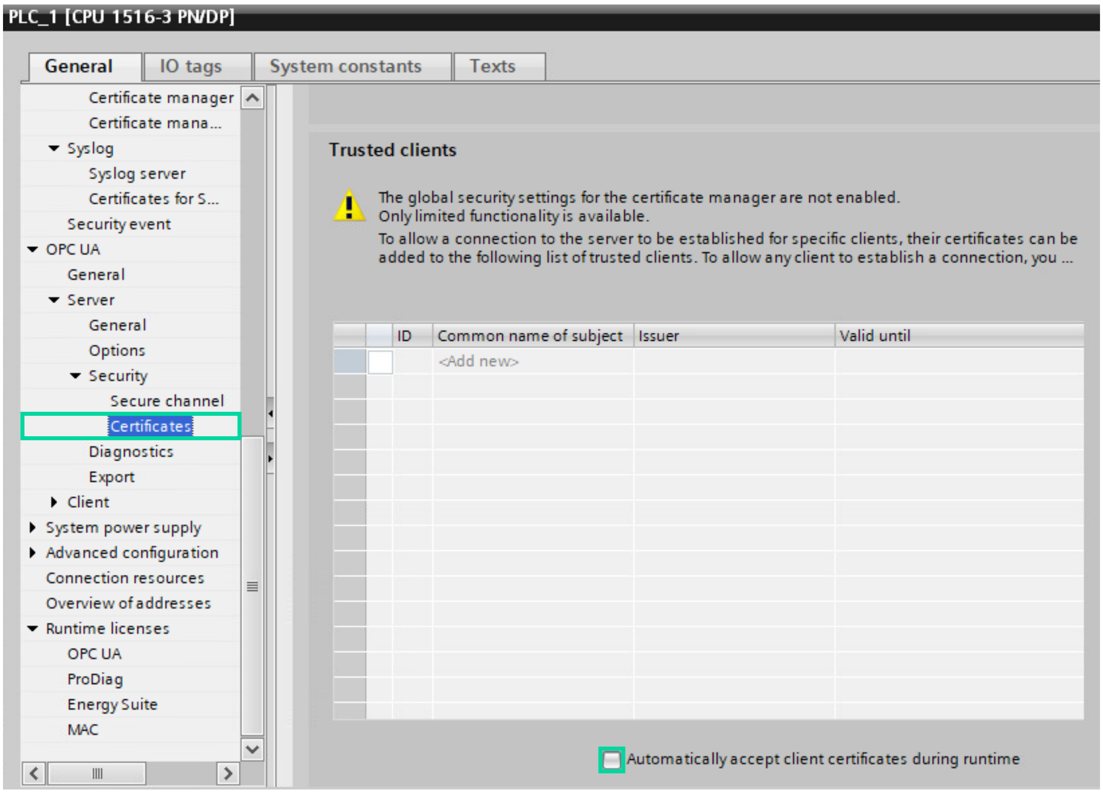
Server certificate

The global security settings for the certificate manager are enabled.
Sufficient function rights or project protection are required to work with the certifi...

The server certificate is used to verify the servers identity when it is accessed and to en...

Server certificate: PLC-1/OPCUA-1-5

5. Beneath the server's certificate is the store for trusted OPC UA clients. To restrict connections exclusively to trusted clients, the "Automatically accept client certificates during runtime" checkbox must be disabled.



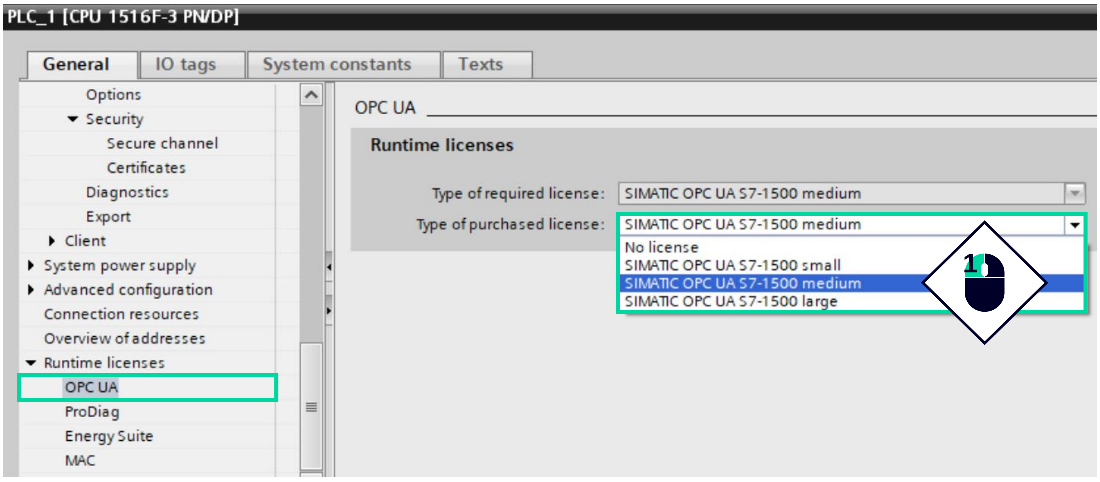
Trusted clients

The global security settings for the certificate manager are not enabled.
Only limited functionality is available.
To allow a connection to the server to be established for specific clients, their certificates can be added to the following list of trusted clients. To allow any client to establish a connection, you ...

ID	Common name of subject	Issuer	Valid until
	<Add new>		

□ Automatically accept client certificates during runtime

6. 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".



PLC_1 [CPU 1516F-3 PN/DP]

OPC UA

Runtime licenses

Type of required license: SIMATIC OPC UA S7-1500 medium

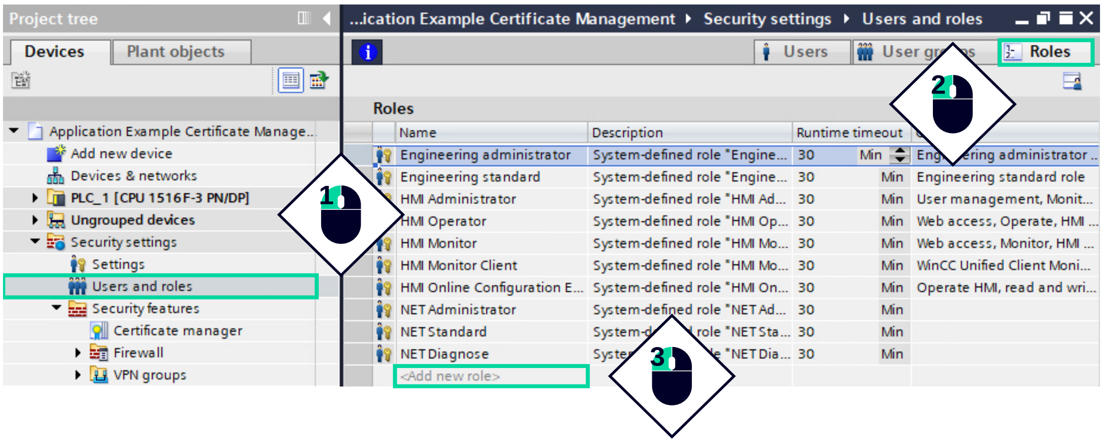
Type of purchased license: SIMATIC OPC UA S7-1500 medium

- No license
- SIMATIC OPC UA S7-1500 small
- SIMATIC OPC UA S7-1500 medium
- SIMATIC OPC UA S7-1500 large

User authentication

CPUs with firmware version 3.1 do not provide the option to manage user access directly from the CPU settings. To create a new user with "OPC UA server access":

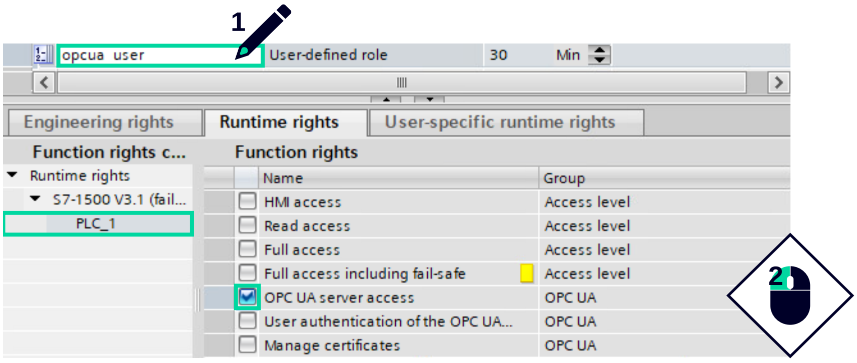
1. Double click on “Security settings > Users and roles” and open the “Roles” tab. Click on “<Add new role>”.



Roles

	Name	Description	Runtime timeout		
	Engineering administrator	System-defined role "Engine...	30	Min	Engineering administrator ...
	Engineering standard	System-defined role "Engine...	30	Min	Engineering standard role
	HMI Administrator	System-defined role "HMI Ad...	30	Min	User management, Monit...
	HMI Operator	System-defined role "HMI Op...	30	Min	Web access, Operate, HMI ...
	HMI Monitor	System-defined role "HMI Mo...	30	Min	Web access, Monitor, HMI ...
	HMI Monitor Client	System-defined role "HMI Mo...	30	Min	WinCC Unified Client Moni...
	HMI Online Configuration E...	System-defined role "HMI On...	30	Min	Operate HMI, read and wri...
	NET Administrator	System-defined role "NET Ad...	30	Min	
	NET Standard	System-defined role "NET Sta...	30	Min	
	NET Diagnose	System-defined role "NET Dia...	30	Min	
	<Add new role>				

2. Create a new role for an OPC UA user. Select “OPC UA server access” from the “Runtime rights” of the target CPU.

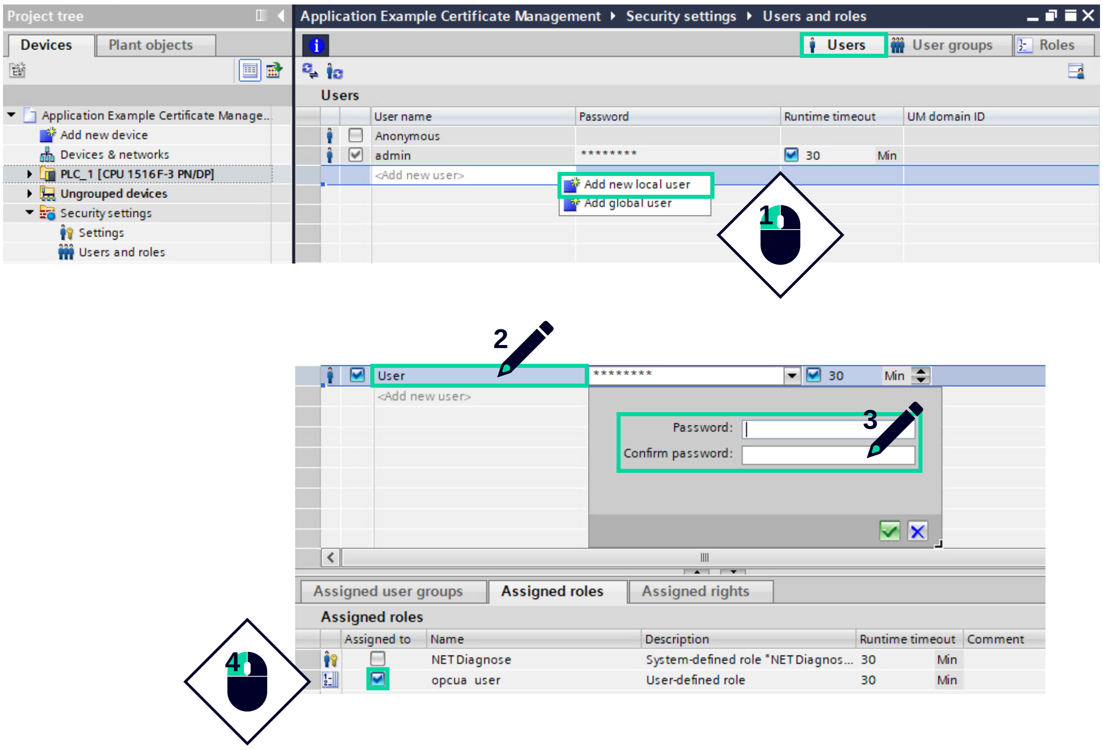


opcua_user | User-defined role | 30 | Min

Function rights

	Name	Group
☐	HMI access	Access level
☐	Read access	Access level
☐	Full access	Access level
☐	Full access including fail-safe	Access level
☑	OPC UA server access	OPC UA
☐	User authentication of the OPC UA...	OPC UA
☐	Manage certificates	OPC UA

3. “Add a new local user” and assign it a username and password. Select the role with OPC UA server access.



Users

	User name	Password	Runtime timeout		UM domain ID
□	Anonymous				
☑	admin	********	☑ 30	Min	
	<Add new user>				

	User	********	☑ 30	Min
	<Add new user>			

Password:

Confirm password:

Assigned roles

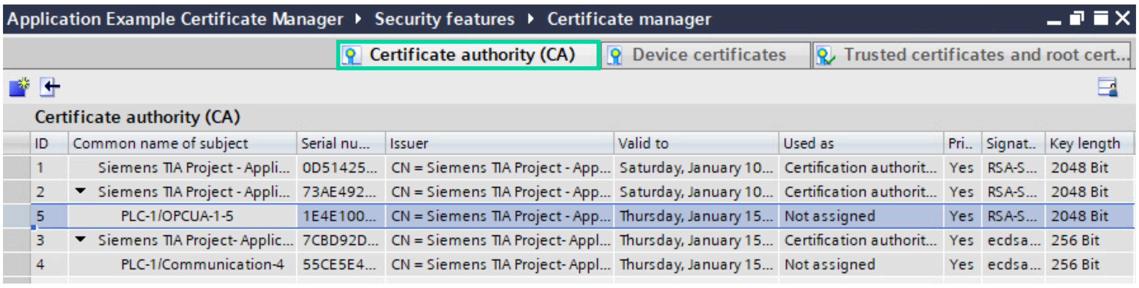
Assigned to	Name	Description	Runtime timeout		Comment
□	NET Diagnose	System-defined role "NET Diagnos...	30	Min	
☑	opcua user	User-defined role	30	Min	

NOTE

While not advisable, it is possible to implement anonymous user authentication by activating the default "Anonymous" user and assigning it the recently created "opcua user" role.

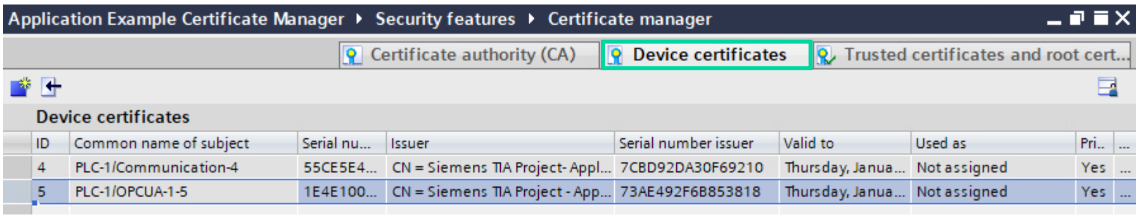
View the server certificate

In section 2.3.3, the CPU was set up with the global security settings. As a result, the server’s certificate can be managed through the global certificate manager, where it can be found under the “Certificate authority (CA)” and "Device certificates" tabs.


Application Example Certificate Manager ▸ Security features ▸ Certificate manager
Certificate authority (CA)
Device certificates
Trusted certificates and root cert...

Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signat..	Key length
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
2	Siemens TIA Project - Appli...	73AE492...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
5	PLC-1/OPCUA-1-5	1E4E100...	CN = Siemens TIA Project - App...	Thursday, January 15...	Not assigned	Yes	RSA-S...	2048 Bit
3	Siemens TIA Project- Applic...	7CBD92D...	CN = Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...	Yes	ecdsa...	256 Bit
4	PLC-1/Communication-4	55CE5E4...	CN = Siemens TIA Project- Appl...	Thursday, January 15...	Not assigned	Yes	ecdsa...	256 Bit


Application Example Certificate Manager ▸ Security features ▸ Certificate manager
Certificate authority (CA)
Device certificates
Trusted certificates and root cert...

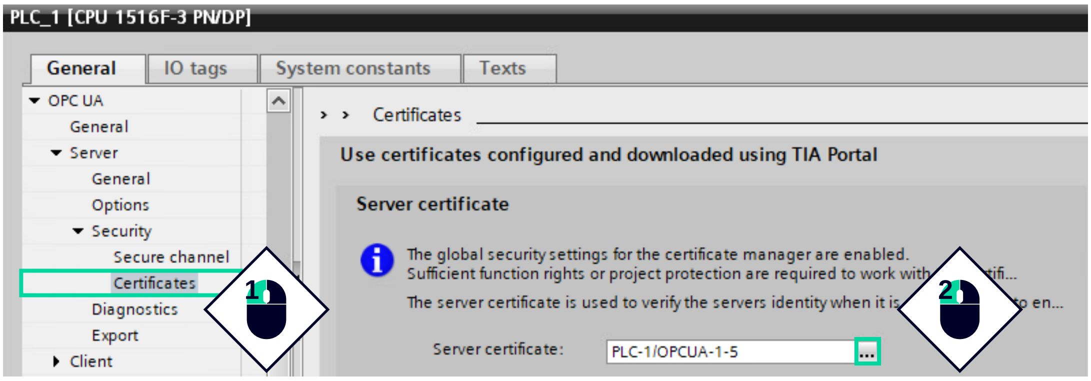
Device certificates

ID	Common name of subject	Serial nu...	Issuer	Serial number issuer	Valid to	Used as	Pri..	...
4	PLC-1/Communication-4	55CE5E4...	CN = Siemens TIA Project- Appl...	7CBD92DA30F69210	Thursday, Janua...	Not assigned	Yes	...
5	PLC-1/OPCUA-1-5	1E4E100...	CN = Siemens TIA Project - App...	73AE492F6B853818	Thursday, Janua...	Not assigned	Yes	...

Create a new server certificate

If the server certificate was deleted due to the activation of the global security settings, proceed as follows to generate a new certificate for the server:

1. Select the entry "OPC UA > Server > Security > Certificates" in the navigation area.
2. To generate a new server certificate or substitute it with an existing one, click on the button integrated in the "Server certificate" drop-down list.



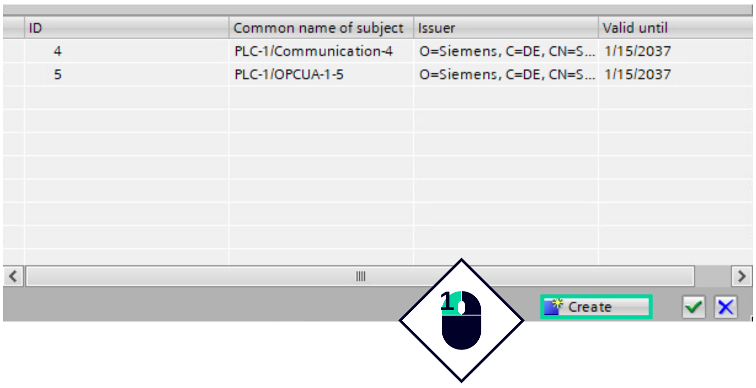
Use certificates configured and downloaded using TIA Portal

Server certificate

The global security settings for the certificate manager are enabled.
Sufficient function rights or project protection are required to work with ...tifi...
The server certificate is used to verify the servers identity when it is ...o en...

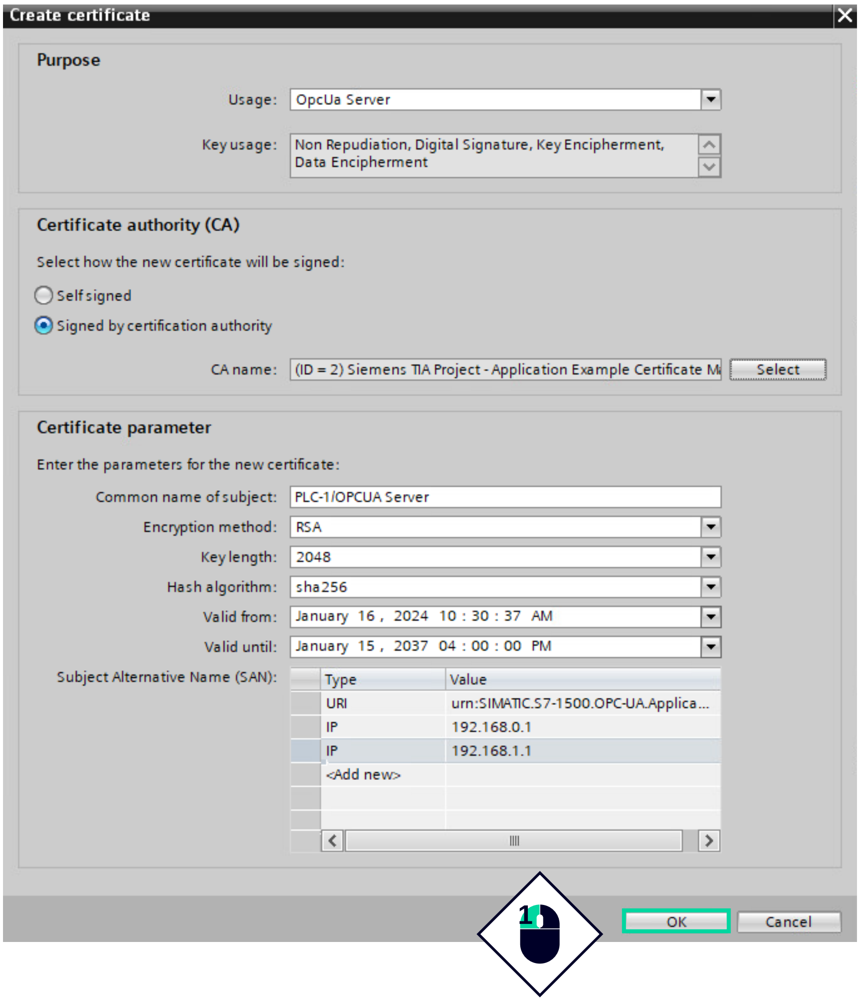
Server certificate: PLC-1/OPCUA-1-5

3. A dialog appears with all available server certificates. To create a new certificate, click on the "Create" button.



ID	Common name of subject	Issuer	Valid until
4	PLC-1/Communication-4	O=Siemens, C=DE, CN=S...	1/15/2037
5	PLC-1/OPCUA-1-5	O=Siemens, C=DE, CN=S...	1/15/2037

4. The dialog "Create certificate" appears. Automatically, the certificate is assigned with the necessary Subject Alternativ Name (SAN) fields.



Create certificate

Purpose

Usage: OpcUa Server

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Data Encipherment

Certificate authority (CA)

Select how the new certificate will be signed:

○ Self signed

● Signed by certification authority

CA name: (ID = 2) Siemens TIA Project - Application Example Certificate M

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1/OPCUA Server

Encryption method: RSA

Key length: 2048

Hash algorithm: sha256

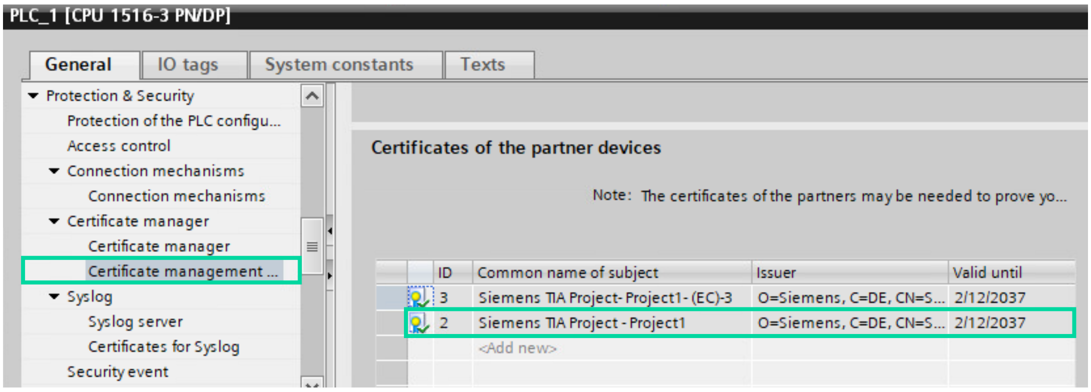
Valid from: January 16 , 2024 10 : 30 : 37 AM

Valid until: January 15 , 2037 04 : 00 : 00 PM

Subject Alternative Name (SAN):

Type	Value
URI	urn:SIMATIC.S7-1500.OPC-UA.Applica...
IP	192.168.0.1
IP	192.168.1.1
<Add new>	

5. If the new certificate is issued by a Certificate Authority, the CA’s certificate must be transferred to the “trusted device certificates” within the CPU's local certificate manager. This is done automatically when the project is compiled.



