SIEMENS
Ingenuity for life

Dynamic certificate management with SIMATIC S7-1500: OPC UA GDS Push

S7-1500 CPU Firmware V2.9/ TIA Portal V17

https://support.industry.siemens.com/cs/ww/en/view/109799888

Siemens
Industry
Online
Support

Legal information

Use of application examples

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

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

Disclaimer of liability

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

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

Other information

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

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

Security information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

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

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

Table of contents

1 Introduction

1.1 Overview

Systems and networks in the world of IT and OT are evolving together all the time. This increases the risk of cyber threats for industrial plants (OT). An established security mechanism from IT is encrypted and signed data transmission that uses certificates as a basis.

However, this alone is not enough to create a high level of security.

The systems need an automated mechanism which ensures that certificates can be regularly refreshed, and that a system cannot be accessed with compromised certificates.

As an open standard, OPC UA is already in use in many plants for vertical and horizontal communication.

With TIA Portal V17, the GDS Push functionality has been integrated into the SIMATIC S7-1500 controller for the OPC UA server. It affords the ability to refresh the certificates of the OPC UA server during the controller's runtime.

1.2 How GDS Push works

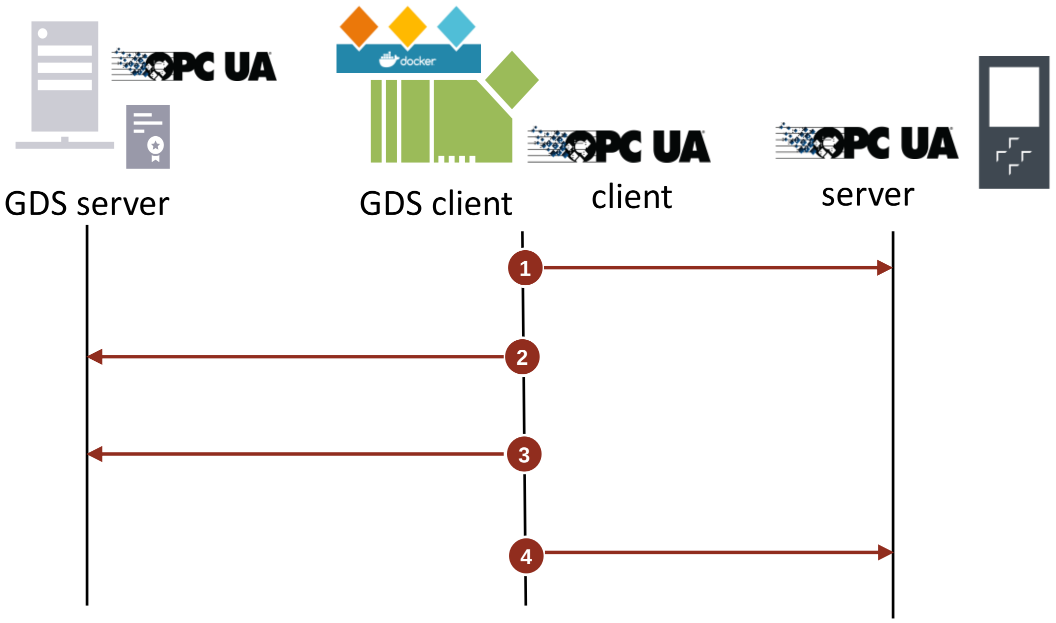
Overview of process steps

The complete system for dynamic loading of certificates is composed of the following components:

- OPC UA server with GDS Push functionality enabled
- GDS server, which provides certificates for all systems
- GDS client, which requests the certificates from the GDS server and transfers them to the server via OPC UA client functionality.