PLC_1 [CPU 1516-3 PN/DP]

Certificates of the partner devices

Note: The certificates of the partners may be needed to prove yo...

ID	Common name of subject	Issuer	Valid until
3	Siemens TIA Project- Project1- (EC)-3	O=Siemens, C=DE, CN=S...	2/12/2037
2	Siemens TIA Project - Project1	O=Siemens, C=DE, CN=S...	2/12/2037
	<Add new>		

2.4.4 Setting up the OPC UA client

Description

In this application example, UaExpert is used as an OPC UA client. Developed by Unified Automation, UaExpert is an easy-to-use, out-of-the-box software application that acts as a client and allows users to access and test connections with OPC UA servers.

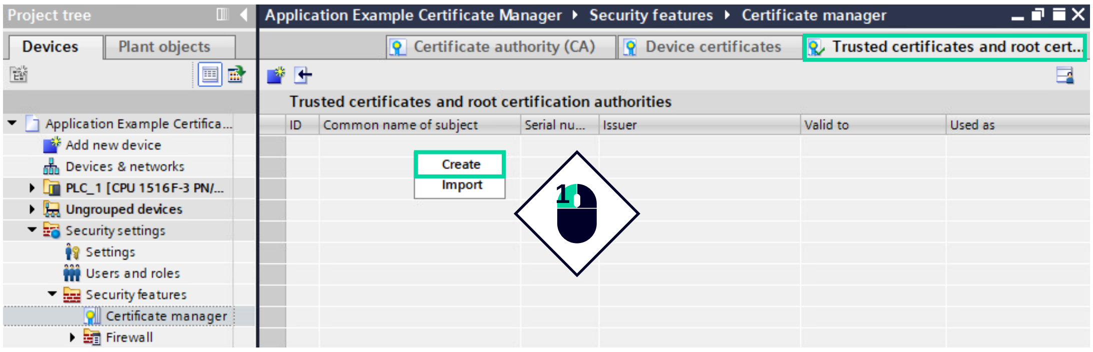
Creation of the client’s certificate

By default, UaExpert generates its own self-signed certificate. To ensure a secure connection with the OPC UA server, it is necessary to import this certificate into the local certificate manager of the CPU, designating it as a trusted device certificate.

However, to take advantage of the trust chain associated with Certificate Authorities, a new certificate for UaExpert will be generated using the default CA from TIA’s certificate manager (ID=2), thereby granting it direct trust and access.

To create the client’s certificate:

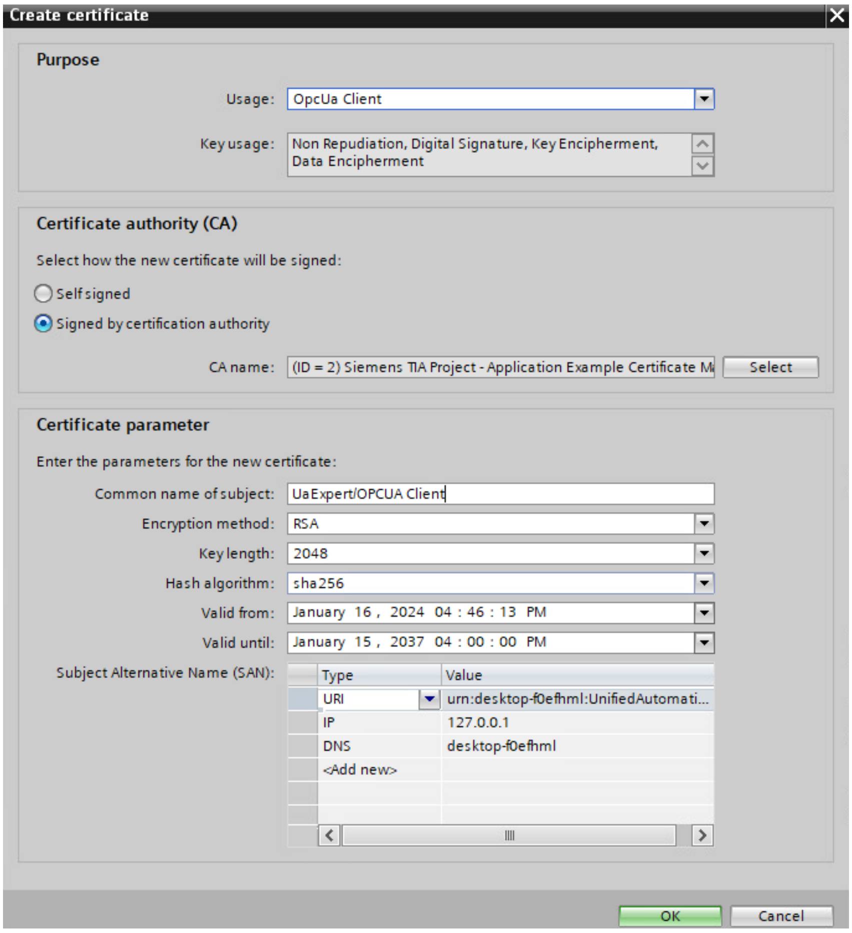
1. Open the global certificate manager. Right-click on an empty row and select "Create" from the context menu.


Project tree
Devices
Plant objects
Application Example Certifica...
Add new device
Devices & networks
PLC_1 [CPU 1516F-3 PN/...
Ungrouped devices
Security settings
Settings
Users and roles
Security features
Certificate manager
Firewall
Application Example Certificate Manager ▸ Security features ▸ Certificate manager
Certificate authority (CA)
Device certificates
Trusted certificates and root cert...
Trusted certificates and root certification authorities
ID
Common name of subject
Serial nu...
Issuer
Valid to
Used as
Create
Import
1

2. In the “Create certificate” window, insert all fields needed to generate the certificate. The Subject Alternative Names for this certificate are:
   - URI: *urn:[PC_Hostname]:UnifiedAutomation:UaExpert*
   - IP: *[IP Address of the client]*
   - DNS: *[PC_Hostname]*

NOTE

> To establish a secure connection with OPC UA servers running on SIMATIC PLCs, client certificates only require the URI field. For PLCs operating on FW version 2.5, the IP is also mandatory.
>
> While some fields are optional, it is advisable to include them all, as other communication partners may consider them compulsory.



Create certificate

Purpose

Usage: OpcUa Client

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Data Encipherment

Certificate authority (CA)

Select how the new certificate will be signed:

○ Self signed

● Signed by certification authority

CA name: (ID = 2) Siemens TIA Project - Application Example Certificate M

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: UaExpert/OPCUA Client

Encryption method: RSA

Key length: 2048

Hash algorithm: sha256

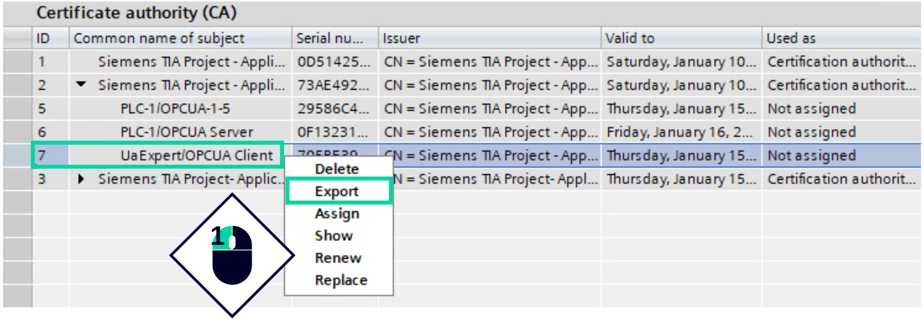
Valid from: January 16 , 2024 04 : 46 : 13 PM

Valid until: January 15 , 2037 04 : 00 : 00 PM

Subject Alternative Name (SAN):

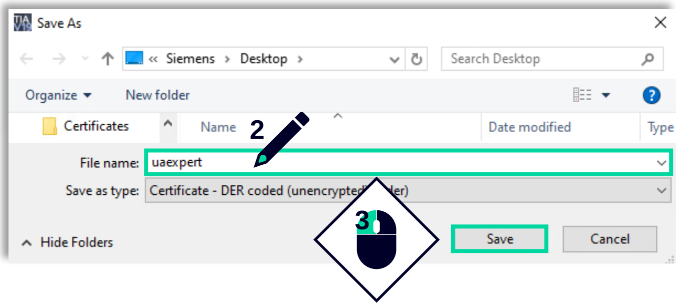
Type	Value
URI	urn:desktop-f0efhml:UnifiedAutomati...
IP	127.0.0.1
DNS	desktop-f0efhml
<Add new>	

3. Upon generating the client's certificate, export it in .der format with the name "uaexpert.der," excluding the private key from the export.



Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
2	Siemens TIA Project - Appli...	73AE492...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
5	PLC-1/OPCUA-1-5	29586C4...	CN = Siemens TIA Project - App...	Thursday, January 15...	Not assigned
6	PLC-1/OPCUA Server	0F13231...	CN = Siemens TIA Project - App...	Friday, January 16, 2...	Not assigned
7	UaExpert/OPCUA Client	70FBF39...	CN = Siemens TIA Project - App...	Thursday, January 15...	Not assigned
3	Siemens TIA Project- Applic...		N = Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...



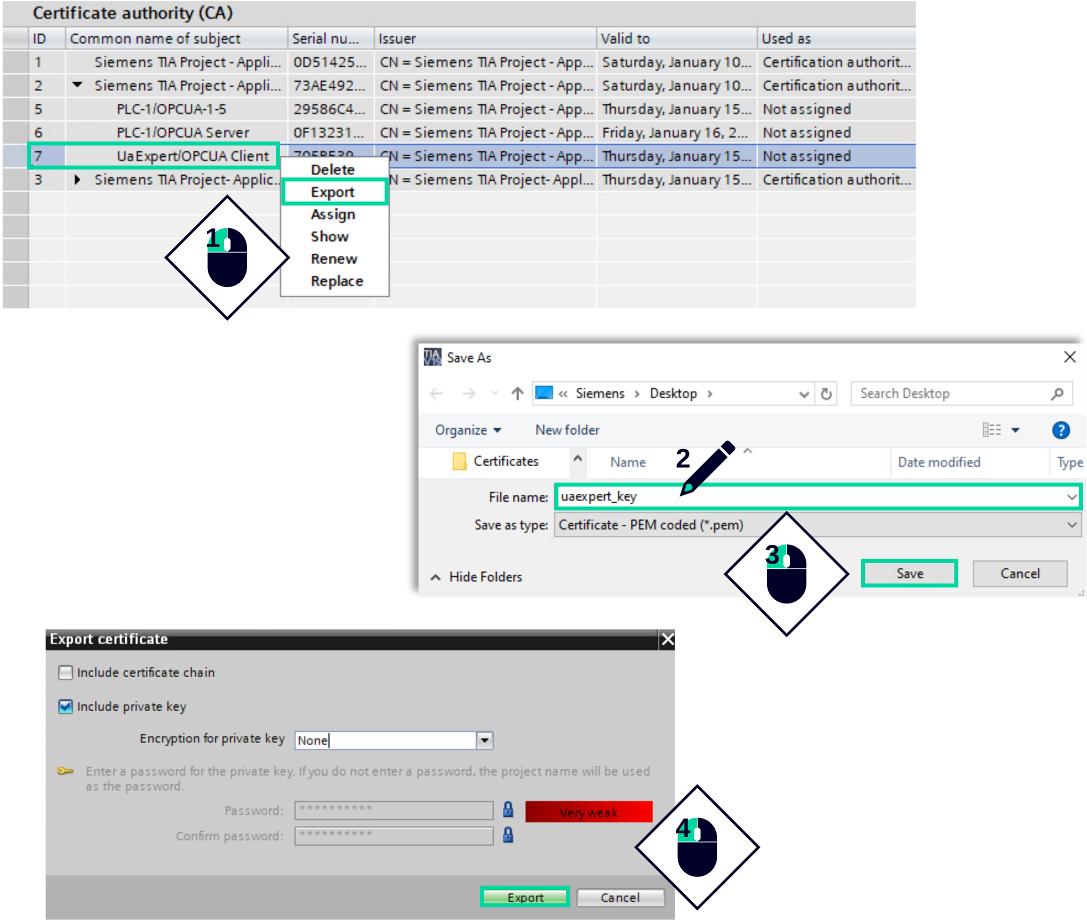
Save As

« Siemens › Desktop ›

File name: uaexpert

Save as type: Certificate - DER coded (unencrypted ...er)

4. To sign and decrypt messages, the client also requires the matching private key. Repeat the steps to export the private key in .pem format. Save the key without encryption and rename it as “uaexpert_key.pem” to ensure that UaExpert can read it.



Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
2	Siemens TIA Project - Appli...	73AE492...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
5	PLC-1/OPCUA-1-5	29586C4...	CN = Siemens TIA Project - App...	Thursday, January 15...	Not assigned
6	PLC-1/OPCUA Server	0F13231...	CN = Siemens TIA Project - App...	Friday, January 16, 2...	Not assigned
7	UaExpert/OPCUA Client	70FB530...	CN = Siemens TIA Project - App...	Thursday, January 15...	Not assigned
3	Siemens TIA Project- Applic...		N = Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...

Save As

« Siemens › Desktop ›

Search Desktop

Organize ▾ New folder

Certificates

Name | Date modified | Type

File name: uaexpert_key

Save as type: Certificate - PEM coded (*.pem)

Hide Folders

Export certificate

☐ Include certificate chain

☑ Include private key

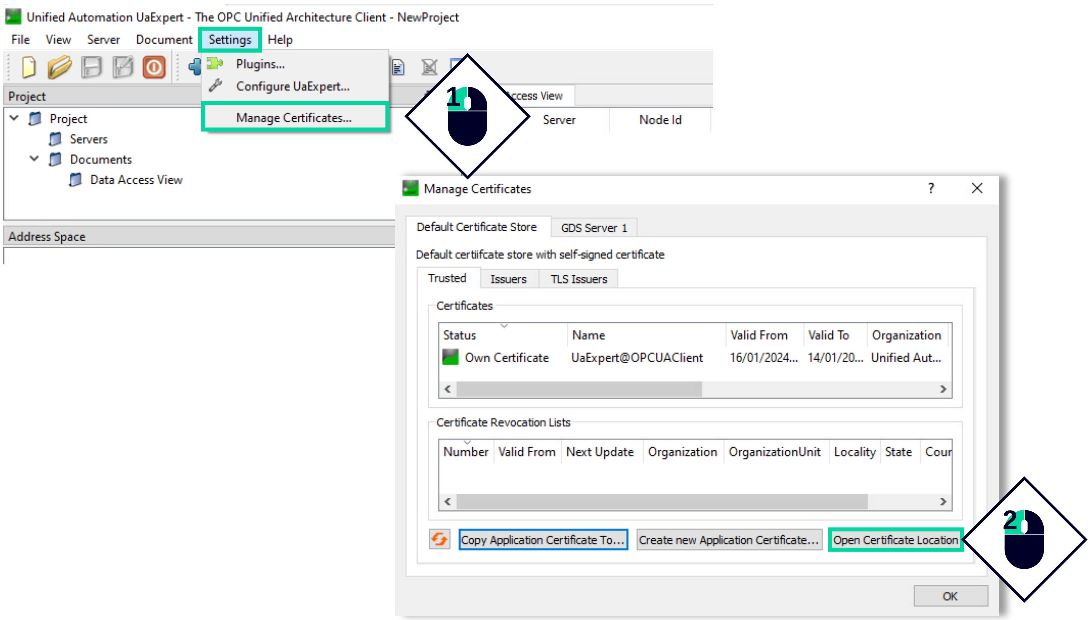
Encryption for private key: None

Enter a password for the private key. If you do not enter a password, the project name will be used as the password.

Password: ********** Very weak

Confirm password: **********

5. Navigate to the "Settings" tab in UaExpert and select "Manage certificates…". A pop-up window appears, presenting UaExpert's self-signed certificate, along with trusted certificates, trusted issuers/CAs, and more.



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject

Manage Certificates

Default Certificate Store | GDS Server 1

Default certifcate store with self-signed certificate

Trusted | Issuers | TLS Issuers

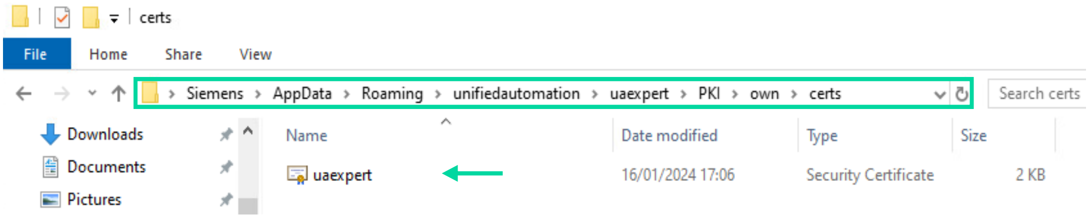
Certificates

Status	Name	Valid From	Valid To	Organization
Own Certificate	UaExpert@OPCUAClient	16/01/2024...	14/01/20...	Unified Aut...

Certificate Revocation Lists

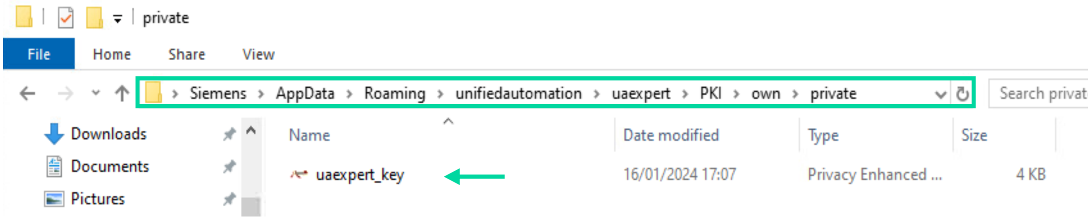
Number	Valid From	Next Update	Organization	OrganizationUnit	Locality	State	Cour

6. Navigate to the “own > certs” folder and copy the newly created certificate. Repeat the process with the private key in the folder “own > private”.



Siemens > AppData > Roaming > unifiedautomation > uaexpert > PKI > own > certs

Name	Date modified	Type	Size
uaexpert	16/01/2024 17:06	Security Certificate	2 KB



Siemens > AppData > Roaming > unifiedautomation > uaexpert > PKI > own > private

Name	Date modified	Type	Size
uaexpert_key	16/01/2024 17:07	Privacy Enhanced ...	4 KB

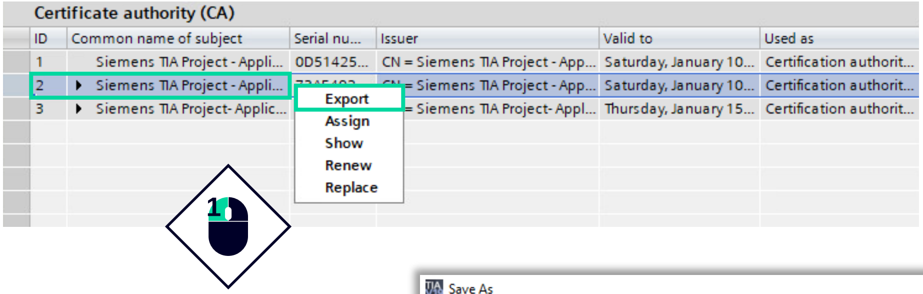
NOTE

Private keys must always remain secret. They should only be exported if necessary and protected with a password.

Import the CA to UaExpert

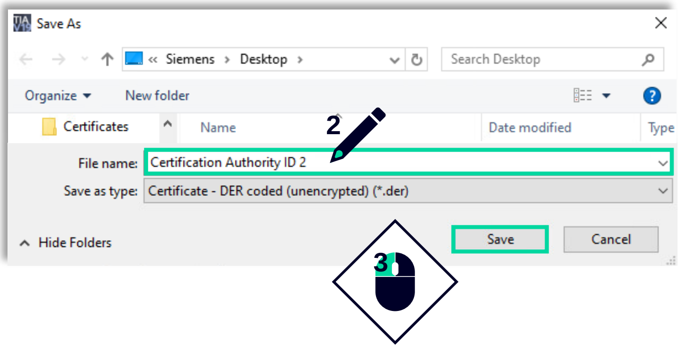
Finally, to establish a trust relationship with the CA, and all certificates issued by it, import the root certificate into UaExpert as a trusted partner.

1. Open the global certificate manager. Export the Certification Authority with ID=2 as a .der file. Do not include the private key in the export.



Certificate authority (CA)

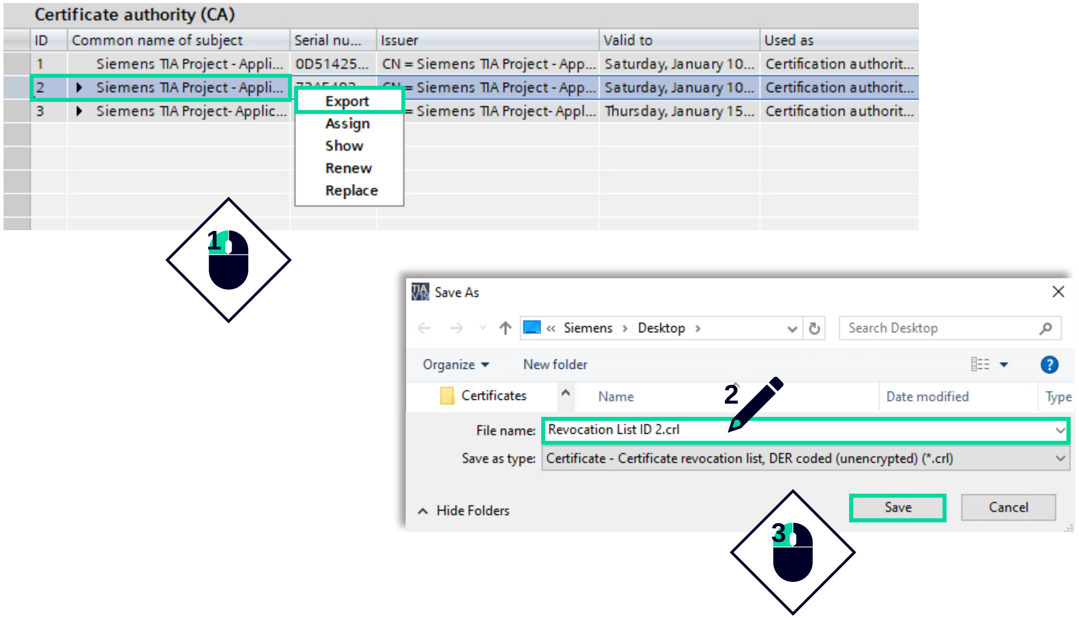
ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
2	Siemens TIA Project - Appli...	[illegible]	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
3	Siemens TIA Project- Applic...		= Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...



File name: Certification Authority ID 2

Save as type: Certificate - DER coded (unencrypted) (*.der)

2. Export the revocation list of the CA.



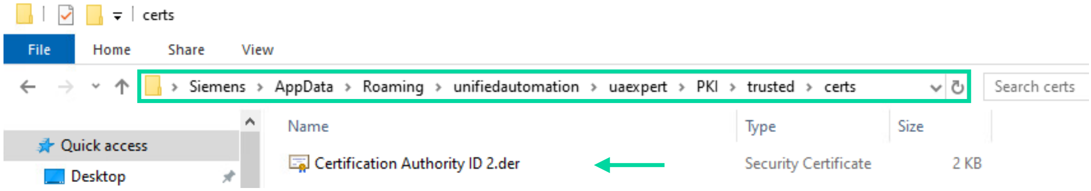
Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
2	Siemens TIA Project - Appli...	[illegible]	= Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...
3	Siemens TIA Project- Applic...		= Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...