The agent which initiates the GDS Push functionality in the system is the GDS client:

Figure 1-1



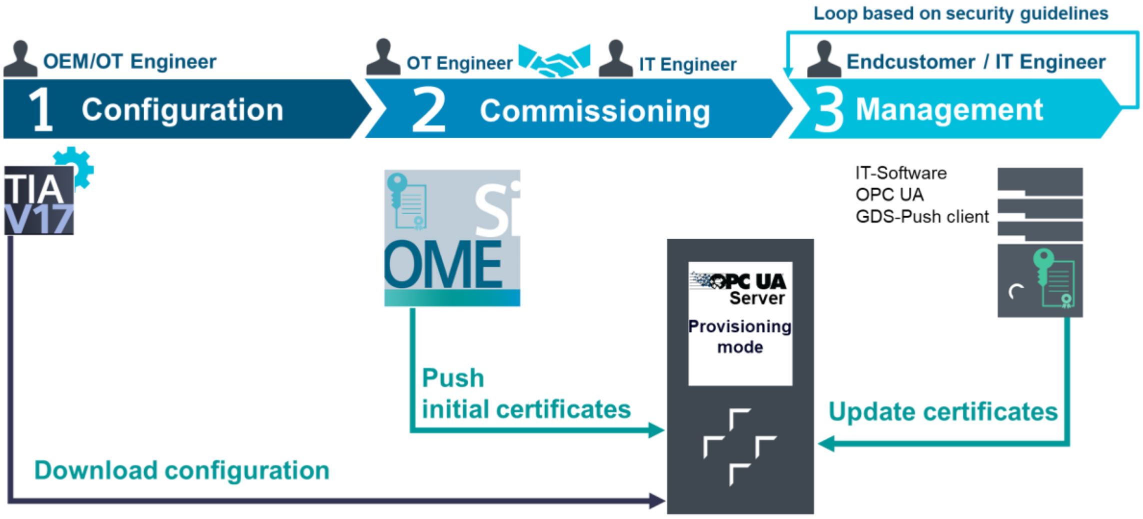
1. The GDS client connects to the OPC UA server of the S7-1500 CPU as an OPC UA client.
2. The GDS client registers the OPC UA server of the S7-1500 CPU with the GDS server.
3. The GDS client requests the certificates from the GDS server; it is these certificates that the OPC UA server must establish a trust relationship with.
4. The GDS client transfers the certificates for the OPC UA server to the CPU.

Certificate management from the CPU's point of view

The use of dynamic certificate handling on the CPU is divided into three phases, which are as follows:

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

Figure 1-2



Functional scope of this example

In this application example, we will consider the following aspects of dynamic certificate management:

- Generation of all necessary certificates, the list of trusted certificates (Certificate Trust List, or CTL), and the list of revoked certificates (Certificate Revocation List, or CRL)
- Configuration of the OPC UA server for the S7-1500 CPU
- Demonstration of dynamic certificate management with the client application "SiOME"
- Testing of the configuration and of the dynamic certificate management with OPC UA client

NOTE The functionality of a GDS client and GDS server are outside the scope of this application example.

1.3 Components used

This application example was created with the following hardware and software components:

Table 1-1

Components	Quantity	Article number	Note
TIA Portal V17	1	• DVD: 6ES7822-1AA07-0YA5 • Download: 6ES7822-1AE07-0YA5 • Upgrade: 6ES7822-1AA07-0YE5, 6ES7822-1AE07-0YE5	
CPU 1518F-4 PN/DP	1	6ES7518-4FP00-0AB0	or any other S7-1500 CPU with FW 2.9 or later
SiOME V2.3.1	1	-	Download and documentation: 109755133