File name: Revocation List ID 2.crl

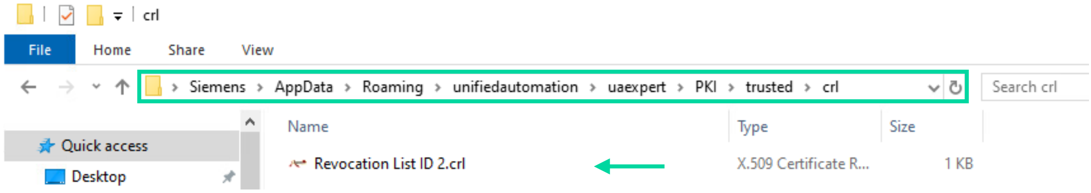
Save as type: Certificate - Certificate revocation list, DER coded (unencrypted) (*.crl)

3. Navigate to the “trusted > certs” folder and copy the root certificate. Repeat the process with the revocation list in the folder “trusted > crl”.



› Siemens › AppData › Roaming › unifiedautomation › uaexpert › PKI › trusted › certs

Name	Type	Size
Certification Authority ID 2.der	Security Certificate	2 KB



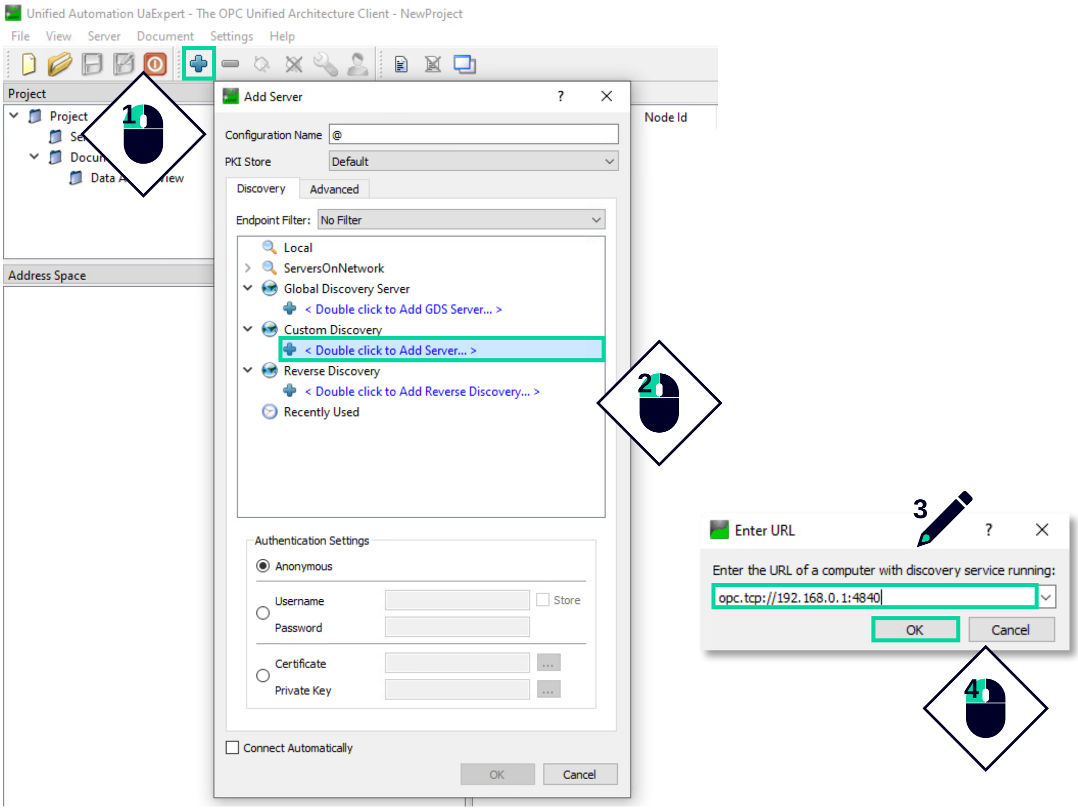
› Siemens › AppData › Roaming › unifiedautomation › uaexpert › PKI › trusted › crl

Name	Type	Size
Revocation List ID 2.crl	X.509 Certificate R...	1 KB

2.4.5 Testing a secure OPC UA connection

After configuring the OPC UA server and client, follow these steps to establish a connection between UaExpert and the CPU.

1. Click the "Add Server" button and then double-click on "<Double click to Add Server…>". A dialog will appear to input the OPC UA server's URL running on the CPU.



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject

Add Server

Configuration Name: @

PKI Store: Default

Endpoint Filter: No Filter

- Local
- ServersOnNetwork
- Global Discovery Server
  - < Double click to Add GDS Server... >
- Custom Discovery
  - < Double click to Add Server... >
- Reverse Discovery
  - < Double click to Add Reverse Discovery... >
- Recently Used

Authentication Settings

● Anonymous

○ Username / Password □ Store

○ Certificate / Private Key

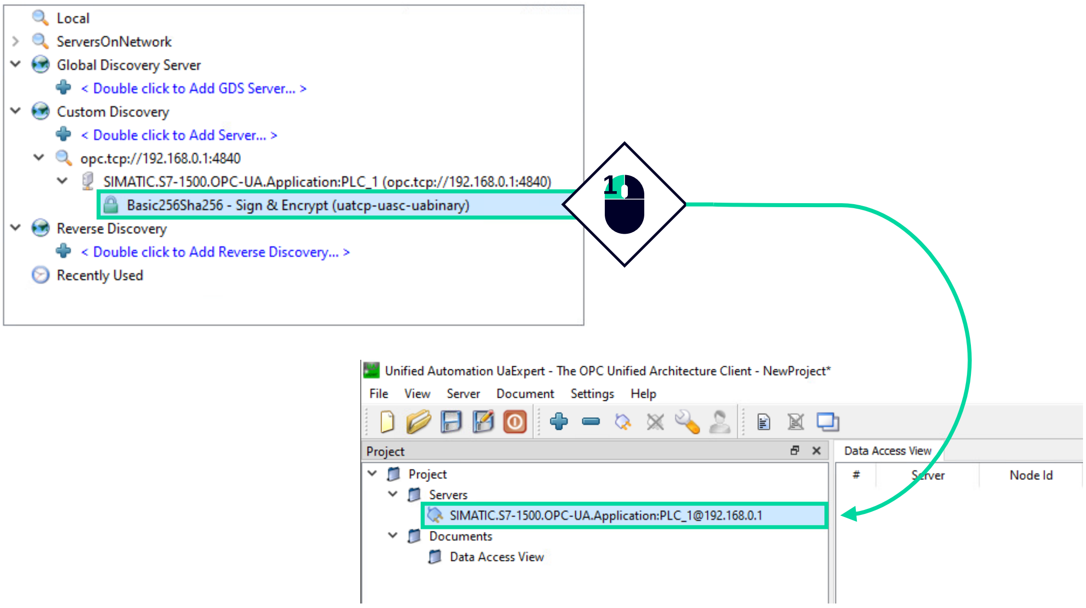
□ Connect Automatically

Enter URL

Enter the URL of a computer with discovery service running:

opc.tcp://192.168.0.1:4840

2. The server endpoints will be displayed under the “Custom Discovery” section. Double-click on the endpoint with the security modes and policies configured earlier. This will add the server to the project.

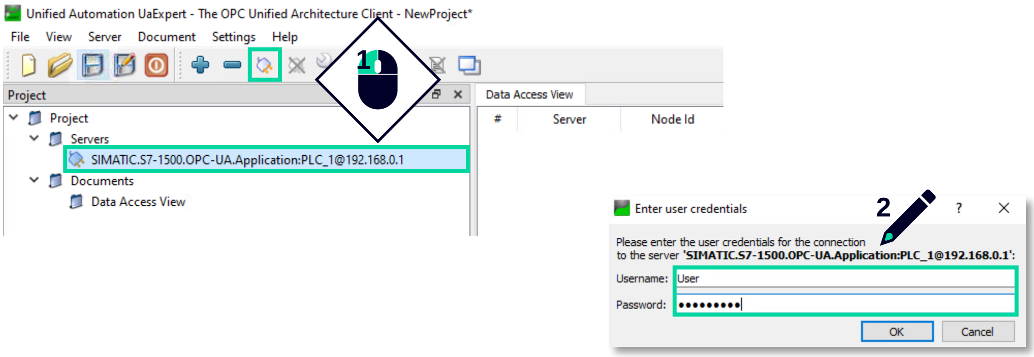


- Local
- ServersOnNetwork
- Global Discovery Server
  - < Double click to Add GDS Server... >
- Custom Discovery
  - < Double click to Add Server... >
  - opc.tcp://192.168.0.1:4840
    - SIMATIC.S7-1500.OPC-UA.Application:PLC_1 (opc.tcp://192.168.0.1:4840)
      - Basic256Sha256 - Sign & Encrypt (uatcp-uasc-uabinary)
- Reverse Discovery
  - < Double click to Add Reverse Discovery... >
- Recently Used

Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*

- Project
  - Servers
    - SIMATIC.S7-1500.OPC-UA.Application:PLC_1@192.168.0.1
  - Documents
    - Data Access View

3. Select the OPC UA server and click on the “Connect server” button. Insert the username and password to perform the user authentication.



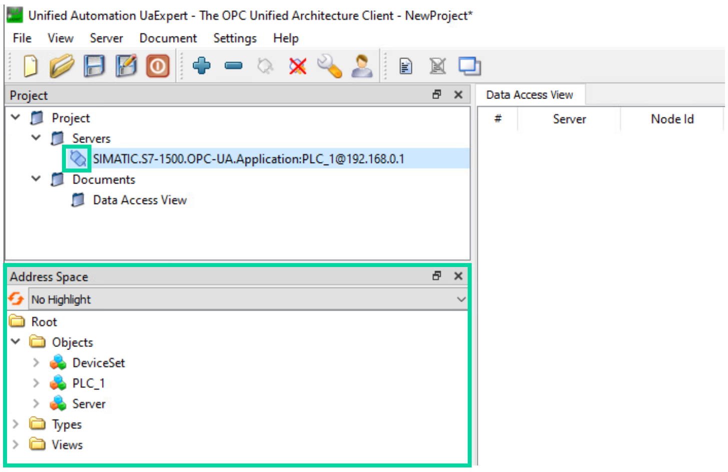
Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*
File View Server Document Settings Help
Project
Project
Servers
SIMATIC.S7-1500.OPC-UA.Application:PLC_1@192.168.0.1
Documents
Data Access View
Data Access View
#
Server
Node Id
1
2
Enter user credentials
?
OK
Cancel

Please enter the user credentials for the connection to the server 'SIMATIC.S7-1500.OPC-UA.Application:PLC_1@192.168.0.1':

Username: User

Password: •••••••••

As a result, the OPC UA client establishes a connection with the server, enabling secure access to the information stored within its AddressSpace.



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*
File View Server Document Settings Help
Project
Project
Servers
SIMATIC.S7-1500.OPC-UA.Application:PLC_1@192.168.0.1
Documents
Data Access View
Data Access View
#
Server
Node Id
Address Space
No Highlight
Root
Objects
DeviceSet
PLC_1
Server
Types
Views

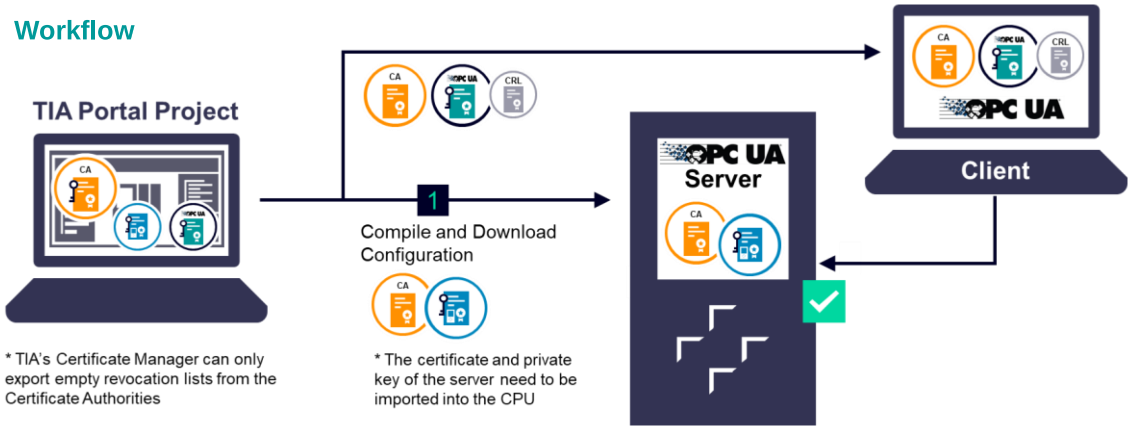
2.4.6 OPC UA certificate handling scenarios–where does each certificate belong?

Description

This chapter concludes with a set of diagrams designed to highlight the correct handling of certificates and private keys in diverse OPC UA communication scenarios. These illustrations should be used as a guide to understand when and where certificates, private keys, and revocation lists should be exported.

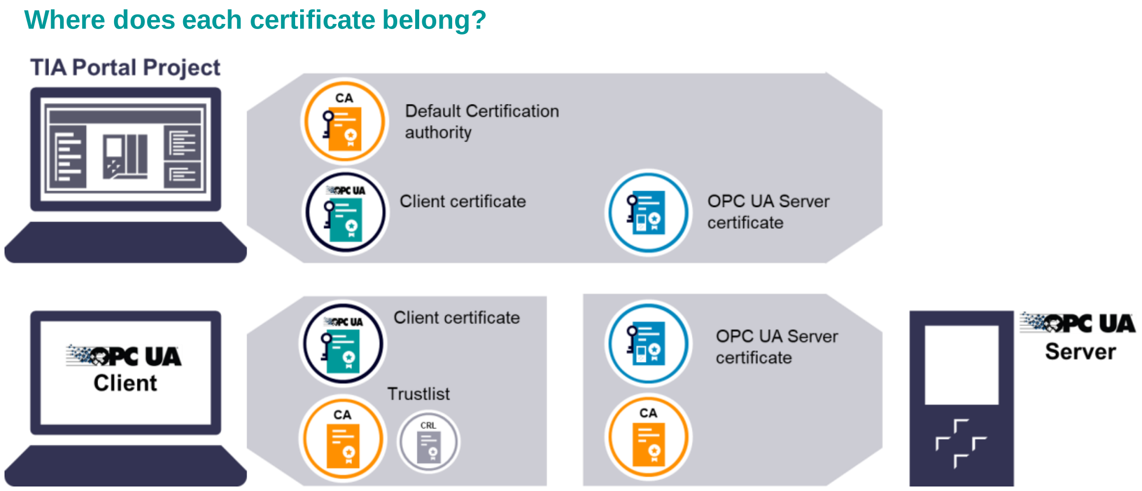
Scenario 1

Using the default Certification Authorities in the global certificate manager to issue certificates for servers (CPU) and clients (external application).



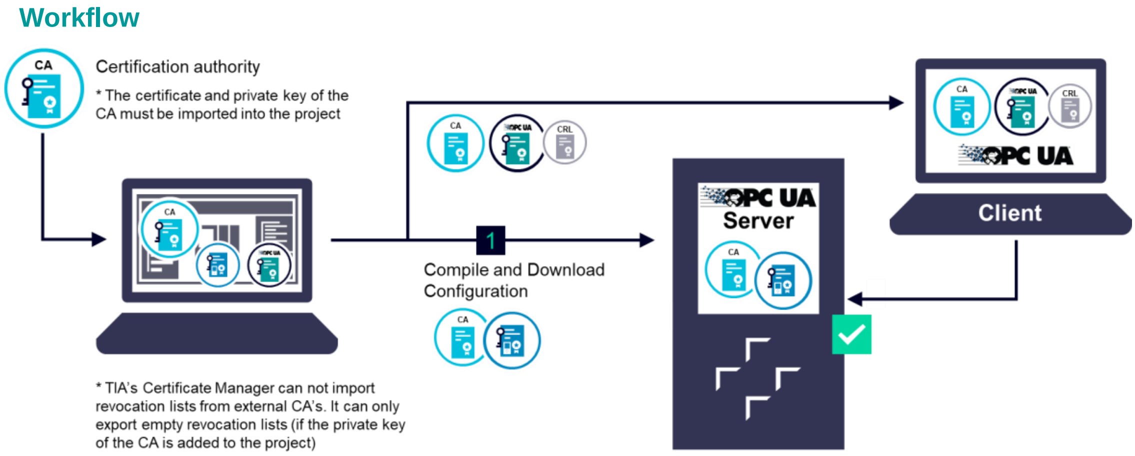
* TIA's Certificate Manager can only export empty revocation lists from the Certificate Authorities

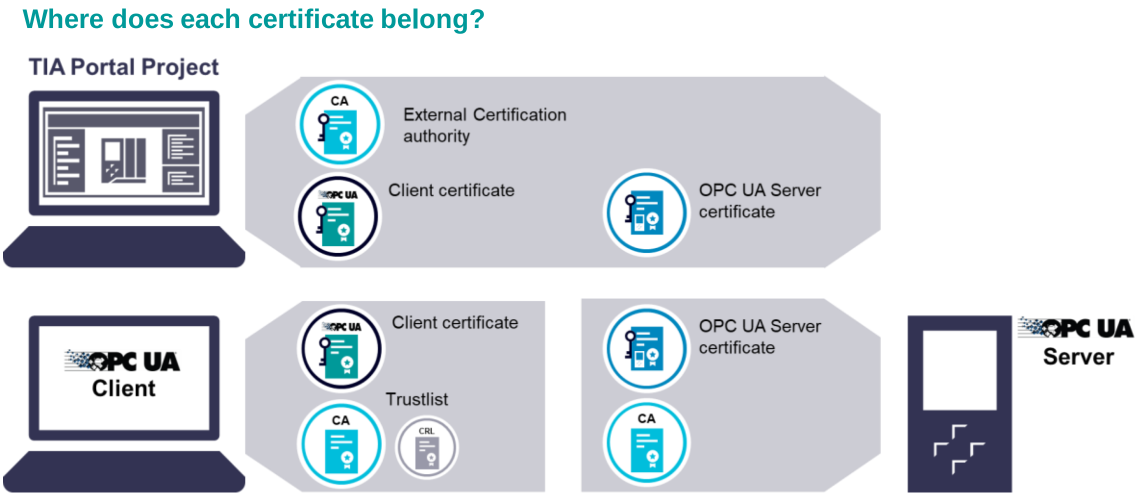
* The certificate and private key of the server need to be imported into the CPU


Where does each certificate belong?
TIA Portal Project
CA
Default Certification authority
Client certificate
OPC UA Server certificate
OPC UA Client
Client certificate
Trustlist
CRL
OPC UA Server certificate
OPC UA Server

Scenario 2

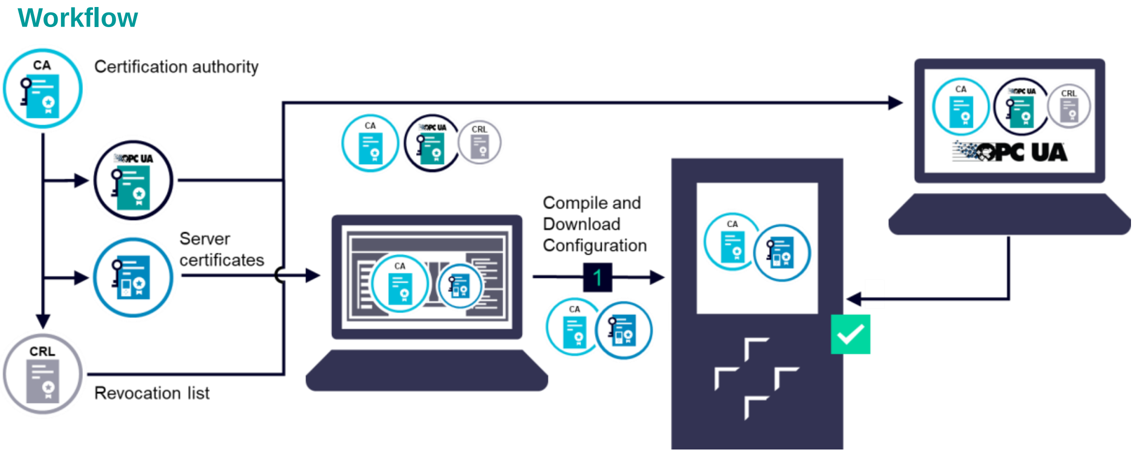
Using an external Certificate Authority managed within TIA Portal’s Certificate Manager.

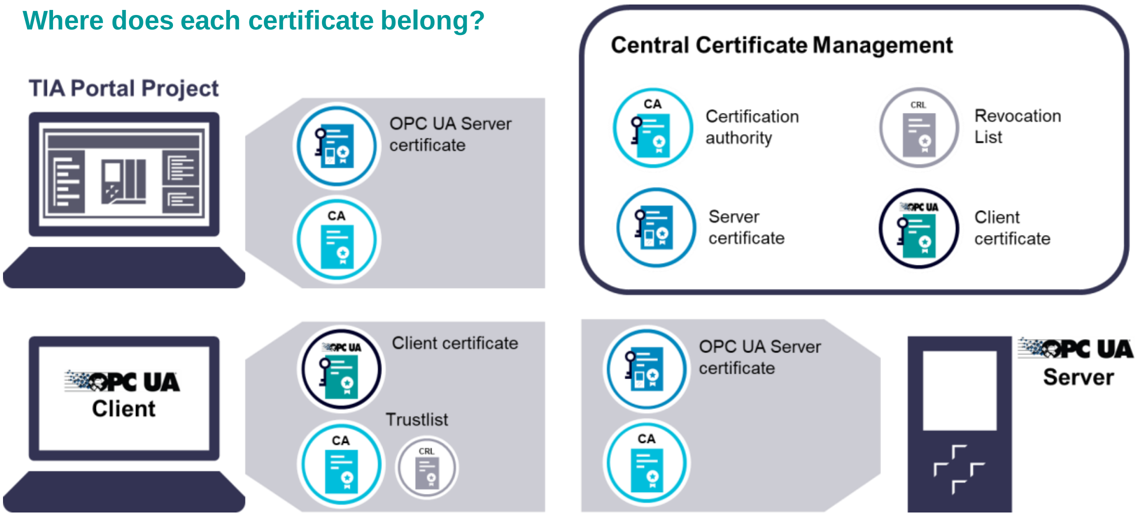

Workflow
CA
Certification authority
* The certificate and private key of the CA must be imported into the project
CA
OPC UA
CRL
1
Compile and Download Configuration
CA
OPC UA Server
CA
OPC UA
Client
* TIA’s Certificate Manager can not import revocation lists from external CA’s. It can only export empty revocation lists (if the private key of the CA is added to the project)


Where does each certificate belong?
TIA Portal Project
CA
External Certification authority
OPC UA
Client certificate
OPC UA Server certificate
OPC UA Client
OPC UA
Client certificate
Trustlist
CA
CRL
OPC UA Server certificate
CA
OPC UA Server

Scenario 3

Using a central certificate manager to issue and manage certificates for clients and servers. The Certificate Authority can belong to the user/company or to a third-party corporation such as DigiCert or RapidSSL among many others.





2.5 Certificates in the scope of HTTPS web server communication

2.5.1 Overview on HTTPS communication

Description

The foundation of HTTPS security lies in the TLS protocol, requiring the presence of certificates on those devices running web servers. To prevent unsecure connections with web servers, CPUs must be configured to exclusively allow access through HTTPS.

In contrast to OPC UA, which mandates mutual authentication and trust, HTTPS places the trust burden solely on the client, which must verify the validity of the web server's certificate.

NOTE

> Self-signed certificates lack trustworthiness in web browsers. This is because web browsers operate on a trust model that relies on Certificate Authorities. Therefore, web server certificates must be issued by recognized CAs whose certificates are trusted within the web browser settings.