NOTE

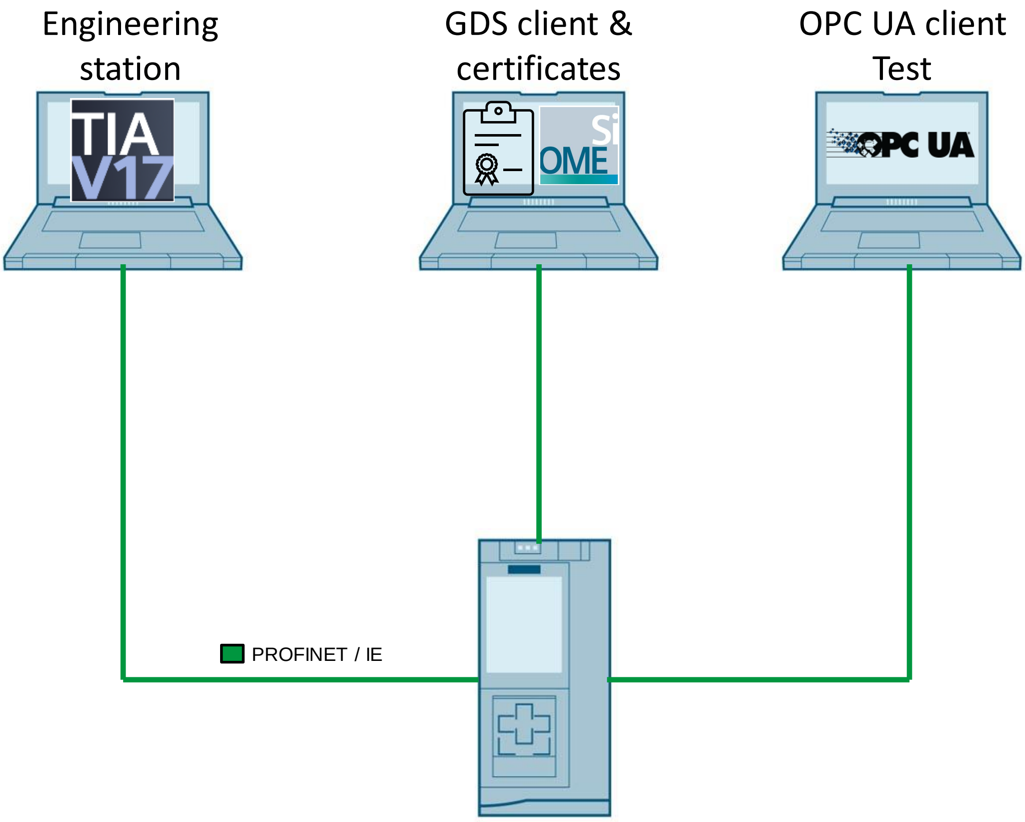
The TIA Portal project is protected. You will need the following credentials to log in:

User: admin
Password: Siemens#1

2 Engineering

2.1 Hardware setup

Figure 2-1



A PG with TIA Portal V17 will be needed for the hardware configuration of the S7-1500 CPU. The GDS functionality is implemented in the "SiOME" client application. "SiOME" needs access to the certificates. An additional OPC UA client is used to test the functionality.