HTTPS certificates

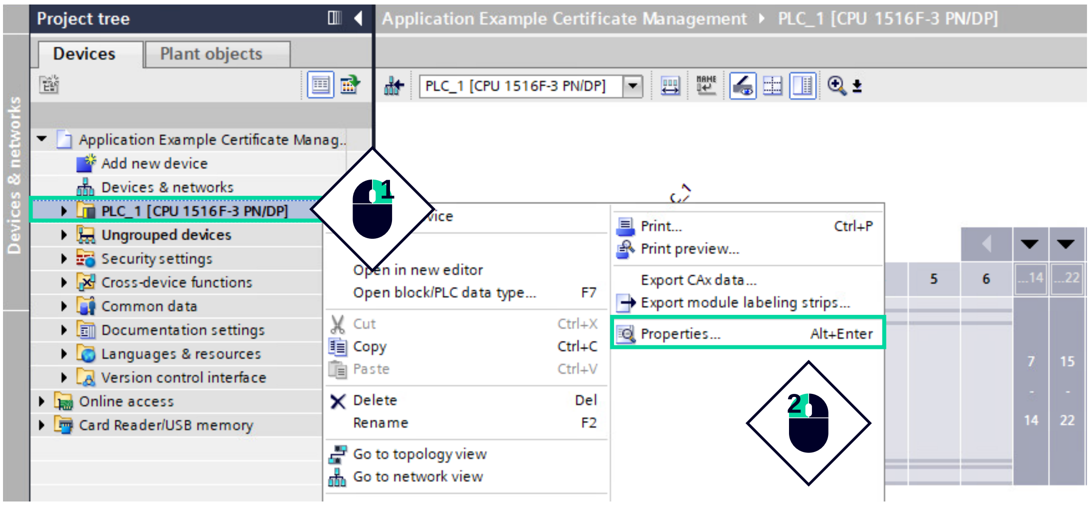
In the context of web servers, X-509 version 3 certificates are commonly used to secure communication over HTTPS. These certificates are issued by Certificate Authorities and provide the trusted means to establish the identity of the server to the client, using asymmetric cryptography before transitioning to symmetric encryption.

2.5.2 Setting up the web server

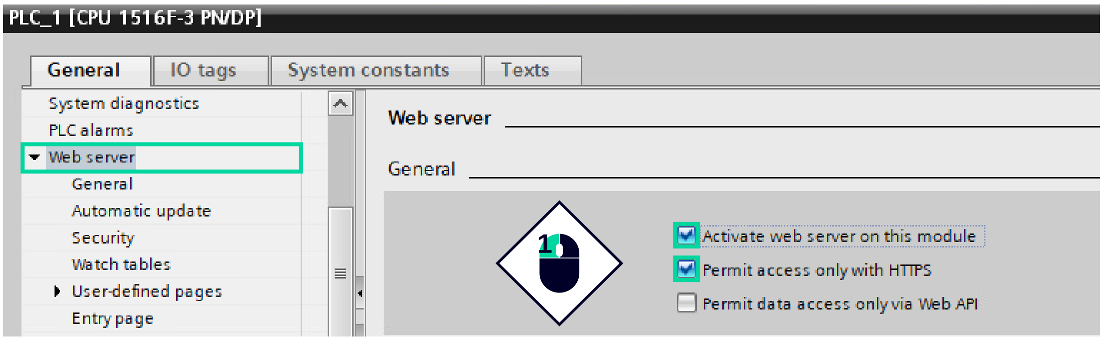
Commissioning of the web server

To configure the web server using HTTPS, the next steps must be followed:

1. Select the CPU in the project tree and navigate to the “Properties” tab.



2. In the navigation area 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". Confirm the security message.



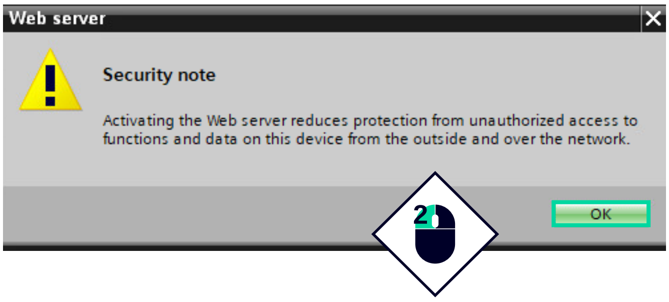
Web server

General

☑ Activate web server on this module

☑ Permit access only with HTTPS

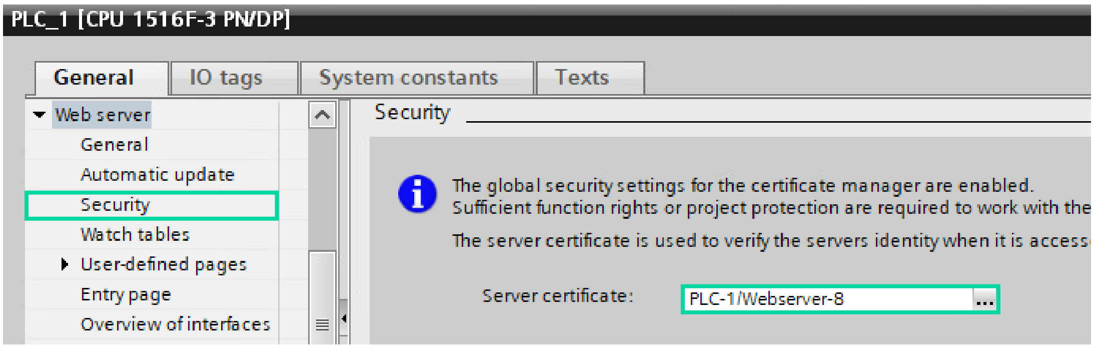
☐ Permit data access only via Web API



Security note

Activating the Web server reduces protection from unauthorized access to functions and data on this device from the outside and over the network.

3. By default, a server certificate is automatically generated in the local certificate manager of the device. As can be seen here, the certificate is issued by a new Certification Authority with ID=3.



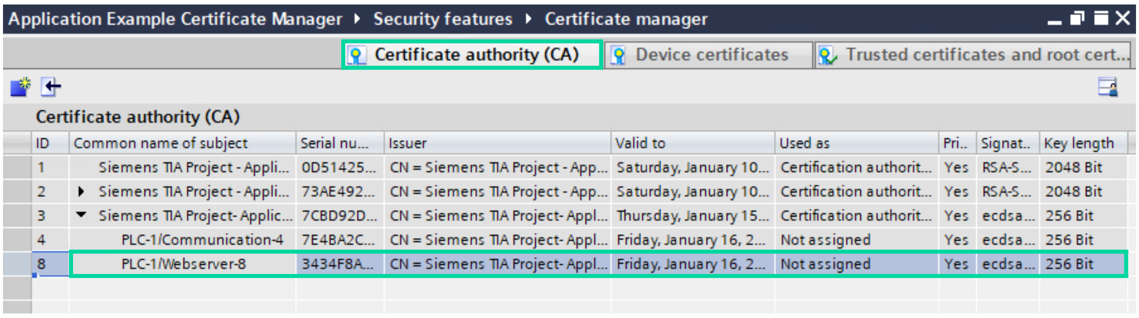
Security

The global security settings for the certificate manager are enabled.
Sufficient function rights or project protection are required to work with the

The server certificate is used to verify the servers identity when it is access

Server certificate: PLC-1/Webserver-8

The web server’s certificate can be found in the global certificate manager, under the “Certificate authority (CA)” and "Device certificates" tabs. In this case, the root certificate with ID=3 has issued the web server certificate as well as the secure PG-HMI communication.


Application Example Certificate Manager ▸ Security features ▸ Certificate manager
Certificate authority (CA)
Device certificates
Trusted certificates and root cert...

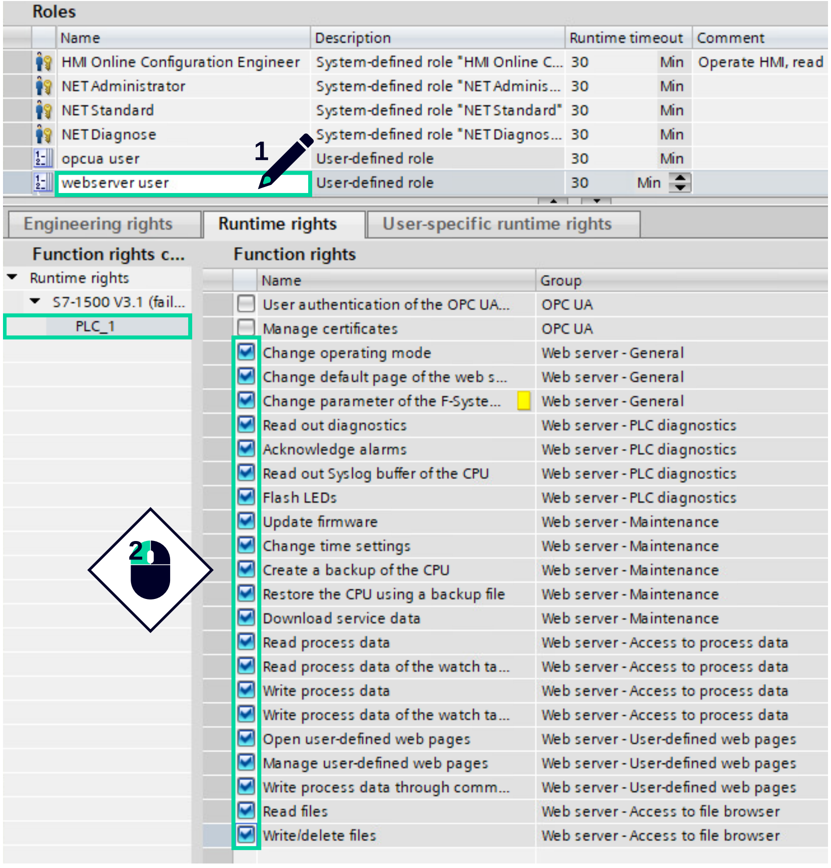
Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signat..	Key length
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
2	▸ Siemens TIA Project - Appli...	73AE492...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
3	▾ Siemens TIA Project- Applic...	7CBD92D...	CN = Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...	Yes	ecdsa...	256 Bit
4	PLC-1/Communication-4	7E4BA2C...	CN = Siemens TIA Project- Appl...	Friday, January 16, 2...	Not assigned	Yes	ecdsa...	256 Bit
8	PLC-1/Webserver-8	3434F8A...	CN = Siemens TIA Project- Appl...	Friday, January 16, 2...	Not assigned	Yes	ecdsa...	256 Bit

User authentication

Like OPC UA, web server access can be controlled through user authentication. To create a new user with "Web server" access rights:

1. Double click on “Security settings > Users and roles” and navigate to the “Roles” tab. Click on “<Add new role>”. From the “Runtime rights” of the target CPU, assign those web server rights strictly required by the user.



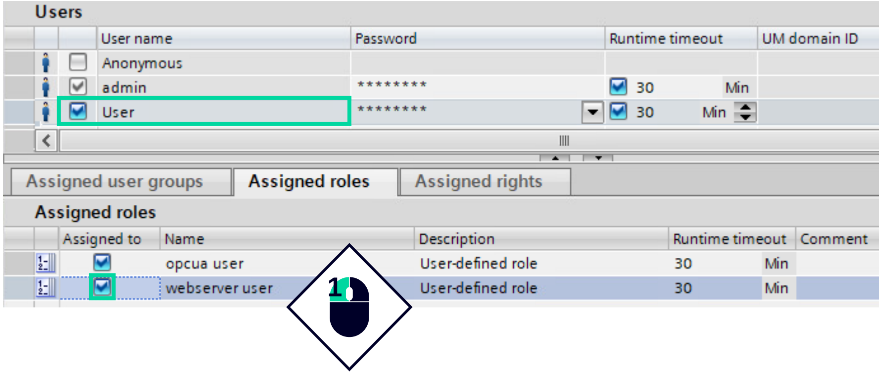
Roles

Name	Description	Runtime timeout		Comment
HMI Online Configuration Engineer	System-defined role "HMI Online C...	30	Min	Operate HMI, read
NET Administrator	System-defined role "NET Adminis...	30	Min	
NET Standard	System-defined role "NET Standard"	30	Min	
NET Diagnose	System-defined role "NET Diagnos...	30	Min	
opcua user	User-defined role	30	Min	
webserver user	User-defined role	30	Min	

Function rights

	Name	Group
□	User authentication of the OPC UA...	OPC UA
□	Manage certificates	OPC UA
☑	Change operating mode	Web server - General
☑	Change default page of the web s...	Web server - General
☑	Change parameter of the F-Syste...	Web server - General
☑	Read out diagnostics	Web server - PLC diagnostics
☑	Acknowledge alarms	Web server - PLC diagnostics
☑	Read out Syslog buffer of the CPU	Web server - PLC diagnostics
☑	Flash LEDs	Web server - PLC diagnostics
☑	Update firmware	Web server - Maintenance
☑	Change time settings	Web server - Maintenance
☑	Create a backup of the CPU	Web server - Maintenance
☑	Restore the CPU using a backup file	Web server - Maintenance
☑	Download service data	Web server - Maintenance
☑	Read process data	Web server - Access to process data
☑	Read process data of the watch ta...	Web server - Access to process data
☑	Write process data	Web server - Access to process data
☑	Write process data of the watch ta...	Web server - Access to process data
☑	Open user-defined web pages	Web server - User-defined web pages
☑	Manage user-defined web pages	Web server - User-defined web pages
☑	Write process data through comm...	Web server - User-defined web pages
☑	Read files	Web server - Access to file browser
☑	Write/delete files	Web server - Access to file browser

2. Assign the new role to a user. Compile and download the project to the CPU.



Users

	User name	Password	Runtime timeout		UM domain ID
□	Anonymous				
☑	admin	********	☑ 30	Min	
☑	User	********	☑ 30	Min	

Assigned roles

Assigned to	Name	Description	Runtime timeout		Comment
☑	opcua user	User-defined role	30	Min	
☑	webserver user	User-defined role	30	Min	

2.5.3 Setting up the web browser

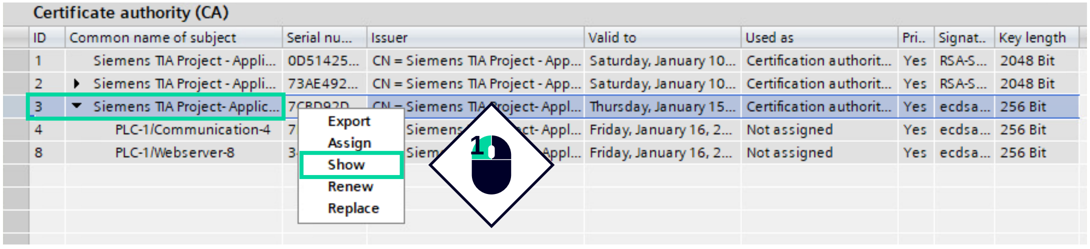
Description

In this Application Example, Microsoft Edge has been selected as the browser to establish the connection with the web server.

Configuration

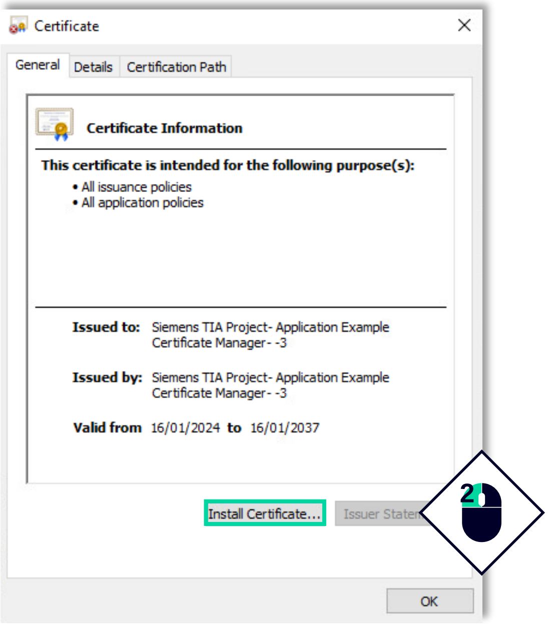
For Microsoft Edge to trust the web server's certificate, it needs to establish a trust relationship with the CA. For this, it is necessary to export the root certificate from TIA Portal and import it into Windows' certificate store.

1. To export the root certificate from the global certificate manager, right-click on the CA and select the "Show" option. Once the certificate is opened, click on "Install Certificate…".



Certificate authority (CA)

ID	Common name of subject	Serial nu...	Issuer	Valid to	Used as	Pri..	Signat..	Key length
1	Siemens TIA Project - Appli...	0D51425...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
2	Siemens TIA Project - Appli...	73AE492...	CN = Siemens TIA Project - App...	Saturday, January 10...	Certification authorit...	Yes	RSA-S...	2048 Bit
3	Siemens TIA Project- Applic...	7CBD92D...	CN = Siemens TIA Project- Appl...	Thursday, January 15...	Certification authorit...	Yes	ecdsa...	256 Bit
4	PLC-1/Communication-4	7	Siemens ct- Appl...	Friday, January 16, 2...	Not assigned	Yes	ecdsa...	256 Bit
8	PLC-1/Webserver-8	3	Siem Appl...	Friday, January 16, 2...	Not assigned	Yes	ecdsa...	256 Bit



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

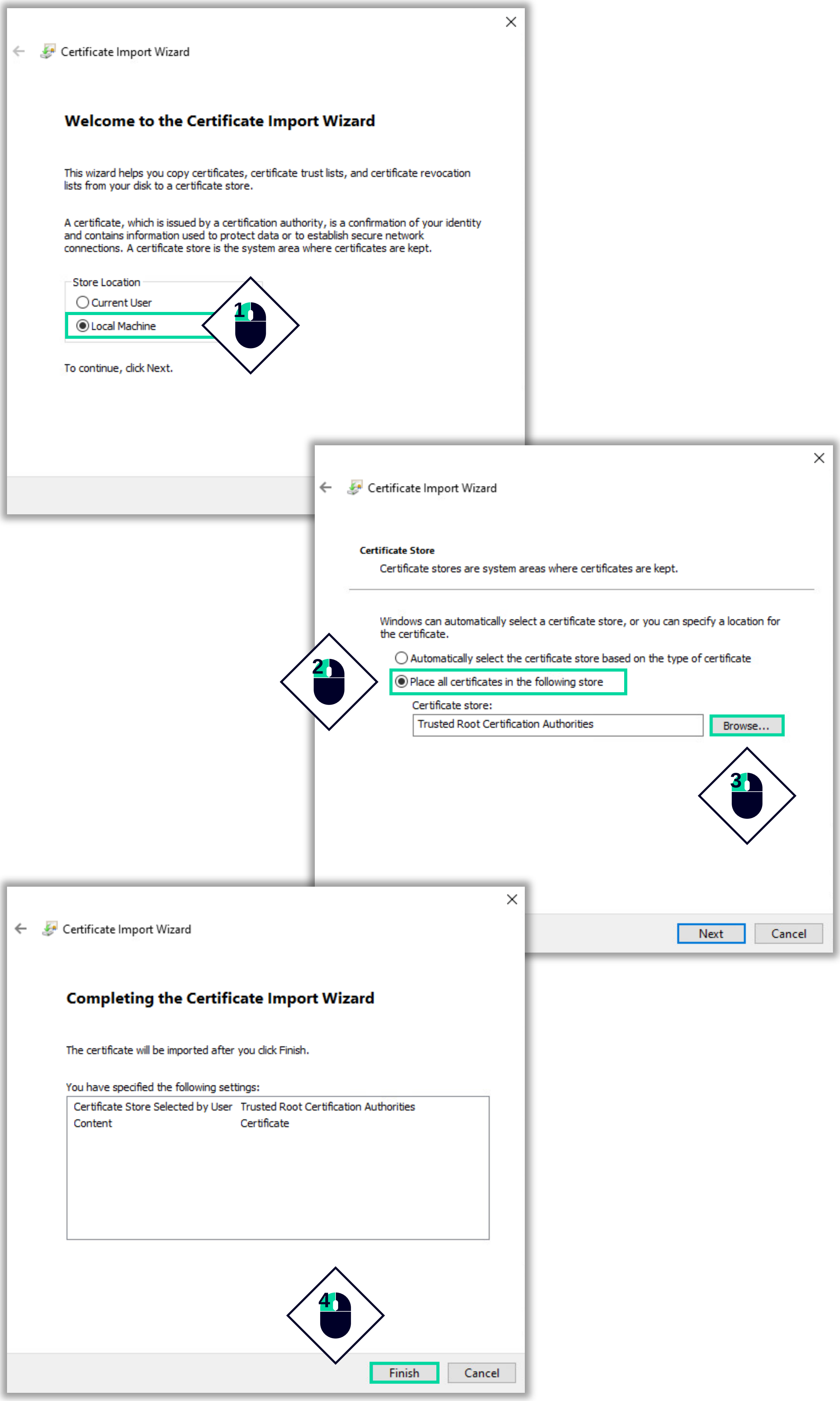
Issued to: Siemens TIA Project- Application Example Certificate Manager- -3

Issued by: Siemens TIA Project- Application Example Certificate Manager- -3

Valid from 16/01/2024 **to** 16/01/2037

2. The wizard is started. Follow the instructions of the installation wizard.
   - Select the "Local Machine" as the storage location.
   - The wizard issues a security warning, which must be acknowledged with "Yes".
   - Store the certificate in the "Trusted Root Certification Authorities" folder.

   The "Finish" button imports the certificate into the selected folder.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

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

Store Location

○ Current User

● Local Machine

To continue, click Next.

Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

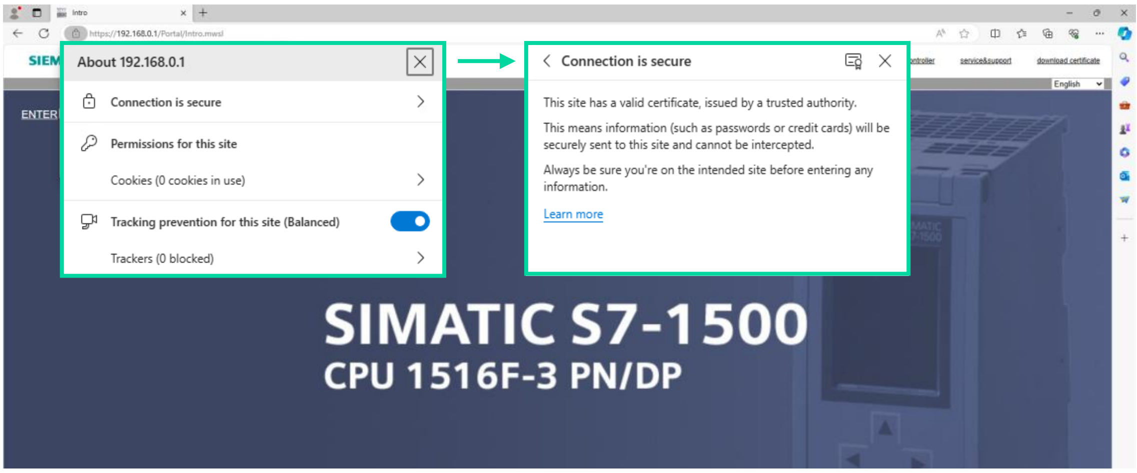
You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

2.5.4 Testing a secure HTTPS connection

With the CPU running and the root certificate imported into Windows' certificate store, establish a connection to the web server using the following URL: https://[CPU IP Address].

As shown in the image below, the connection is secured by TLS, and the web server's certificate is considered trustworthy.



About 192.168.0.1

Connection is secure

Permissions for this site

Cookies (0 cookies in use)

Tracking prevention for this site (Balanced)

Trackers (0 blocked)

Connection is secure

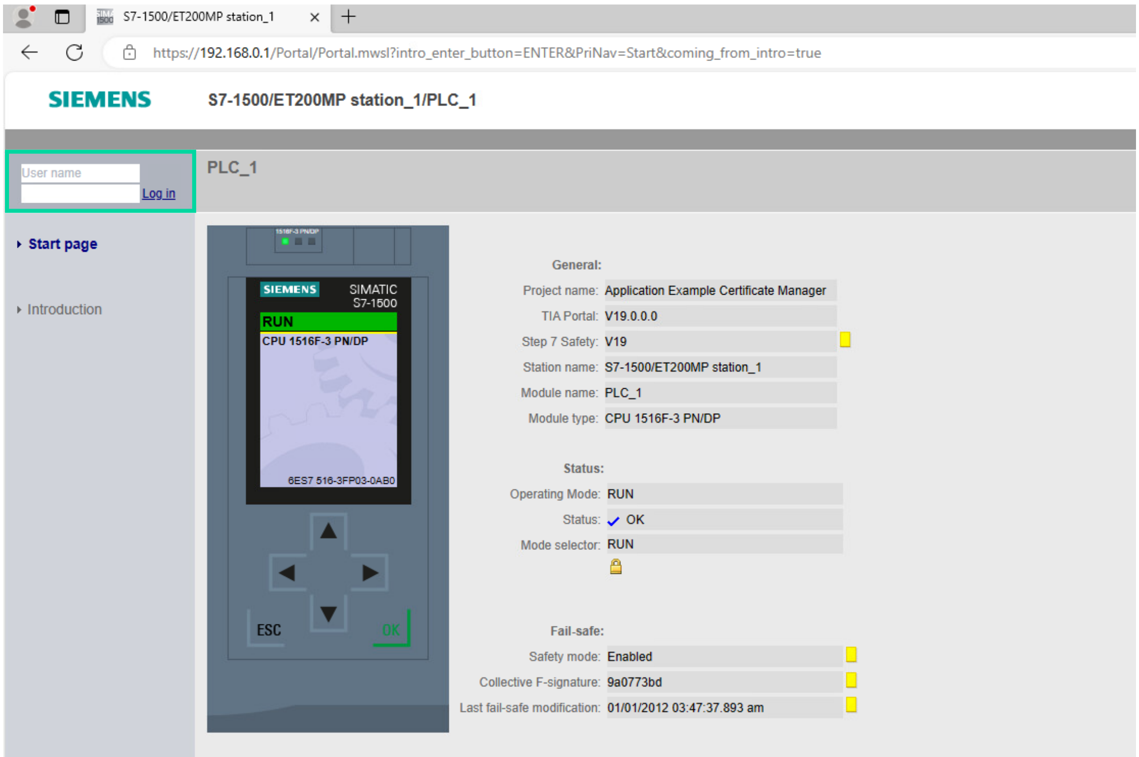
This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Learn more

To test the user authentication, press the "ENTER" button. As observed, anonymous users have limited access to the information displayed on the web server.



https://192.168.0.1/Portal/Portal.mwsl?intro_enter_button=ENTER&PriNav=Start&coming_from_intro=true

S7-1500/ET200MP station_1/PLC_1

PLC_1

General:

Project name:	Application Example Certificate Manager
TIA Portal:	V19.0.0.0
Step 7 Safety:	V19
Station name:	S7-1500/ET200MP station_1
Module name:	PLC_1
Module type:	CPU 1516F-3 PN/DP

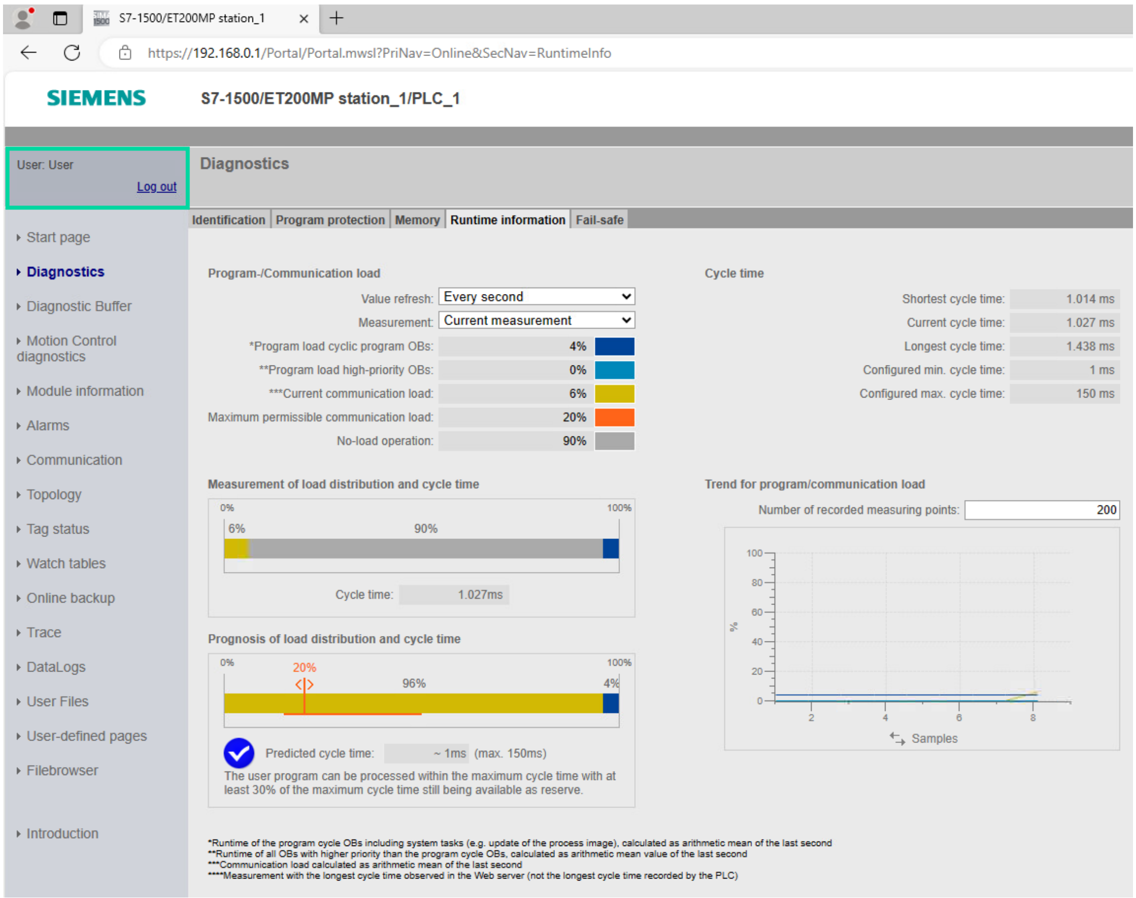
Status:

Operating Mode:	RUN
Status:	✓ OK
Mode selector:	RUN

Fail-safe:

Safety mode:	Enabled
Collective F-signature:	9a0773bd
Last fail-safe modification:	01/01/2012 03:47:37.893 am

After logging in with username and password, the web server checks the user’s rights and grants it access to further features.



Program-/Communication load

Value refresh:	Every second
Measurement:	Current measurement
*Program load cyclic program OBs:	4%
**Program load high-priority OBs:	0%
***Current communication load:	6%
Maximum permissible communication load:	20%
No-load operation:	90%

Cycle time

Shortest cycle time:	1.014 ms
Current cycle time:	1.027 ms
Longest cycle time:	1.438 ms
Configured min. cycle time:	1 ms
Configured max. cycle time:	150 ms

Measurement of load distribution and cycle time

Cycle time: 1.027ms

Trend for program/communication load

Number of recorded measuring points: 200

Prognosis of load distribution and cycle time

Predicted cycle time: ~ 1ms (max. 150ms)

The user program can be processed within the maximum cycle time with at least 30% of the maximum cycle time still being available as reserve.

*Runtime of the program cycle OBs including system tasks (e.g. update of the process image), calculated as arithmetic mean of the last second
**Runtime of all OBs with higher priority than the program cycle OBs, calculated as arithmetic mean value of the last second
***Communication load calculated as arithmetic mean of the last second
****Measurement with the longest cycle time observed in the Web server (not the longest cycle time recorded by the PLC)

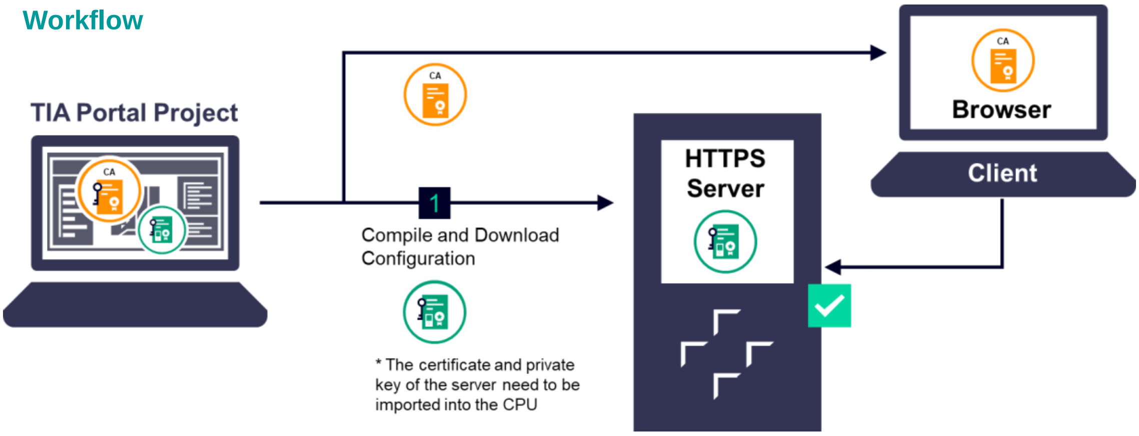
2.5.5 HTTPS certificate handling scenarios–where does each certificate belong?

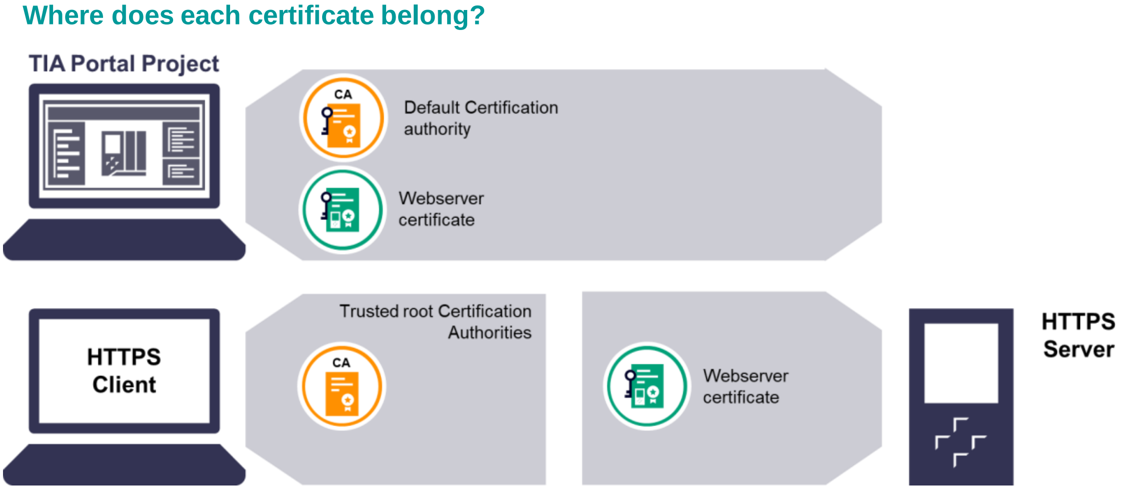
Description

The chapter concludes with a set of diagrams designed to highlight the correct handling of certificates and private keys in diverse HTTPS communication scenarios. These diagrams do not include any client certificates in the web browser, as HTTPS does not often require them for client authentication.

Scenario 1

Using TIA Portal’s default CAs in the Certificate Manager to issue certificates for web servers.

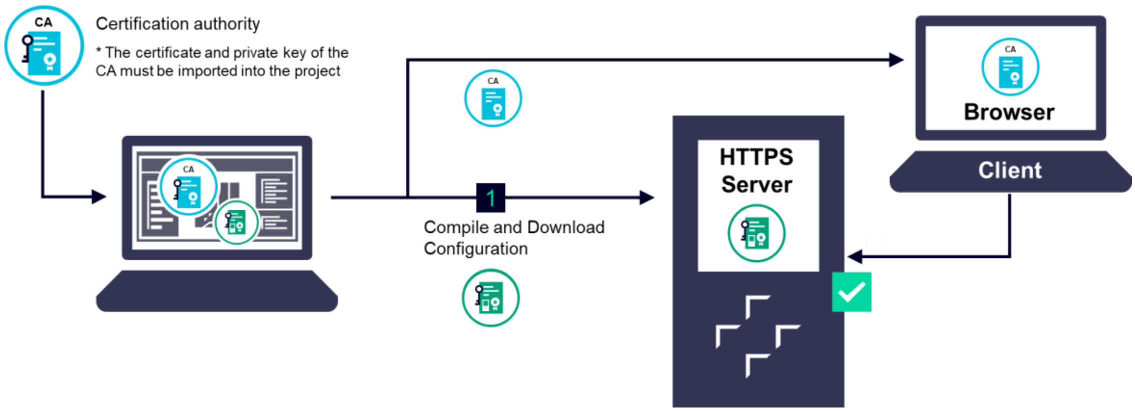

Workflow
TIA Portal Project
CA
CA
1
Compile and Download Configuration
* The certificate and private key of the server need to be imported into the CPU
HTTPS Server
CA
Browser
Client


Where does each certificate belong?
TIA Portal Project
CA
Default Certification authority
Webserver certificate
HTTPS Client
Trusted root Certification Authorities
CA
Webserver certificate
HTTPS Server

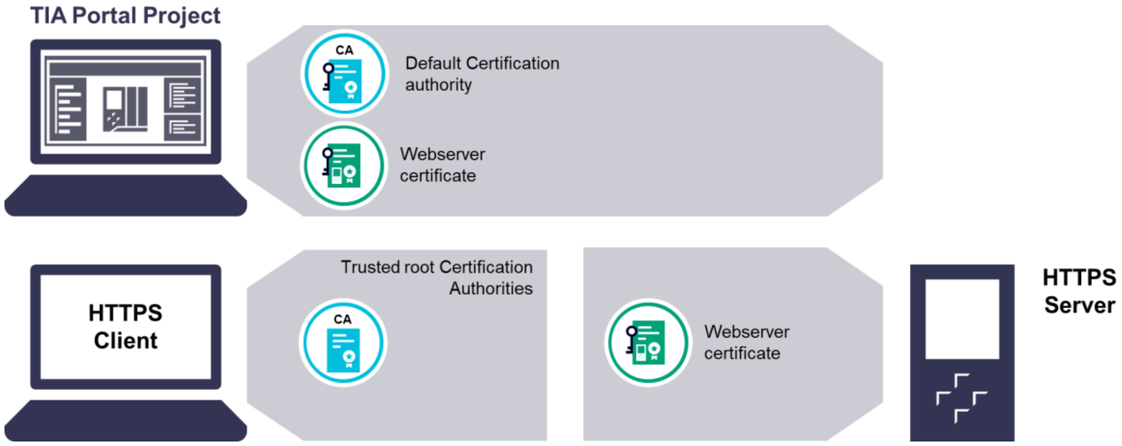
Scenario 2

Using an external Certificate Authority managed within TIA's Certificate Manager.

Workflow

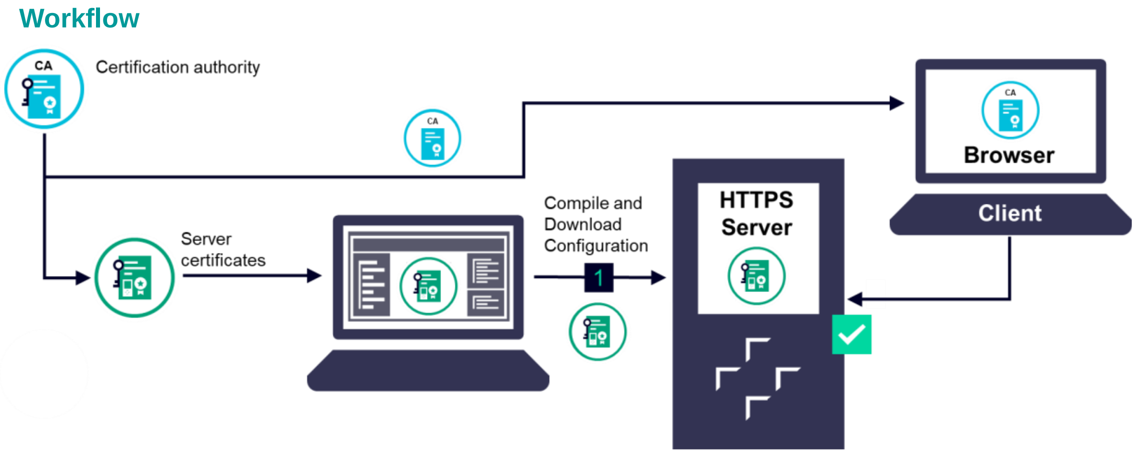

CA
Certification authority
* The certificate and private key of the CA must be imported into the project
CA
CA
1
Compile and Download Configuration
HTTPS Server
CA
Browser
Client

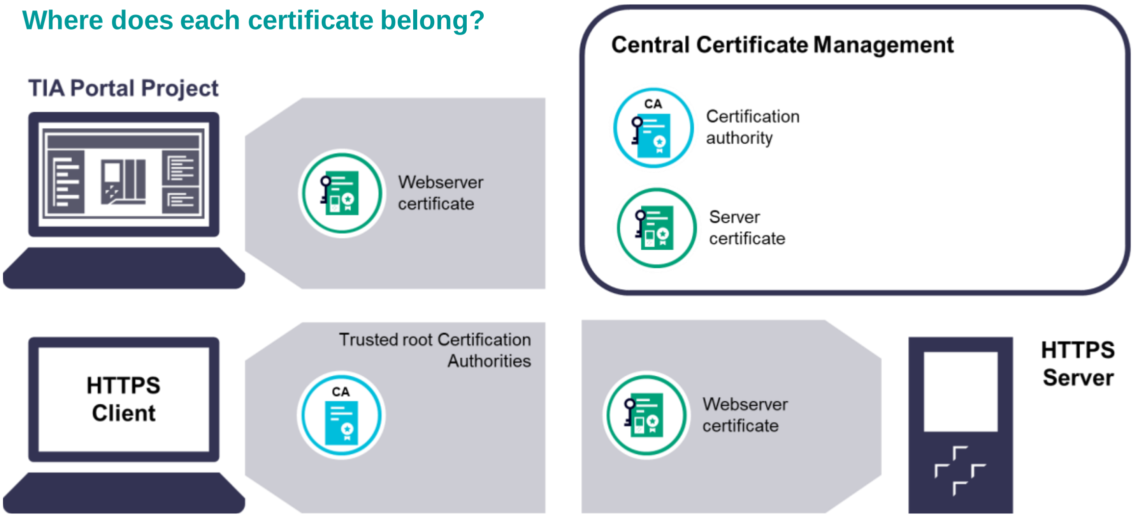
Where does each certificate belong?



Scenario 3

Using a central certificate manager to issue and manage certificates for the web server. The Certificate Authority can belong to the user/company or to a third-party corporation such as DigiCert or RapidSSL among many others.





2.6 Certificates in the scope of Secure OUC communication

2.6.1 Overview on Open User Communication

Description

Open User Communication is an open standard that enables communication between SIMATIC CPUs as well as with suitable third-party devices. It supports various communication protocols, some of which can be secured through TLS v1.2 and v1.3.

Transport protocol	Via interface
TCP	PROFINET/IE
ISO-on-TCP	PROFINET/IE
ISO	Industrial Ethernet (only CP 1543-1)
UDP	PROFINET/IE
FDL	PROFIBUS

Application protocol	Used transport protocol
Modbus TCP	TCP
E-Mail	TCP
FTP	TCP

The application example titled “Basic Examples for Open User Communication (OUC)” provides in-depth details on establishing non-secure OUC, focusing on ISO-on-TCP, TCP and UDP communication protocols. (https://support.industry.siemens.com/cs/document/109747710)

OUC certificates

Secure OUC employs X-509 v3 certificates with key usage and subject alternative names that comply with TLS requirements. In this configuration, one device functions as a server and opens a designated port to establish the TCP connection, while a second device, the TLS client, initiates and establishes the connection with the server through this port.

Like web servers, only the client side is required to trust the server’s certificate. However, users can modify this setting, making it mandatory to establish a mutual trust relationship between server and client.

2.6.2 Setting up the TLS server

Description

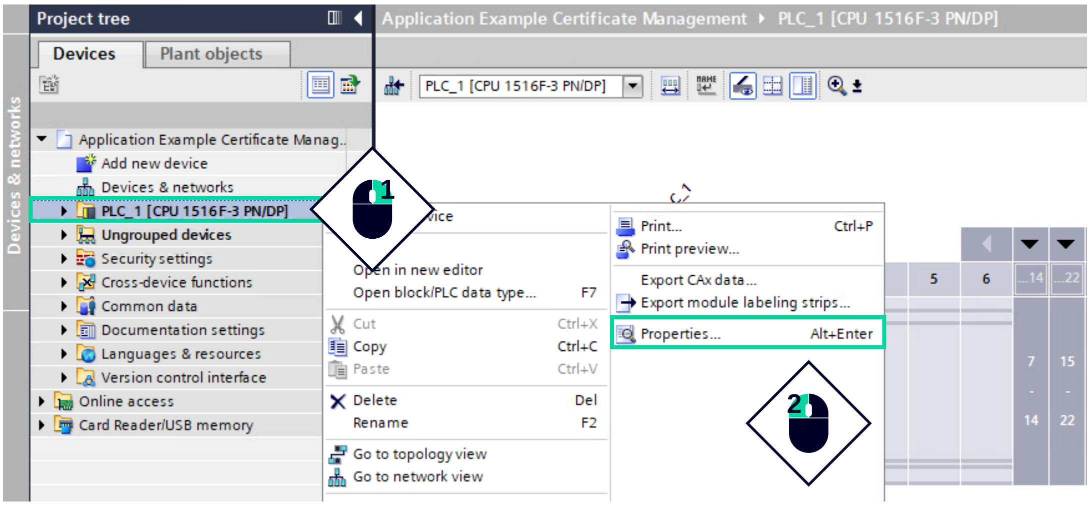
In this application example, the CPU will be used as a TLS server. To communicate with it, a second PLC will be configured as a TLS client.

To implement the Secure Open User Communication, the function blocks "TRCV_C" and "TSEND_C" will be utilized in the Main Organization Block (OB) of both the server and client. These blocks combine the functionalities of TCON (connect), TRCV (receive) / TSEND (send), and TDISCON (disconnect) into a single, integrated block.

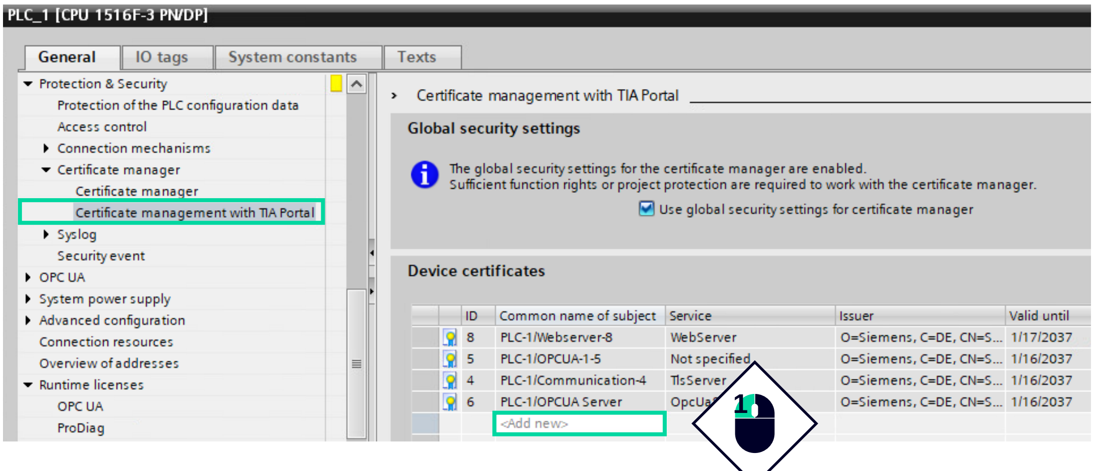
Creation of the server's certificate

To set up a TLS server in the CPU, the first step is to create a new TLS client/server certificate:

1. Select the CPU in the project tree and navigate to the "Properties" tab.



2. Navigate to the entry "Protection & Security > Certificate manager > Certificate management with TIA Portal" and create a new certificate in the "Device certificates" section.