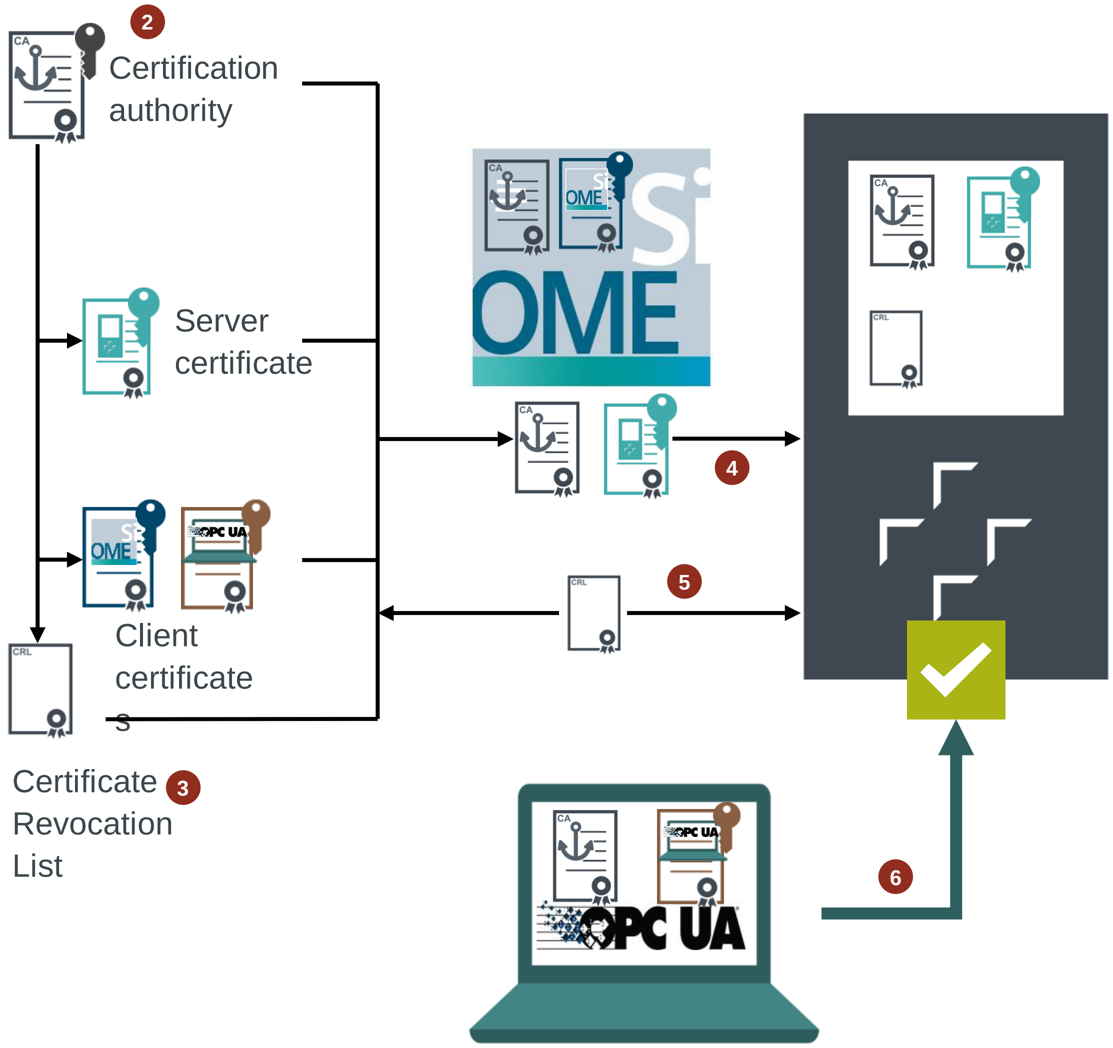
2.2 Overview

The engineering of the GDS push certificate management in this example is divided into several steps, which are explained in detail in the corresponding chapters, and each is verified with an access test.

Engineering and testing access

1. Initial configuration of the S7-1500 CPU in TIA Portal
   By the end of this step, the S7-1500 CPU will be in "Provisioning state" (see chapter 2.3)
2. Generate private keys and certificates for CA, GDS client "SiOME" and OPC UA client "UA Expert" (see chapter 2.4.2)
3. Generate empty Certificate Revocation List (CLR) (see chapter 2.4.2)
4. Load Certificate Trust List and Certificate Revocation List into the S7-1500 CPU via "SiOME" (see chapter 2.4.3 and 2.4.4)
5. Activate request of a new server certificate via the S7-1500 CPU (OPC UA method call) (2.4.5)
   Engineering of the access and "Provisioning state" are complete. The S7-1500 CPU is in productive operation.
6. In this application example, the configuration is tested with the OPC UA client "UA Expert" using the generated certificate (see chapter 2.5).
   The OPC UA client "UA Expert" has access to the OPC UA server of the S7-1500 CPU.