Certificate management with TIA Portal

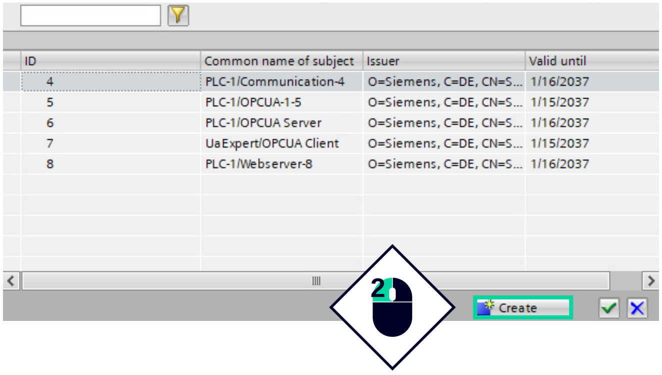
Global security settings

The global security settings for the certificate manager are enabled.
Sufficient function rights or project protection are required to work with the certificate manager.

☑ Use global security settings for certificate manager

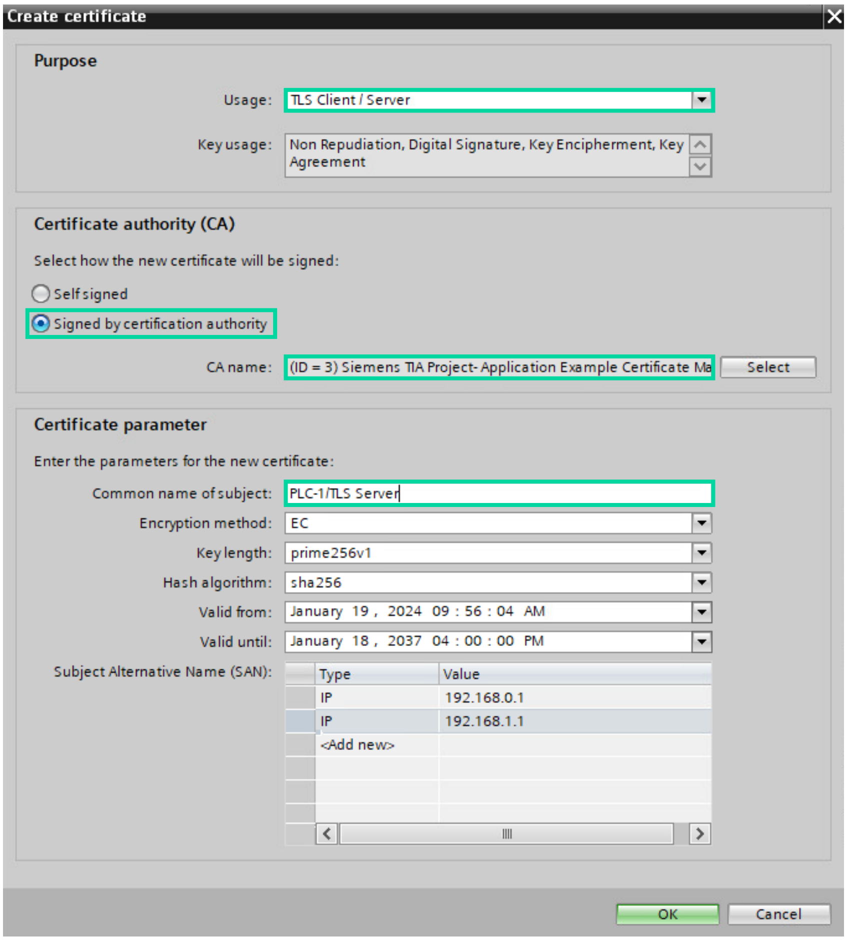
Device certificates

ID	Common name of subject	Service	Issuer	Valid until
8	PLC-1/Webserver-8	WebServer	O=Siemens, C=DE, CN=S...	1/17/2037
5	PLC-1/OPCUA-1-5	Not specified	O=Siemens, C=DE, CN=S...	1/16/2037
4	PLC-1/Communication-4	TlsServer	O=Siemens, C=DE, CN=S...	1/16/2037
6	PLC-1/OPCUA Server	OpcUa	O=Siemens, C=DE, CN=S...	1/16/2037
	<Add new>			



ID	Common name of subject	Issuer	Valid until
4	PLC-1/Communication-4	O=Siemens, C=DE, CN=S...	1/16/2037
5	PLC-1/OPCUA-1-5	O=Siemens, C=DE, CN=S...	1/15/2037
6	PLC-1/OPCUA Server	O=Siemens, C=DE, CN=S...	1/16/2037
7	UaExpert/OPCUA Client	O=Siemens, C=DE, CN=S...	1/15/2037
8	PLC-1/Webserver-8	O=Siemens, C=DE, CN=S...	1/16/2037

3. Select the usage “TLS Client/Server” and choose a Certification Authority to issue the certificate. The Subject Alternative Names (SANs) are automatically generated.



Create certificate

Purpose

Usage: TLS Client / Server

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Key Agreement

Certificate authority (CA)

Select how the new certificate will be signed:

○ Self signed

● Signed by certification authority

CA name: (ID = 3) Siemens TIA Project-Application Example Certificate Ma

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-1/TLS Server

Encryption method: EC

Key length: prime256v1

Hash algorithm: sha256

Valid from: January 19, 2024 09 : 56 : 04 AM

Valid until: January 18, 2037 04 : 00 : 00 PM

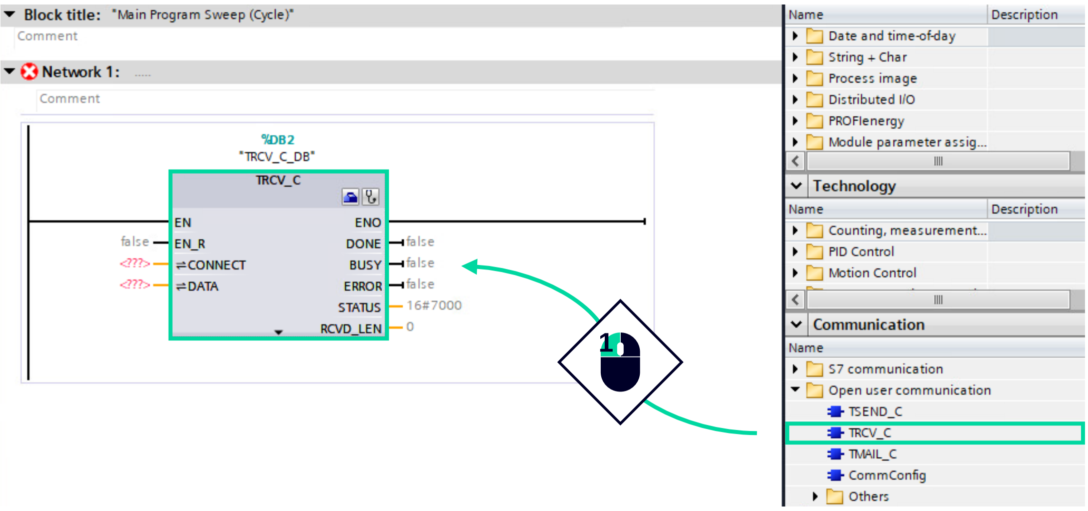
Subject Alternative Name (SAN):

Type	Value
IP	192.168.0.1
IP	192.168.1.1
<Add new>	

Program the OUC communication block

Once the certificate is created, open the “Main” OB of the CPU.

1. In the “Instructions” tab, open the folder “Communication > Open user communication” and drag-and-drop the “TRCV_C” function block to the main program.



Block title: "Main Program Sweep (Cycle)"

Comment

Network 1: .....

Comment

%DB2
"TRCV_C_DB"
TRCV_C

Input	Value	Output	Value
EN		ENO	
EN_R	false	DONE	false
CONNECT	<???>	BUSY	false
DATA	<???>	ERROR	false
		STATUS	16#7000
		RCVD_LEN	0

Name	Description
Date and time-of-day	
String + Char	
Process image	
Distributed I/O	
PROFIenergy	
Module parameter assig...	

Technology

Name	Description
Counting, measurement...	
PID Control	
Motion Control	

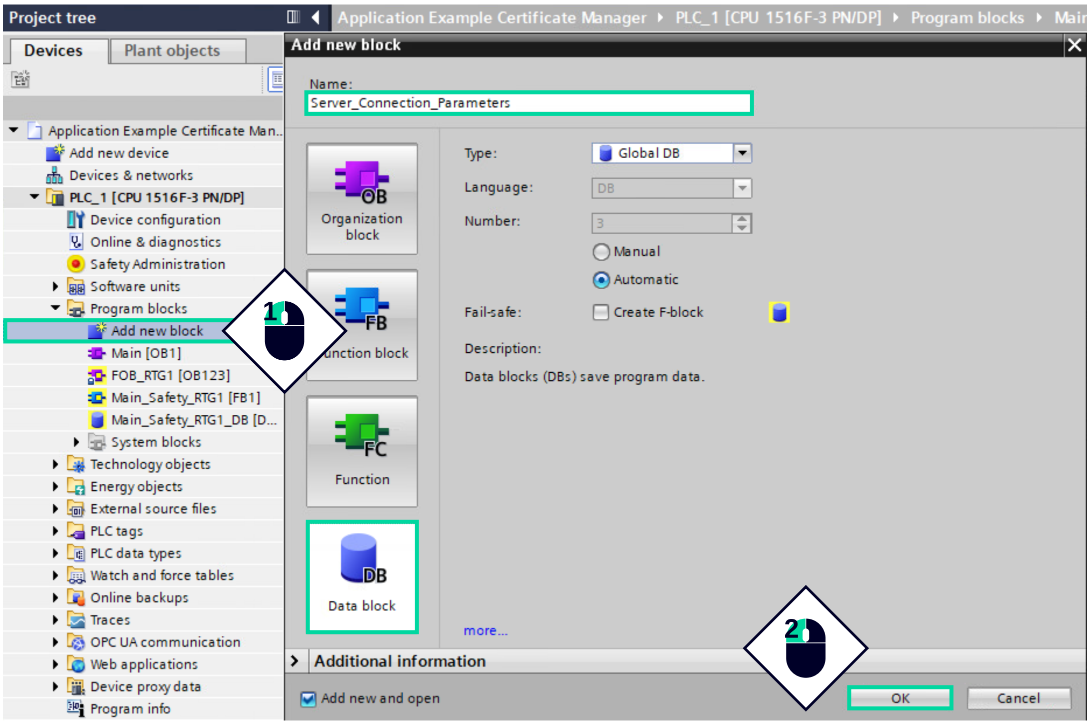
Communication

Name
S7 communication
Open user communication
TSEND_C
TRCV_C
TMAIL_C
CommConfig
Others

This function block requires three main input parameters:

- EN_R (Enable receive): indicates if the server is ready to receive data.
- CONNECT: variable with all necessary connection parameters.
- DATA: variables that will be overwritten with the data being sent by the client.

2. To set up the variable with the necessary connection parameters, create a new data block in the project and add a “TCON_IP_V4_SEC” variable. Set up this variable as shown in the image below.



Name: Server_Connection_Parameters

Type: Global DB

Language: DB

Number: 3

○ Manual

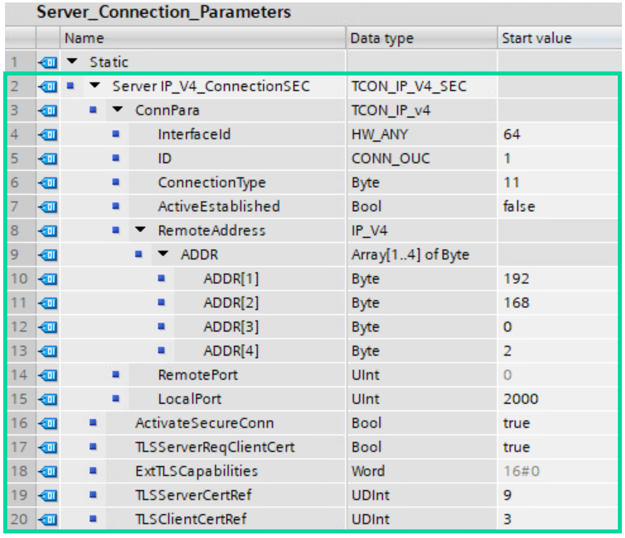
● Automatic

Fail-safe: □ Create F-block

Description:

Data blocks (DBs) save program data.

☑ Add new and open



Server_Connection_Parameters

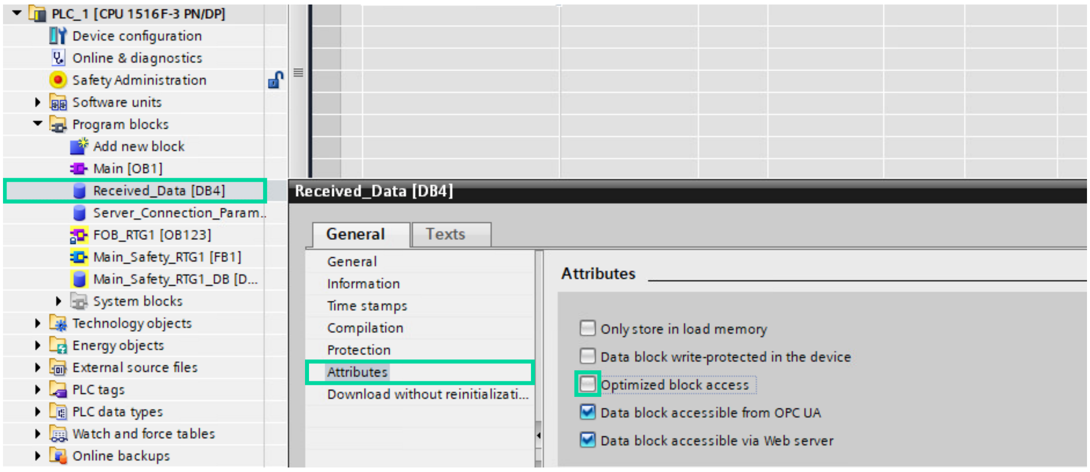
	Name	Data type	Start value
1	Static		
2	Server IP_V4_ConnectionSEC	TCON_IP_V4_SEC	
3	ConnPara	TCON_IP_v4	
4	InterfaceId	HW_ANY	64
5	ID	CONN_OUC	1
6	ConnectionType	Byte	11
7	ActiveEstablished	Bool	false
8	RemoteAddress	IP_V4	
9	ADDR	Array[1..4] of Byte	
10	ADDR[1]	Byte	192
11	ADDR[2]	Byte	168
12	ADDR[3]	Byte	0
13	ADDR[4]	Byte	2
14	RemotePort	UInt	0
15	LocalPort	UInt	2000
16	ActivateSecureConn	Bool	true
17	TLSServerReqClientCert	Bool	true
18	ExtTLSCapabilities	Word	16#0
19	TLSServerCertRef	UDInt	9
20	TLSClientCertRef	UDInt	3

NOTE

The “TLSServerCertRef” field must contain the ID, specified within the global certificate manager, of the server’s certificate.

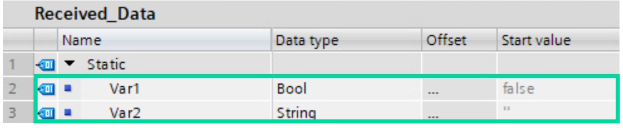
The “TLSClientCertRef” is configured with the root certificate (ID = 3), as this CA will issue the client’s certificate. If the server trusts the CA, it automatically extends that trust to the client.

3. Add a second data block to store the incoming information sent by the client. Configure the data block to operate without "Optimized block access" and include the variables that are intended for transfer during communication.



Attributes

□ Only store in load memory
□ Data block write-protected in the device
□ Optimized block access
☑ Data block accessible from OPC UA
☑ Data block accessible via Web server

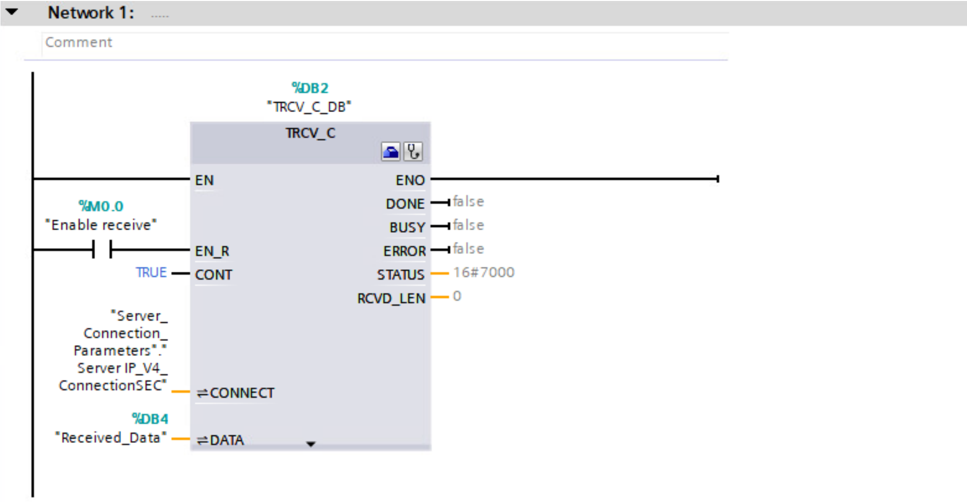


Received_Data

	Name	Data type	Offset	Start value
1	▼ Static			
2	▪ Var1	Bool	...	false
3	▪ Var2	String	...	''

4. Include the "Server IP_V4_ConnectionSEC" variable into the “CONNECT” field of the function block and drag-and-drop the "Received_Data" DB to the “DATA” field.

   To indicate when the server is ready to receive data, add a new tag to the “EN_R” field. Set the “CONT” field to true to maintain the connection alive.

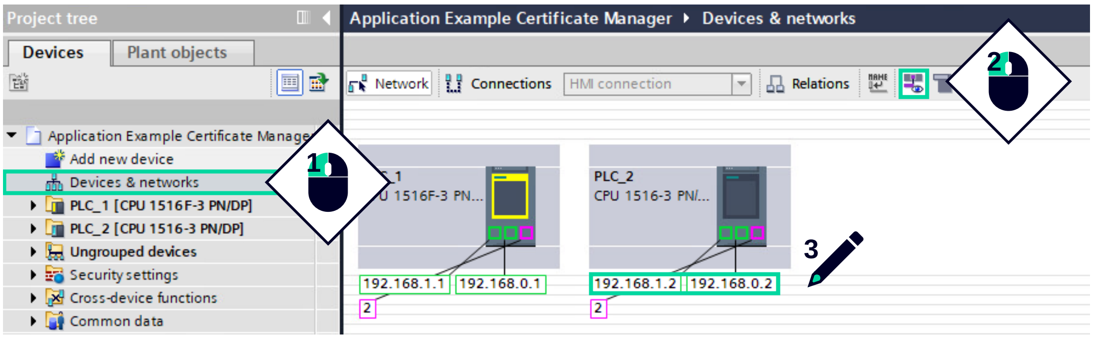


2.6.3 Setting up the TLS client

Commissioning of a new device

As previously mentioned, the TLS client will be running on a second CPU. Therefore, add a new CPU to the project and commission it:

1. Navigate to the “Network view” and assign new IP Addresses to the second CPU.

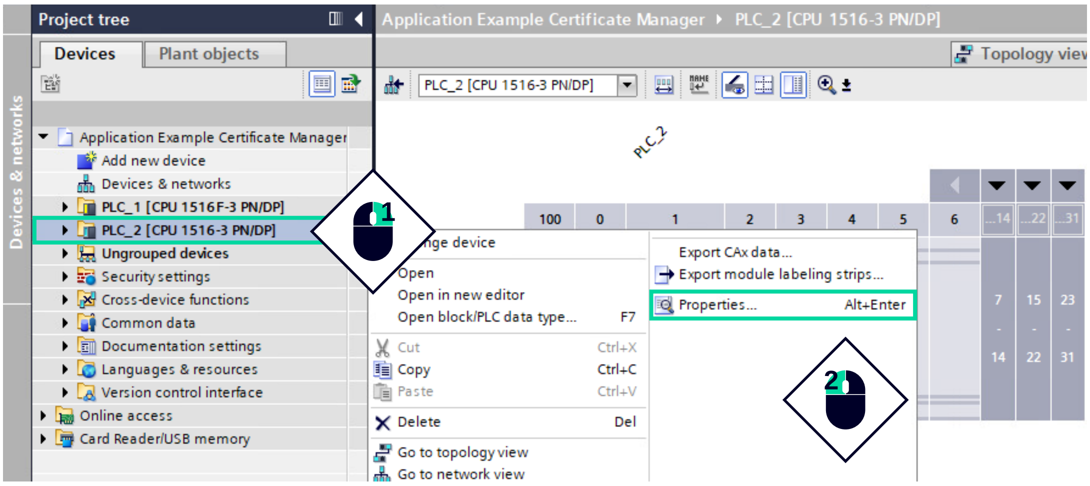


2. Activate the global security settings in the device following the steps covered in section 2.3.3. Renew the secure PG-HMI communication certificate if it was deleted during this step.
3. Set up a new user and role with the necessary “Access Level” rights to access the CPU.

Creation of the client’s certificate

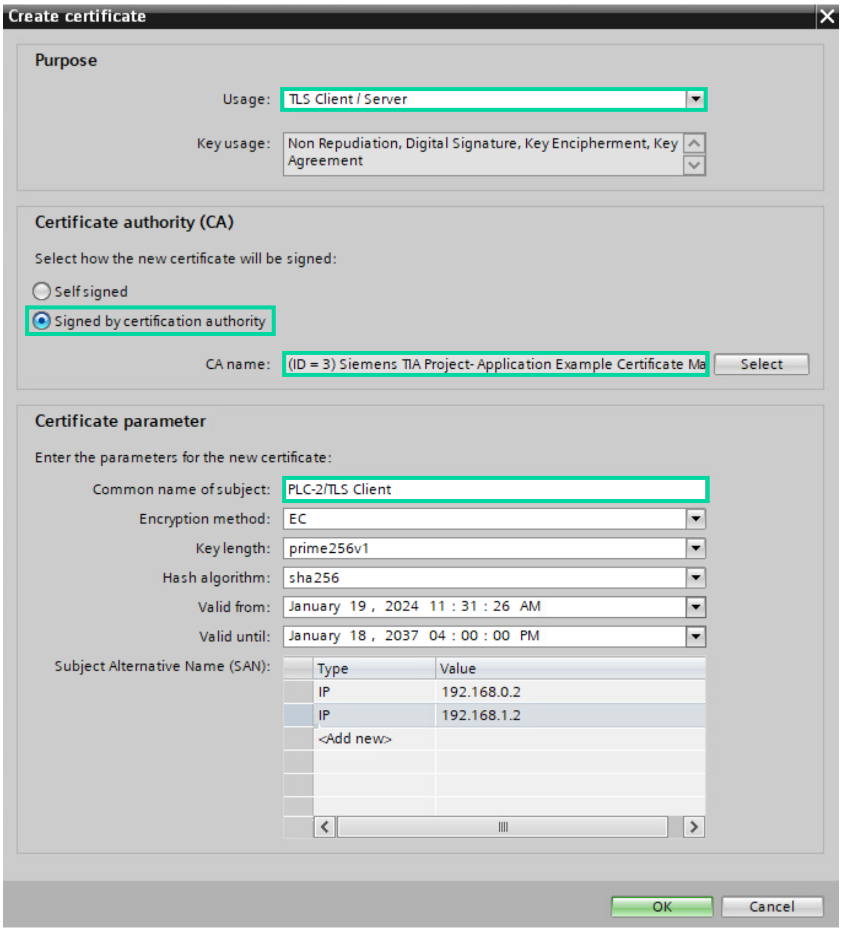
To set up the TLS client, create a new TLS client/server certificate:

1. Select the CPU in the project tree and navigate to the “Properties” tab.



2. Navigate to the entry “Protection and Security > Certificate Manager > Certificate management within TIA Portal” and create a new certificate in the “Device certificate” section.