Figure 2-2

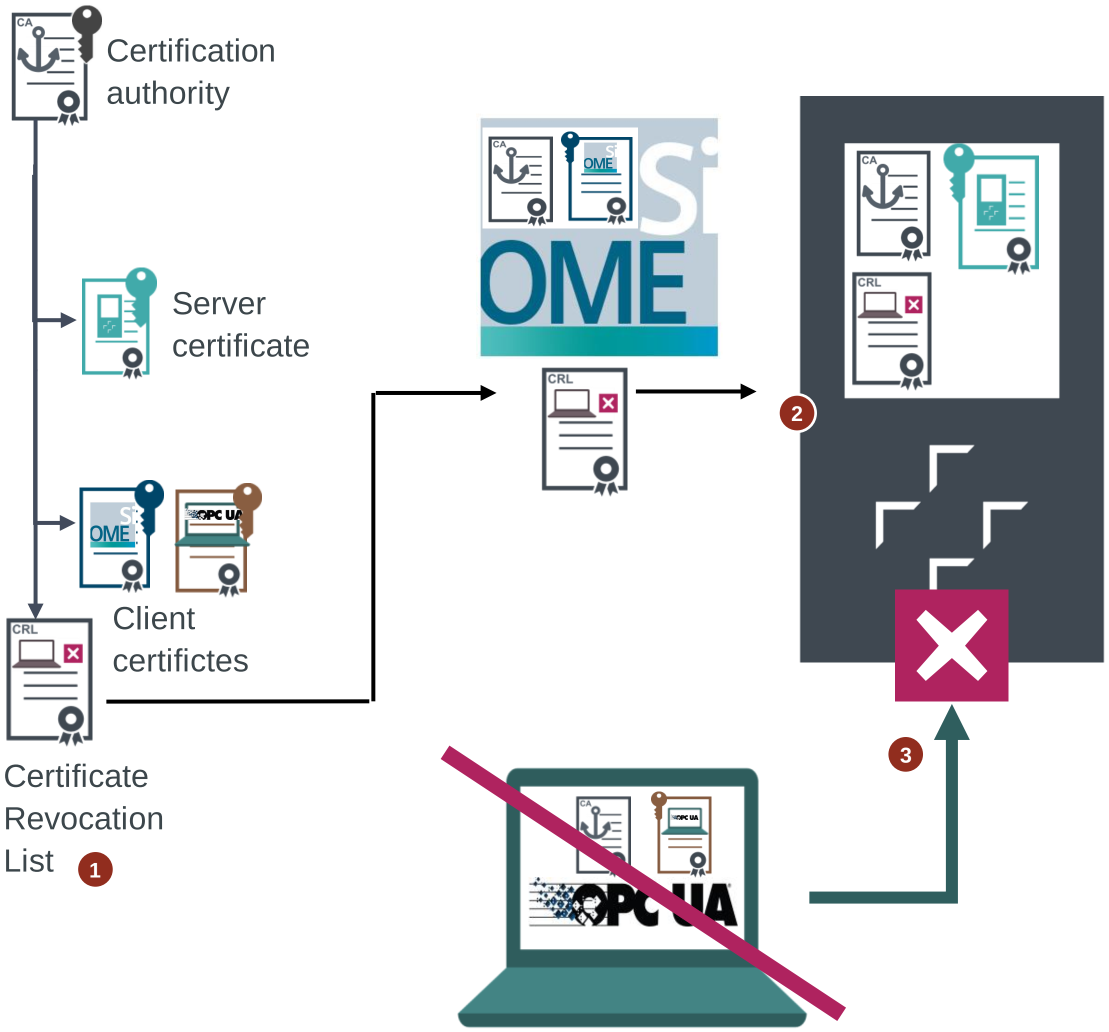


Engineering for rejecting access

The Certificate Revocation List is modified to prevent the OPC UA test client from accessing the CPU (see chapter 2.6).

1. Add certificate for the OPC UA client "UA Expert" to the Certificate Revocation List (see chapter 2.6.2)
2. Load the updated Certificate Revocation List into the S7-1500 CPU (see chapter 0)
3. In this application example, the configuration is tested with the OPC UA client "UA Expert" (see chapter 2.6.4).
   The OPC UA client "UA Expert" does not have access to the OPC UA server of the S7-1500 CPU.