3. Select the usage “TLS Client/Server” and choose Certification Authority with ID 3 to issue the certificate. The Subject Alternative Names (SANs) are automatically generated.



Create certificate

Purpose

Usage: TLS Client / Server

Key usage: Non Repudiation, Digital Signature, Key Encipherment, Key Agreement

Certificate authority (CA)

Select how the new certificate will be signed:

○ Self signed

● Signed by certification authority

CA name: (ID = 3) Siemens TIA Project-Application Example Certificate Ma | Select

Certificate parameter

Enter the parameters for the new certificate:

Common name of subject: PLC-2/TLS Client

Encryption method: EC

Key length: prime256v1

Hash algorithm: sha256

Valid from: January 19 , 2024 11 : 31 : 26 AM

Valid until: January 18 , 2037 04 : 00 : 00 PM

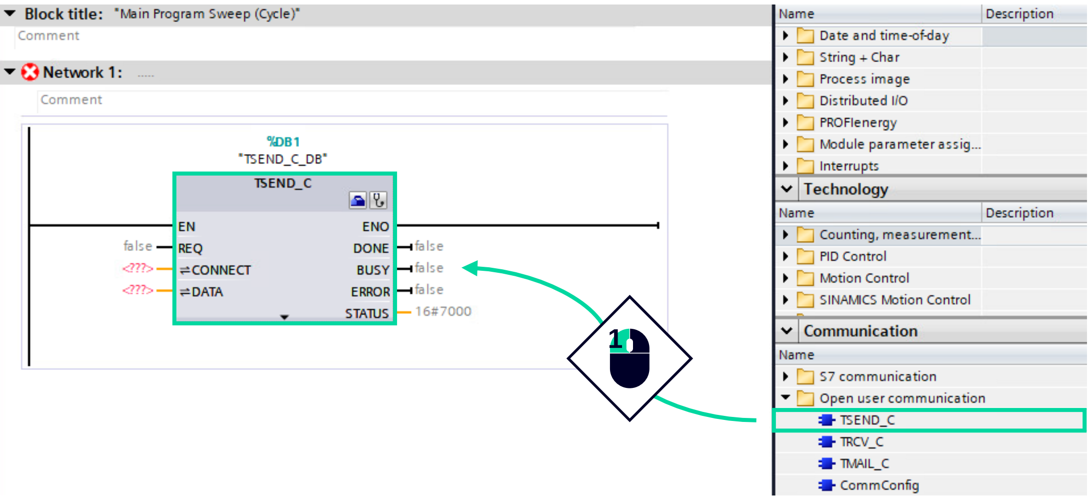
Subject Alternative Name (SAN):

Type	Value
IP	192.168.0.2
IP	192.168.1.2
<Add new>	

OK | Cancel

Program the OUC communication block

1. Open the folder “Communication > Open user communication” and drag-and-drop the “TSEND_C” function block to the main program.



Block title: "Main Program Sweep (Cycle)"

Comment

Network 1: .....

Comment

Name	Description
Date and time-of-day	
String + Char	
Process image	
Distributed I/O	
PROFIenergy	
Module parameter assig...	
Interrupts	

Technology

Name	Description
Counting, measurement...	
PID Control	
Motion Control	
SINAMICS Motion Control	

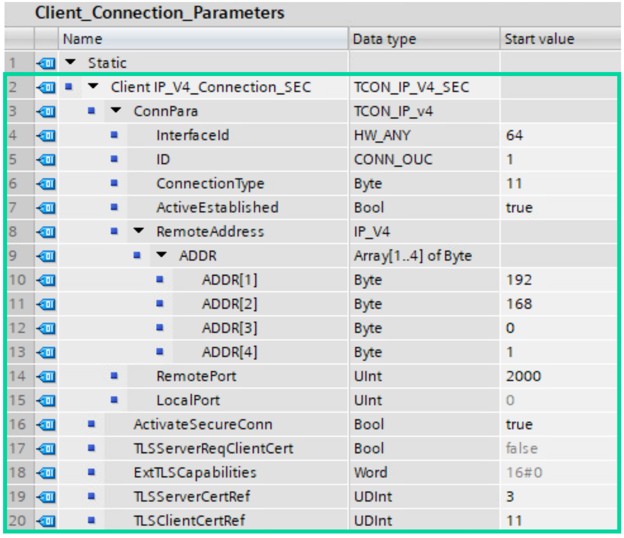
Communication

Name
S7 communication
Open user communication
TSEND_C
TRCV_C
TMAIL_C
CommConfig

This function block requires three main input parameters:

- REQ: trigger to send the data.
- CONNECT: variable with all necessary connection parameters.
- DATA: variables that will be sent by the client.

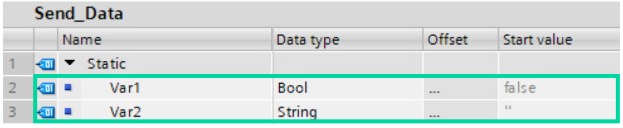
2. To set up the variable with the necessary connection parameters, create a new data block in the project and add a “TCON_IP_V4_SEC” variable. Set up this variable as shown in the image below.



Client_Connection_Parameters

	Name	Data type	Start value
1	▼ Static		
2	▼ Client IP_V4_Connection_SEC	TCON_IP_V4_SEC	
3	▼ ConnPara	TCON_IP_v4	
4	InterfaceId	HW_ANY	64
5	ID	CONN_OUC	1
6	ConnectionType	Byte	11
7	ActiveEstablished	Bool	true
8	▼ RemoteAddress	IP_V4	
9	▼ ADDR	Array[1..4] of Byte	
10	ADDR[1]	Byte	192
11	ADDR[2]	Byte	168
12	ADDR[3]	Byte	0
13	ADDR[4]	Byte	1
14	RemotePort	UInt	2000
15	LocalPort	UInt	0
16	ActivateSecureConn	Bool	true
17	TLSServerReqClientCert	Bool	false
18	ExtTLSCapabilities	Word	16#0
19	TLSServerCertRef	UDInt	3
20	TLSClientCertRef	UDInt	11

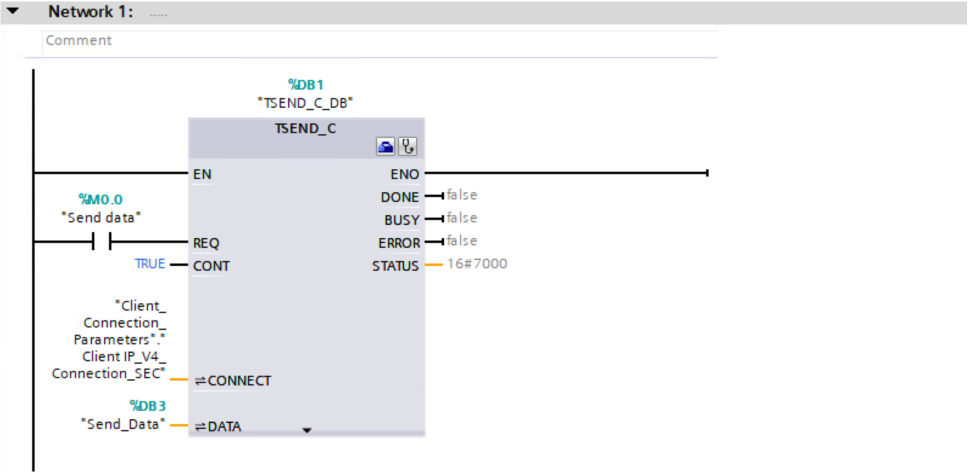
3. Add a second data block to store the information that is going to be sent by the client. Configure the data block to operate without "Optimized block access" and include the variables that are intended for transfer during communication.



Send_Data

	Name	Data type	Offset	Start value
1	▼ Static			
2	Var1	Bool	...	false
3	Var2	String	...	''

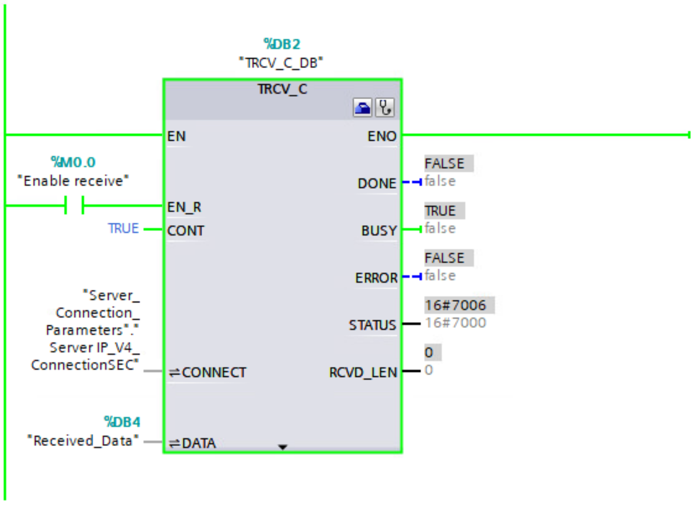
4. Include the "Client IP_V4_ConnectionSEC" variable into the “CONNECT” field of the function block and drag-and-drop the "Send_Data" DB to the “DATA” field. To trigger the send data instruction, add a new tag to the “REQ” field. Set the “CONT” field to true to maintain the connection alive.



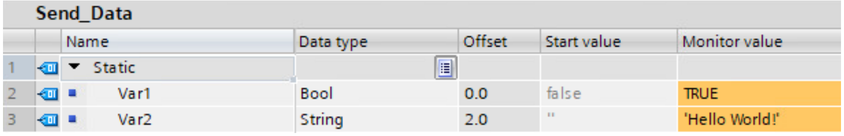
2.6.4 Testing a Secure OUC communication

Once both devices are configured and running, the Secure Open User Communication can be tested. To establish the connection between server and client:

1. Activate “Enable receive” to allow data reception on the server’s side. Confirm that the status of the output field "BUSY" is true.

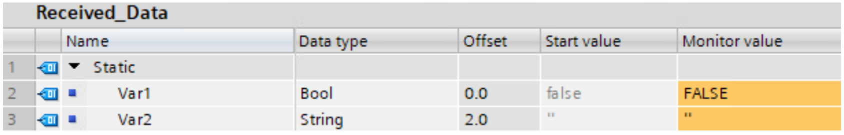


2. Apply changes to the variables that the client is set to transmit. As depicted bellow, there are different values in the respective data blocks of client and server.



Send_Data

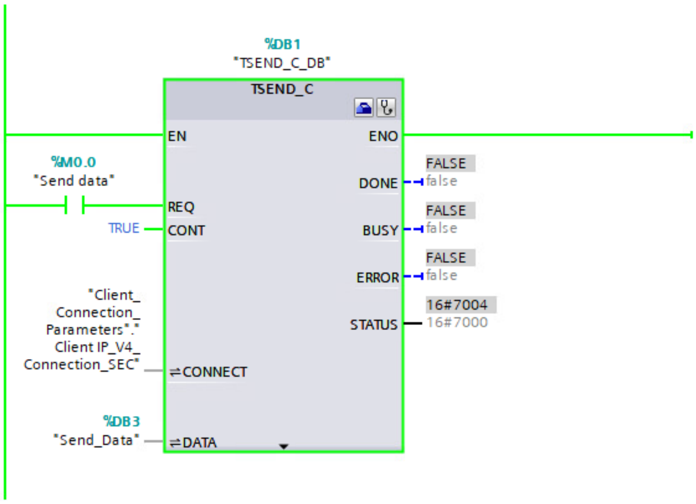
	Name	Data type	Offset	Start value	Monitor value
1	▼ Static				
2	Var1	Bool	0.0	false	TRUE
3	Var2	String	2.0	''	'Hello World!'



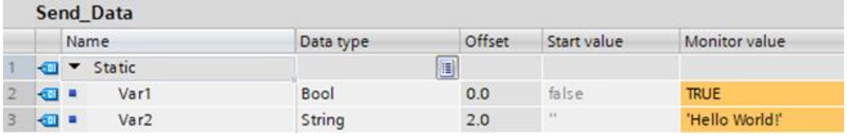
Received_Data

	Name	Data type	Offset	Start value	Monitor value
1	▼ Static				
2	Var1	Bool	0.0	false	FALSE
3	Var2	String	2.0	''	''

3. Activate the client’s trigger to transmit the data.

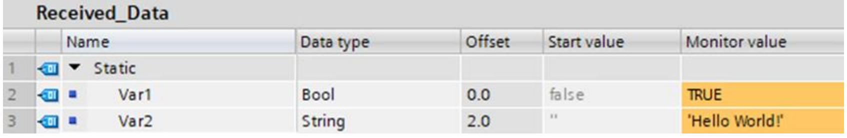


4. Verify that the new updated values are received in the "Received_Data" DB.



Send_Data

		Name	Data type	Offset	Start value	Monitor value
1		▼ Static				
2		■ Var1	Bool	0.0	false	TRUE
3		■ Var2	String	2.0	''	'Hello World!'



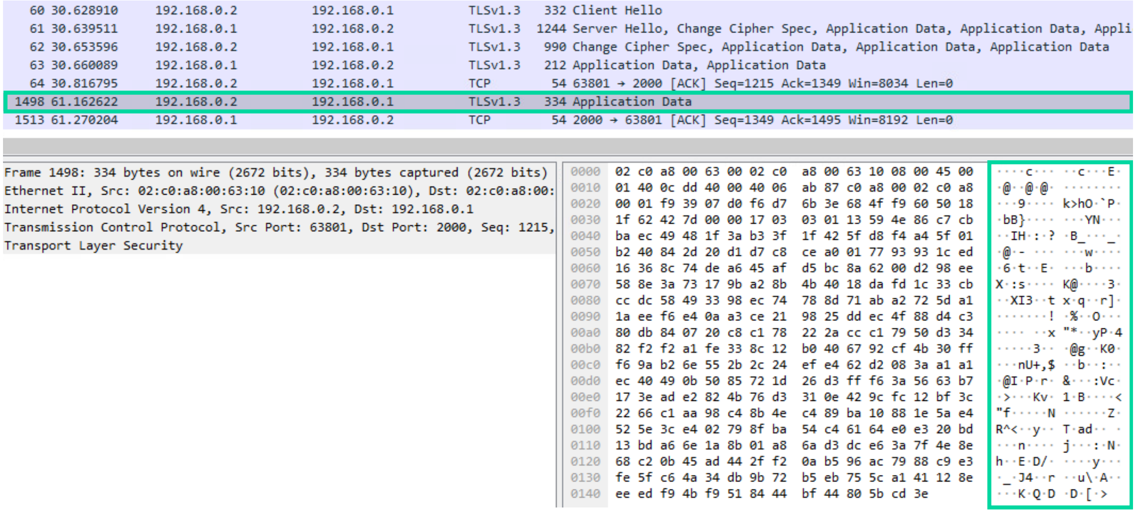
Received_Data

		Name	Data type	Offset	Start value	Monitor value
1		▼ Static				
2		■ Var1	Bool	0.0	false	TRUE
3		■ Var2	String	2.0	''	'Hello World!'

Secure OUC vs Unsecured OUC

To understand the importance of encrypting and signing data, Wireshark is used to analyze the communication packages sent during transmission.

When data is transmitted via secure communication, it is encrypted and safeguarded with TLS v1.3. This ensures confidentiality of sensitive data, maintains its integrity, and authenticates the sender.

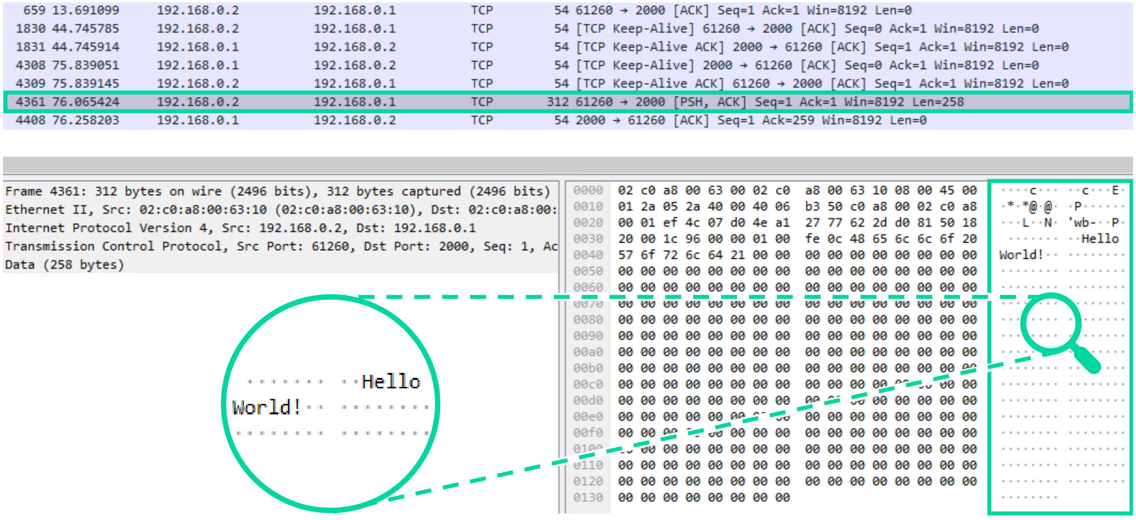


```
  60 30.628910    192.168.0.2     192.168.0.1     TLSv1.3   332 Client Hello
  61 30.639511    192.168.0.1     192.168.0.2     TLSv1.3  1244 Server Hello, Change Cipher Spec, Application Data, Application Data, Appli
  62 30.653596    192.168.0.2     192.168.0.1     TLSv1.3   990 Change Cipher Spec, Application Data, Application Data, Application Data
  63 30.660089    192.168.0.1     192.168.0.2     TLSv1.3   212 Application Data, Application Data
  64 30.816795    192.168.0.2     192.168.0.1     TCP        54 63801 → 2000 [ACK] Seq=1215 Ack=1349 Win=8034 Len=0
1498 61.162622    192.168.0.2     192.168.0.1     TLSv1.3   334 Application Data
1513 61.270204    192.168.0.1     192.168.0.2     TCP        54 2000 → 63801 [ACK] Seq=1349 Ack=1495 Win=8192 Len=0
```

```
Frame 1498: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits)
Ethernet II, Src: 02:c0:a8:00:63:10 (02:c0:a8:00:63:10), Dst: 02:c0:a8:00:
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 63801, Dst Port: 2000, Seq: 1215,
Transport Layer Security
```

```
0000  02 c0 a8 00 63 00 02 c0  a8 00 63 10 08 00 45 00   ····c··· ··c···E·
0010  01 40 0c dd 40 00 40 06  ab 87 c0 a8 00 02 c0 a8   ·@··@·@· ········
0020  00 01 f9 39 07 d0 f6 d7  6b 3e 68 4f f9 60 50 18   ···9···· k>hO·`P·
0030  1f 62 42 7d 00 00 17 03  03 01 13 59 4e 86 c7 cb   ·bB}···· ···YN···
0040  ba ec 49 48 1f 3a b3 3f  1f 42 5f d8 f4 a4 5f 01   ··IH·:·? ·B_···_·
0050  b2 40 84 2d 20 d1 d7 c8  ce a0 01 77 93 93 1c ed   ·@·- ··· ···w····
0060  16 36 8c 74 de a6 45 af  d5 bc 8a 62 00 d2 98 ee   ·6·t··E· ···b····
0070  58 8e 3a 73 17 9b a2 8b  4b 40 18 da fd 1c 33 cb   X·:s···· K@····3·
0080  cc dc 58 49 33 98 ec 74  78 8d 71 ab a2 72 5d a1   ··XI3··t x·q··r]·
0090  1a ee f6 e4 0a a3 ce 21  98 25 dd ec 4f 88 d4 c3   ·······! ·%··O···
00a0  80 db 84 07 20 c8 c1 78  22 2a cc c1 79 50 d3 34   ···· ··x "*··yP·4
00b0  82 f2 f2 a1 fe 33 8c 12  b0 40 67 92 cf 4b 30 ff   ·····3·· ·@g··K0·
00c0  f6 9a b2 6e 55 2b 2c 24  ef e4 62 d2 08 3a a1 a1   ···nU+,$ ··b··:··
00d0  ec 40 49 0b 50 85 72 1d  26 d3 ff f6 3a 56 63 b7   ·@I·P·r· &···:Vc·
00e0  17 3e ad e2 82 4b 76 d3  31 0e 42 9c fc 12 bf 3c   ·>···Kv· 1·B····<
00f0  22 66 c1 aa 98 c4 8b 4e  c4 89 ba 10 88 1e 5a e4   "f·····N ······Z·
0100  52 5e 3c e4 02 79 8f ba  54 c4 61 64 e0 e3 20 bd   R^<··y·· T·ad·· ·
0110  13 bd a6 6e 1a 8b 01 a8  6a d3 dc e6 3a 7f 4e 8e   ···n···· j···:·N·
0120  68 c2 0b 45 ad 44 2f f2  0a b5 96 ac 79 88 c9 e3   h··E·D/· ····y···
0130  fe 5f c6 4a 34 db 9b 72  b5 eb 75 5c a1 41 12 8e   ·_·J4··r ··u\·A··
0140  ee ed f9 4b f9 51 84 44  bf 44 80 5b cd 3e         ···K·Q·D ·D·[·>
```

On the other hand, unsecure OUC transmits data in plain text, leaving sensitive information vulnerable to easy access and manipulation by attackers.



```
 659 13.691099    192.168.0.2     192.168.0.1     TCP        54 61260 → 2000 [ACK] Seq=1 Ack=1 Win=8192 Len=0
1830 44.745785    192.168.0.2     192.168.0.1     TCP        54 [TCP Keep-Alive] 61260 → 2000 [ACK] Seq=0 Ack=1 Win=8192 Len=0
1831 44.745914    192.168.0.1     192.168.0.2     TCP        54 [TCP Keep-Alive ACK] 2000 → 61260 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4308 75.839051    192.168.0.1     192.168.0.2     TCP        54 [TCP Keep-Alive] 2000 → 61260 [ACK] Seq=0 Ack=1 Win=8192 Len=0
4309 75.839145    192.168.0.2     192.168.0.1     TCP        54 [TCP Keep-Alive ACK] 61260 → 2000 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4361 76.065424    192.168.0.2     192.168.0.1     TCP       312 61260 → 2000 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=258
4408 76.258203    192.168.0.1     192.168.0.2     TCP        54 2000 → 61260 [ACK] Seq=1 Ack=259 Win=8192 Len=0
```

```
Frame 4361: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits)
Ethernet II, Src: 02:c0:a8:00:63:10 (02:c0:a8:00:63:10), Dst: 02:c0:a8:00:
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 61260, Dst Port: 2000, Seq: 1, Ac
Data (258 bytes)
```

```
0000  02 c0 a8 00 63 00 02 c0  a8 00 63 10 08 00 45 00   ····c··· ··c···E·
0010  01 2a 05 2a 40 00 40 06  b3 50 c0 a8 00 02 c0 a8   ·*·*@·@· ·P······
0020  00 01 ef 4c 07 d0 4e a1  27 77 62 2d d0 81 50 18   ···L··N· 'wb-··P·
0030  20 00 1c 96 00 00 01 00  fe 0c 48 65 6c 6c 6f 20    ······· ··Hello 
0040  57 6f 72 6c 64 21 00 00  00 00 00 00 00 00 00 00   World!·· ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0130  00 00 00 00 00 00 00 00                            ········
```

3 Additional information – Certificate management via OPC UA

3.1 GDS Push for dynamic certificate management

3.1.1 Overview

Supported TIA Portal and firmware versions

With TIA Portal V17 and firmware version V2.9, the GDS Push functionality has been integrated into the SIMATIC S7-1500 controller for OPC UA server certificates. Additionally, as of TIA Portal version V18 and firmware version V3.0, GDS push management for web server certificates is also supported.