Figure 2-3

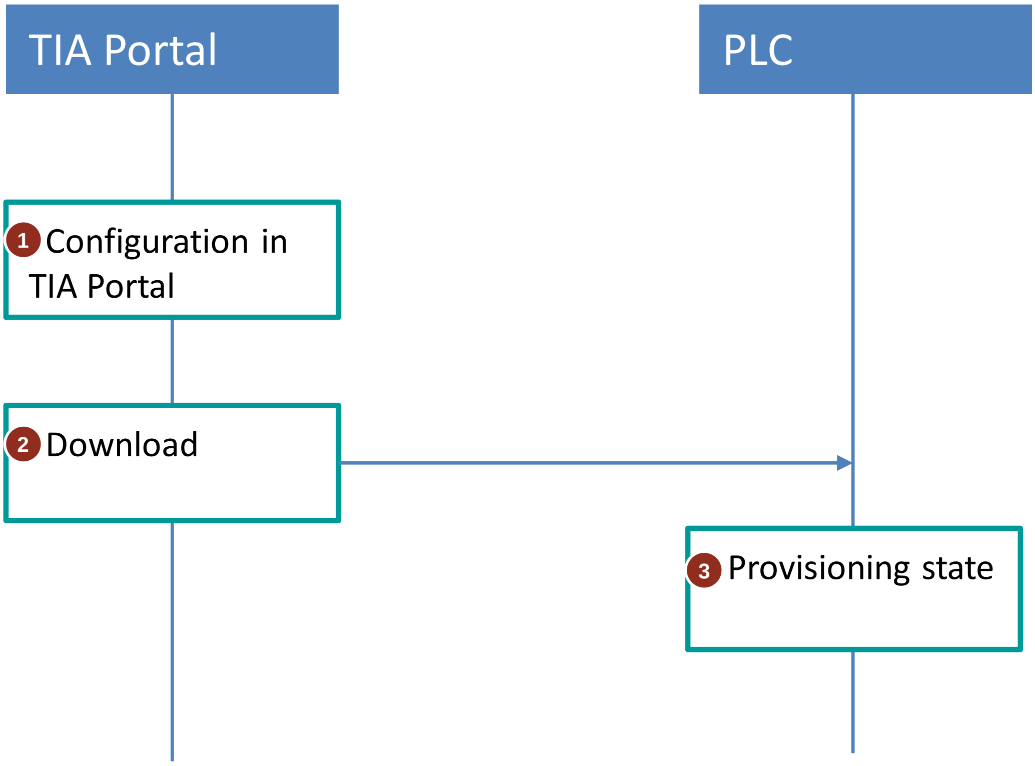


2.3 Configuring the S7-1500 CPU

2.3.1 Overview

The following graphic shows the actions and configuration steps which are relevant in this section.

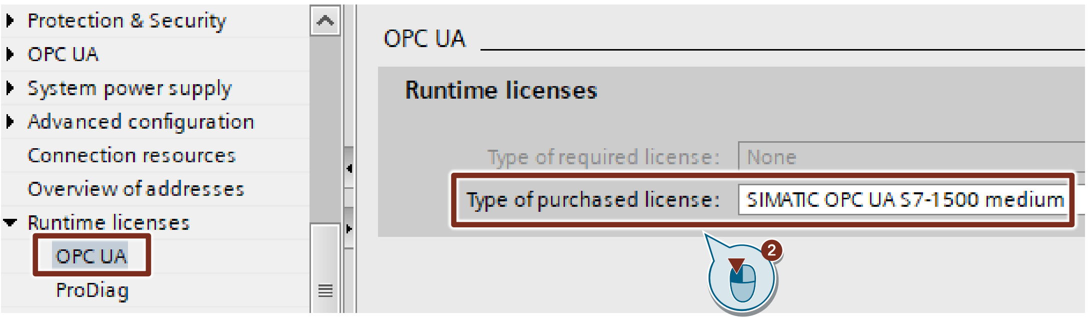
Figure 2-4



2.3.2 Configuration in TIA Portal

Activate the OPC UA server

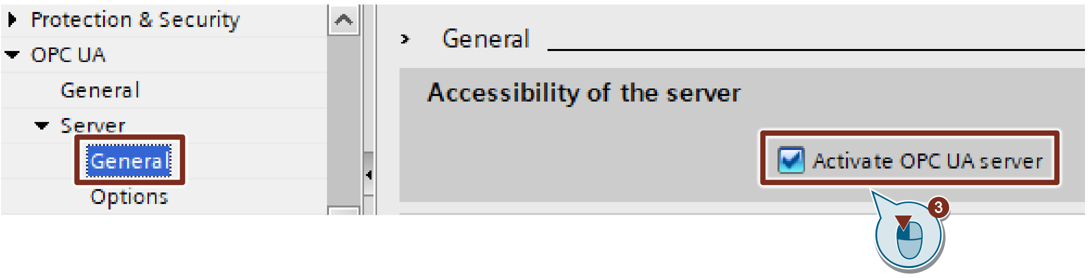
1. In TIA Portal, open the "Properties" of the configured S7-1500 CPU.
2. In the Inspector window, navigate to "Runtime licenses > OPC UA" and select the necessary license from there.