Description

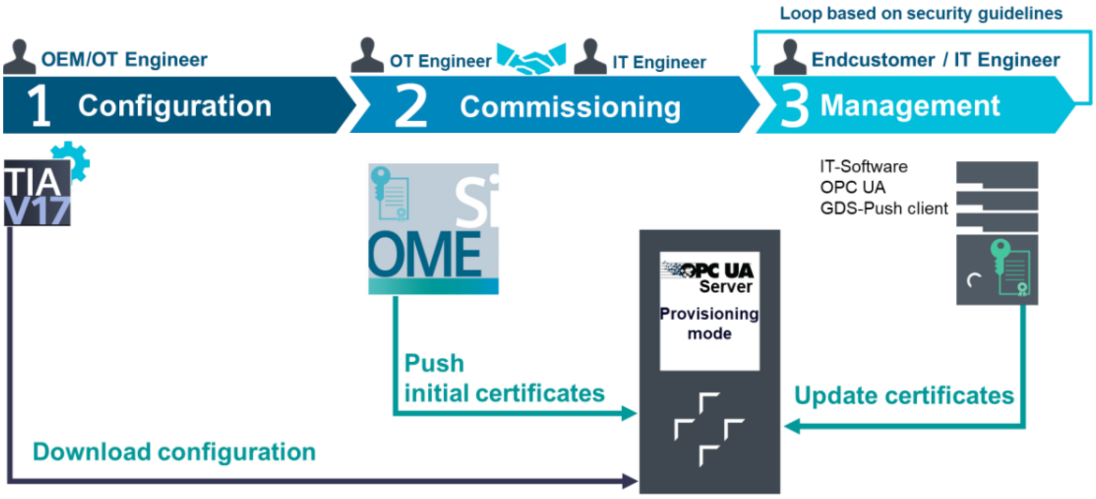
GDS Push utilizes the certificate management services of an OPC UA server to transfer web and OPC UA server certificates during runtime, as well as trust lists and certificate revocation lists for the latter.

After the CPU has been provisioned, certificates can be managed without TIA Portal, offering enhanced flexibility and convenience for long-term maintenance. This dynamic certificate management approach eliminates any manual work required for reconfiguring the CPU, i.e. after the period of validity of a certificate has expired. Moreover, GDS Push can transfer certificates and lists with the CPU in STOP and RUN mode, enabling operators to handle certificates with minimal disruptions to production.

Certificate management from the CPU's point of view

The use of dynamic certificate handling on the CPU is divided into three phases:

1. CPU configuration in TIA Portal and downloading of the configuration to the CPU.
2. Initial provisioning of a trust list and a server certificate.
3. Regular updating of certificates according to the security policies of a company.



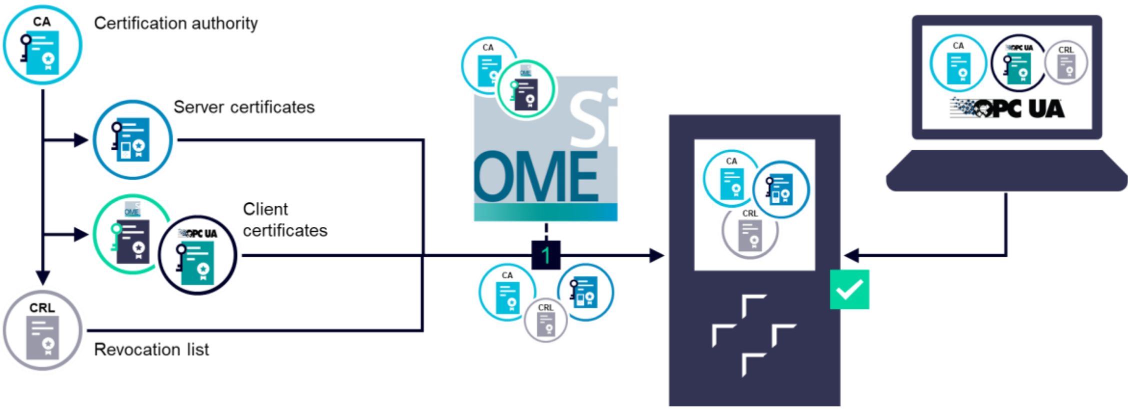
Refer to the application example titled "Dynamic certificate management with OPC UA GDS Push" for detailed instructions on how to commission a CPU with GDS Push (https://support.industry.siemens.com/cs/document/109799888).

3.1.2 GDS Push certificate handling scenarios

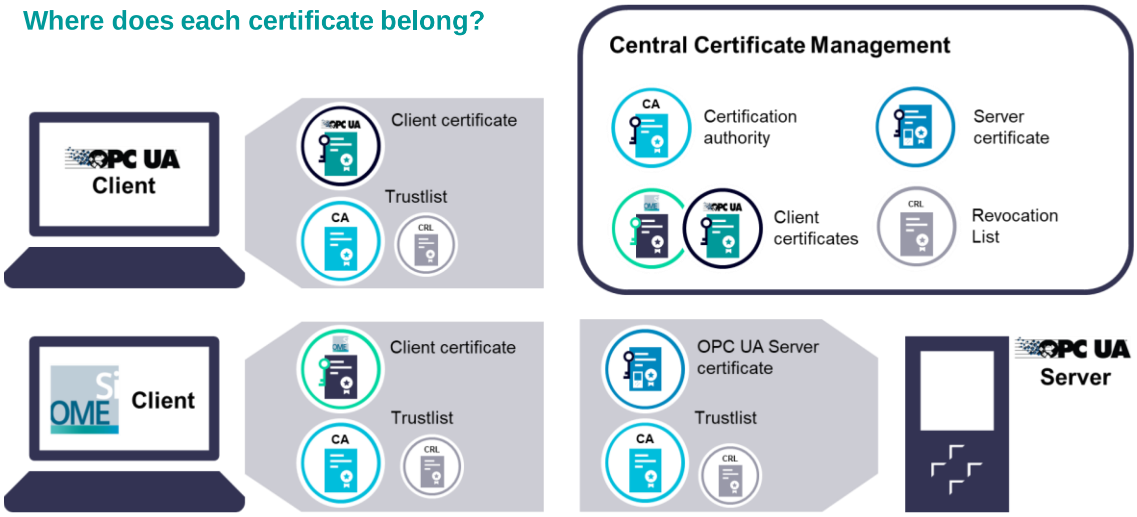
Scenario 1 - OPC UA certificates

Certificates need to be managed dynamically with GDS Push while controllers are in running mode. Both the certificate and private key of the server are generated using a central certificate management.

Workflow

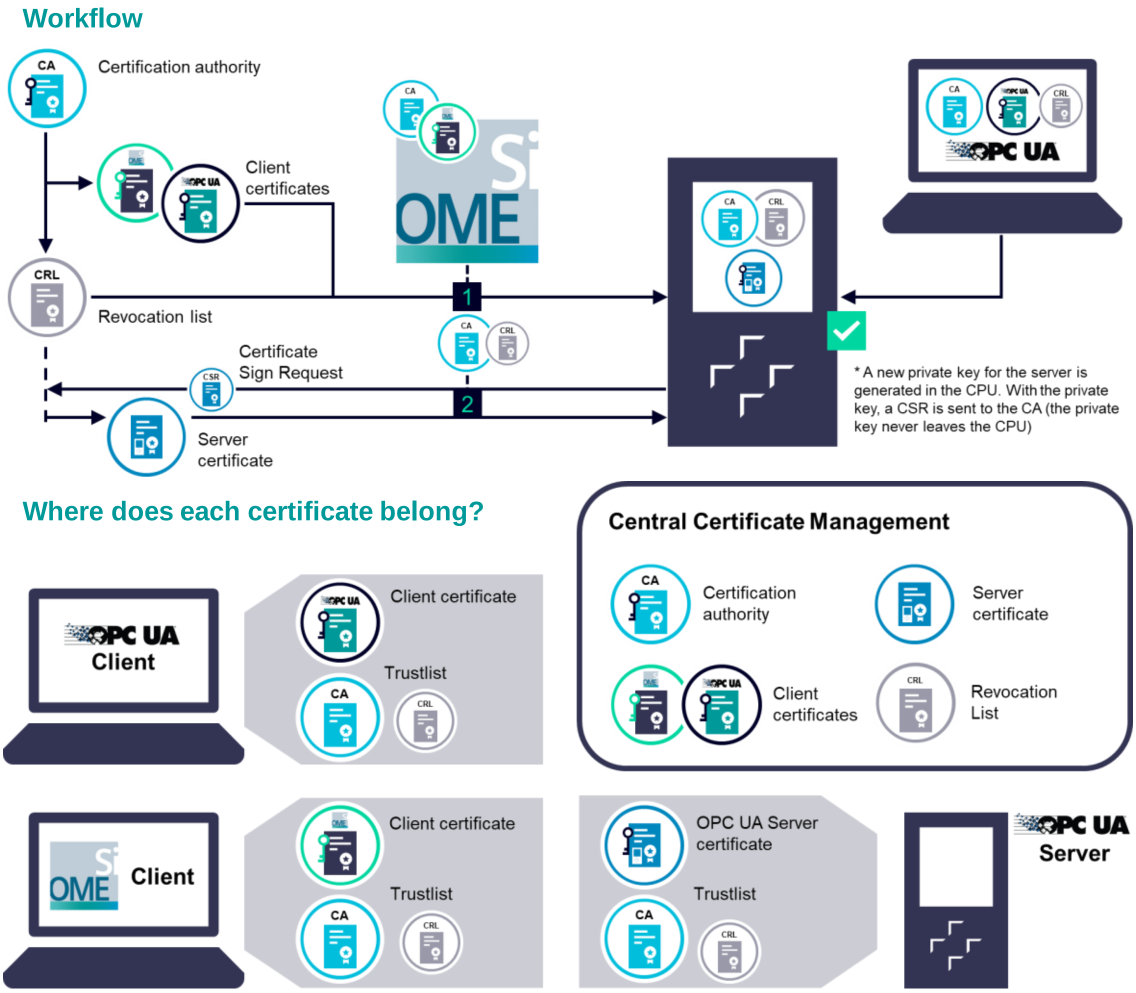


Where does each certificate belong?



Scenario 2 - OPC UA certificates

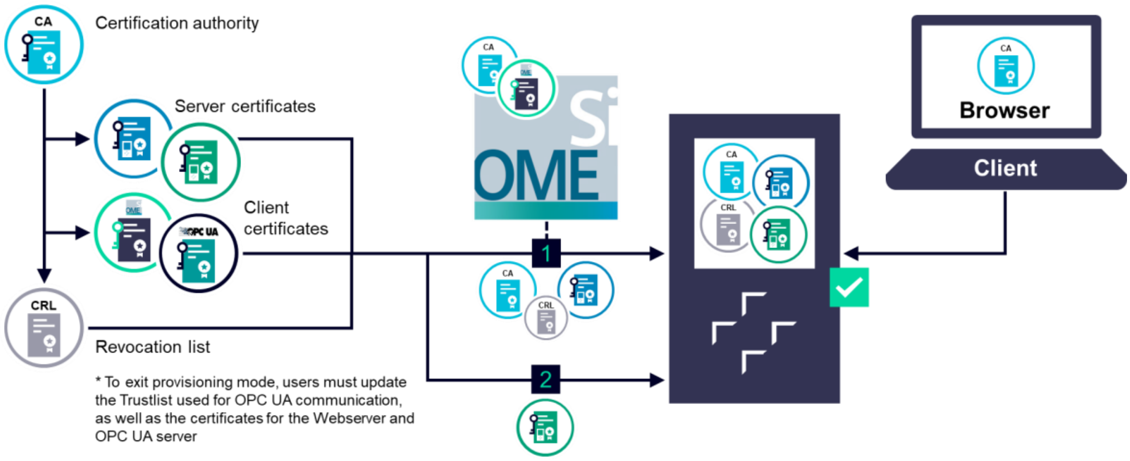
Certificates need to be managed dynamically with GDS Push while controllers are in running mode. To enhance security and stick to safety recommendations, it has been decided to use a Certificate Signing Request (CSR) to guarantee that the private key of the controller never leaves the CPU.



Scenario 3 - Web server certificates

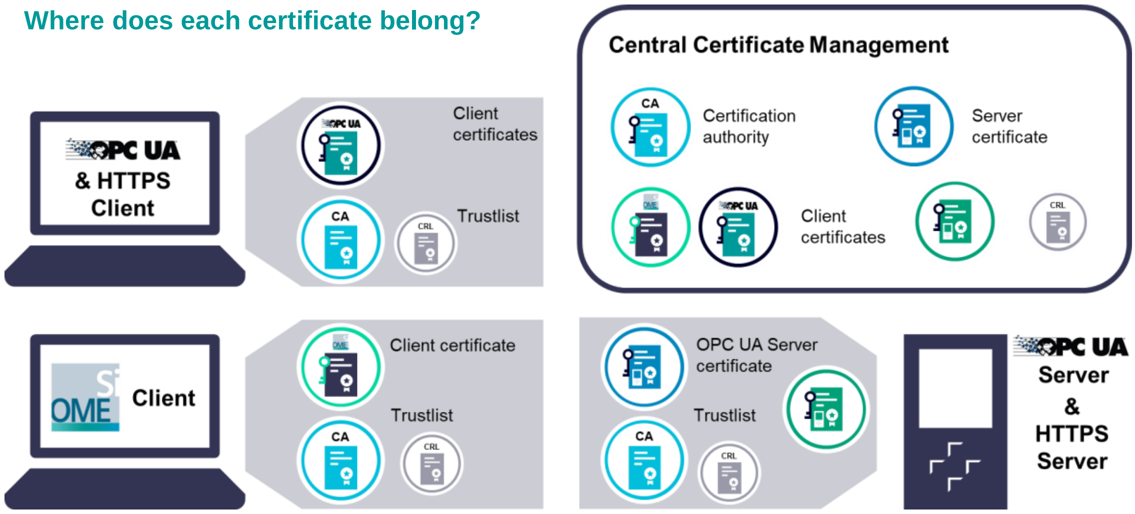
Certificates need to be managed dynamically with GDS Push while controllers are in running mode.

Workflow



* To exit provisioning mode, users must update the Trustlist used for OPC UA communication, as well as the certificates for the Webserver and OPC UA server

Where does each certificate belong?



4 FAQ / Error Handling

4.1 Certificates

4.1.1 Is it possible to work with certificates without protecting the project?

The only available method to work with certificates in TIA Portal, without protecting the project, is by using the local certificate manager with the global security settings disabled. Nonetheless, this approach offers limited functionality and restricts certificates to being self-signed.

4.1.2 How long should a certificate be valid?

In OT environments, the recommended certificate validity is regulated by the specific needs and security practices of the organization. There are, however, some general guidelines highlighted in chapter 1.4.

4.1.3 Which changes on the device configuration will require a new certificate?

Any information of the device configuration that has been included in the certificate, such as IP addresses, will require a certificate renewal.

Certificates generated through the local certificate manager are automatically updated, when relevant configuration changes are applied, once the project is compiled. However, certificates created via the global certificate manager do not undergo automatic updates, requiring users to “Renew” them manually.

4.1.4 Which SAN fields are mandatory?

Different communication protocols may impose mandatory fields within the SAN. The table below provides a summary of the required fields for each use case.

Table 4-1

	OPC UA server and client	TLS server *
URI	Mandatory	-
IP	Optional (Mandatory with FW 2.5)	Mandatory
DNS	Optional	Optional
RID	-	-
Email	-	-
Other Name	-	-

* HTTPS, Secure OUC and PG/HMI communication.

4.1.5 What is the difference between exporting the certificate chain vs certificate?

Exporting the certificate chain involves the export of not just the certificate itself but also of all intermediary and root authorities above it. This results in an export of all public keys from the trust hierarchy, which can be interesting in certain scenarios, such as debugging and troubleshooting.

Check Table 2-3 to determine which file formats support the export of certificate chains.

4.1.6 What happens if an incomplete chain of trust is loaded into the PLC’s “trusted certificate store”?

If an OPC UA client, such as UaExpert, possesses a certificate issued by an intermediate authority, which, in turn, was issued by a root CA, the server must have access to the entire trust chain in its "trusted certificate store".

If an incomplete chain of trust is loaded into the PLC’s “trusted certificate store”, the connection with the server will not be established.

NOTE

Usually, when trusting a higher certificate—be it the root or intermediate CA—automatic trust is extended to all certificates below the one that has been trusted. However, this principle is not applied in the local certificate manager of SIMATIC CPUs.

4.1.7 Which tools can be used to create certificates without TIA Portal?

Some useful tools to create certificates are:

- OpenSSL: is an open-source software used for general-purpose cryptography and to secure communications. To configure the necessary extensions needed for OPC UA and TLS communication, configuration files can be used to summarize all certificate requitements.

  The main drawback of OpenSSL is its reliance on command-line execution, resulting in a steep learning curve that can pose challenges for new users.
- XCA: built on top of OpenSSL, XCA incorporates a graphical interface that offers a user-friendly and intuitive experience for working with certificates. It is designed to handle various tasks, including creating, managing, and renewing X-509 certificates, securely storing private keys, generating revocation lists, processing certificate sign requests and more.

4.1.8 How can certificates be managed without downloading via TIA Portal?

As mentioned in section 3.1.1, GDS Push makes use of the certificate management services of an OPC UA server to transfer certificates during runtime. Additionally, trust lists and certificate revocation lists can also be updated dynamically.

A notable advantage of GDS Push is that, after provisioning the CPU, certificates can be managed without TIA Portal, offering enhanced flexibility and convenience for long-term maintenance.

4.2 OPC UA

4.2.1 Are certificates required to authenticate via username and password?

When a client session is authenticated via username and password, encryption of the password is essential to protect it from being stolen. Nonetheless, only the server’s certificate is required, as the client uses the server's public key to encrypt the password.

Therefore, a client without public key (certificate) and private key can connect to an endpoint, with SecurityMode “None”, employing username and password authentication.

NOTE

Regardless of the SecurityMode and authentication method used, the OPC UA server always sends its certificate to the client before starting the SecureChannel.

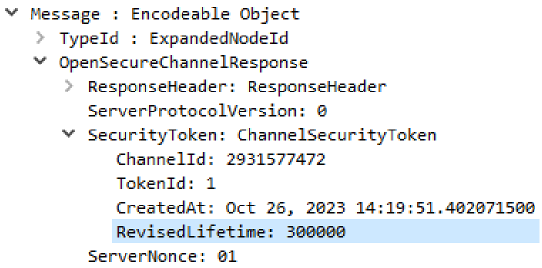
4.2.2 What happens to the OPC UA connection if one certificate expires?

If the OPC UA connection has already been established, the communication between client and server is maintained until the SecureChannel is renewed.

4.2.3 What is the SecureChannel and how often is it renewed?

Before initiating a session, OPC UA communication partners are required to establish a SecureChannel using the Private Key Infrastructure for asymmetric signing and encryption. The SecureChannel is then used to transfer the symmetric key between client and server without the risk of it being intercepted.

To initiate a SecureChannel, the OPC UA client sends a request to the server, specifying the desired Lifetime for the SecureChannel. The server then processes this request and responds to the client by generating a SecurityToken with a designated RevisedLifetime.



```
Message : Encodeable Object
  TypeId : ExpandedNodeId
  OpenSecureChannelResponse
    ResponseHeader: ResponseHeader
    ServerProtocolVersion: 0
    SecurityToken: ChannelSecurityToken
      ChannelId: 2931577472
      TokenId: 1
      CreatedAt: Oct 26, 2023 14:19:51.402071500
      RevisedLifetime: 300000
    ServerNonce: 01
```

OPC UA clients are configured to reopen the SecureChannel when 75% of the SecurityToken Lifetime has elapsed, ensuring that they will receive a new SecurityToken before the previous one expires.

- The minimum lifetime of a SecureChannel in a SIMATIC controller is 300.000 milliseconds, 5 minutes, while the maximum lifetime is set to 3.600.000 milliseconds, 1 hour. Therefore, OPC UA servers running on SIMATIC controllers have a maximum SecurityToken Lifetime of 60 minutes. Due to the 75% rule, clients renew the SecureChannel every 45 minutes.
- Other OPC UA servers have a configuration file where these minimum and maximum values can be modified. SIMATIC controllers don’t have an accessible configuration file that users can modify.

```
<TransportQuotas>
   <OperationTimeout>600000</OperationTimeout>
   <MaxStringLength>1048576</MaxStringLength>
   <MaxByteStringLength>1048576</MaxByteStringLength>
   <MaxArrayLength>65535</MaxArrayLength>
   <MaxMessageSize>4194304</MaxMessageSize>
   <MaxBufferSize>65535</MaxBufferSize>
   <ChannelLifetime>300000</ChannelLifetime>
   <SecurityTokenLifetime>3600000</SecurityTokenLifetime>
 </TransportQuotas>
```

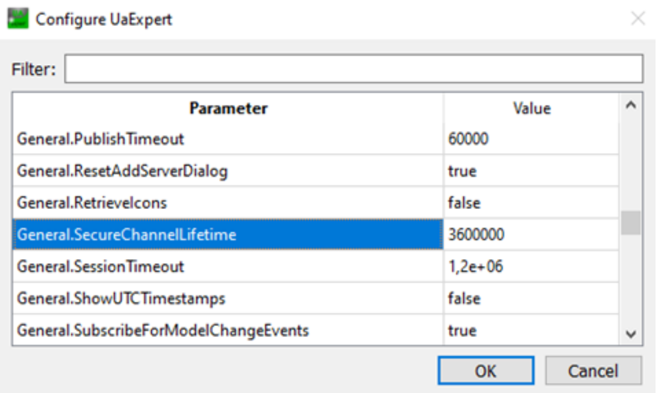
4.2.4 Why is it important to renew the SecureChannel?

Renewing the SecureChannel is important for two main reasons:

1. Attackers can decipher keys by analyzing encrypted messages. The more messages sent using the same key, the easier it becomes to perform “cryptanalytic attacks”. Therefore, symmetric keys used in OPC UA communication should periodically be renewed to avoid this threat.
2. If a server/client certificate expires or its private key gets compromised, it is important to terminate ongoing communications. Applications are only able to verify their partners’ certificates during the process of opening or renewing the SecureChannel. Therefore, without a predefined expiration mechanism for the SecurityToken, clients and servers would not know if their partner’s certificate has expired or if it has been revoked.

NOTE

> The OPC Foundation recommends shorter SecurityToken lifetimes for applications where the number of exchanged messages is expected to be high. This parameter can easily be modified in certain OPC UA client's like UaExpert.



Parameter	Value
General.PublishTimeout	60000
General.ResetAddServerDialog	true
General.RetrieveIcons	false
General.SecureChannelLifetime	3600000
General.SessionTimeout	1,2e+06
General.ShowUTCTimestamps	false
General.SubscribeForModelChangeEvents	true

4.2.5 What limitations exist for GDS Push?

For the OPC UA Push function, an S7-1500 CPU, regardless of the type, has a configuration limit of 62 trust list entries as of firmware version V2.9.

- Each activated certificate-based service, web server and OPC UA server, "consumes" one entry for the certificate and an entry for the private key.
- A Certificate Revocation List (CRL) counts as one entry in the list of trusted certificates.
- A certificate that is used by different services counts as a single trust list entry.

Additionally, the push function has a maximum size limit for elements, such as certificates, of 4096 bytes.

To gain deeper understanding of GDS Push, refer to chapter 11.2.7 of the Manual titled “SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Communication” (https://support.industry.siemens.com/cs/document/59192925).

5 Appendix

5.1 Service and support

SiePortal

The integrated platform for product selection, purchasing and support - and connection of Industry Mall and Online support. The SiePortal home page replaces the previous home pages of the Industry Mall and the Online Support Portal (SIOS) and combines them.

- Products & Services
  In Products & Services, you can find all our offerings as previously available in Mall Catalog.
- Support
  In Support, you can find all information helpful for resolving technical issues with our products.
- mySieportal
  mySiePortal collects all your personal data and processes, from your account to current orders, service requests and more. You can only see the full range of functions here after you have logged in.

You can access SiePortal via this address: sieportal.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:
support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

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:
siemens.com/sitrain

Industry Online Support app

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

Available on the App Store

ANDROID APP ON Google play

5.2 Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109769068
\3\	

5.3 Change documentation

Version	Date	Modification
V1.0	09/2019	First version
V2.0	03/2024	Complete rework