Type of required license: None

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

3. In the Inspector window, navigate to "OPC UA > Server > General" and activate the checkbox "Activate OPC UA server".



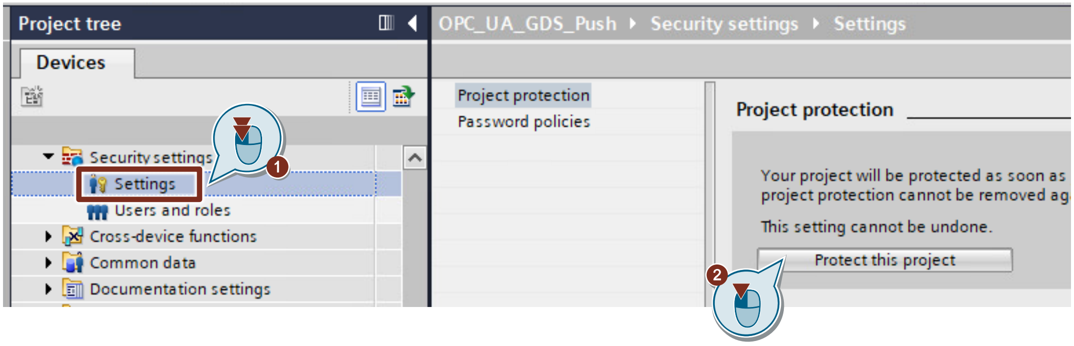
☑ Activate OPC UA server

The OPC UA Server has been activated.

Enable functionality for dynamic certificate management

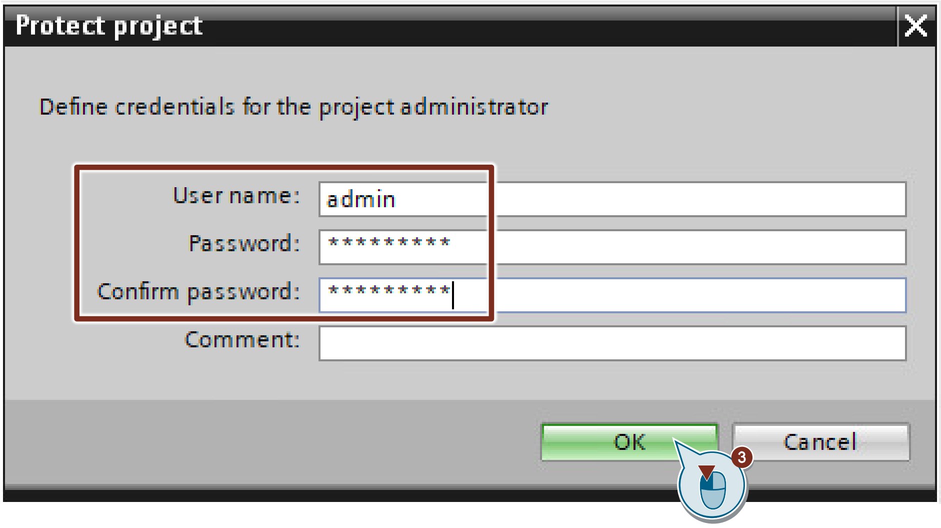
For security reasons, dynamic certificate management can only be enabled in protected projects.

1. In the project tree of the TIA Portal project, double-click on "Settings" in the "Security Settings" area.
2. Click the "Protect this project" button.



Your project will be protected as soon as
project protection cannot be removed ag
This setting cannot be undone.

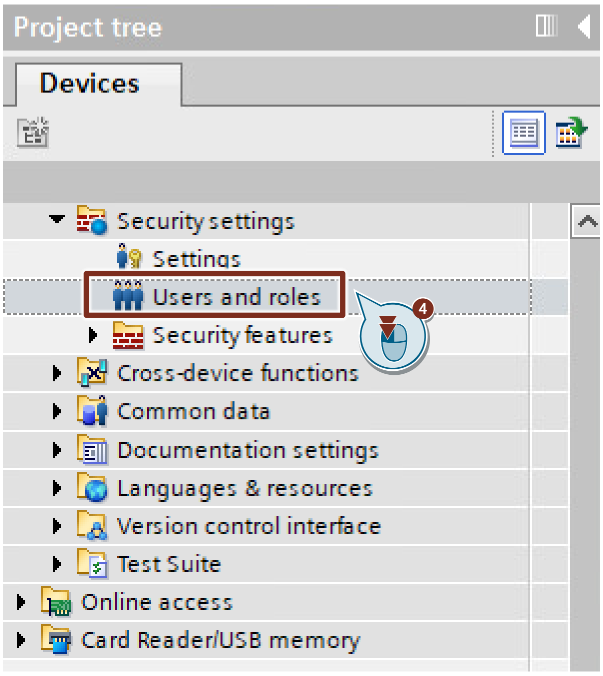
3. Enter a username and a password and then click the "OK" button.



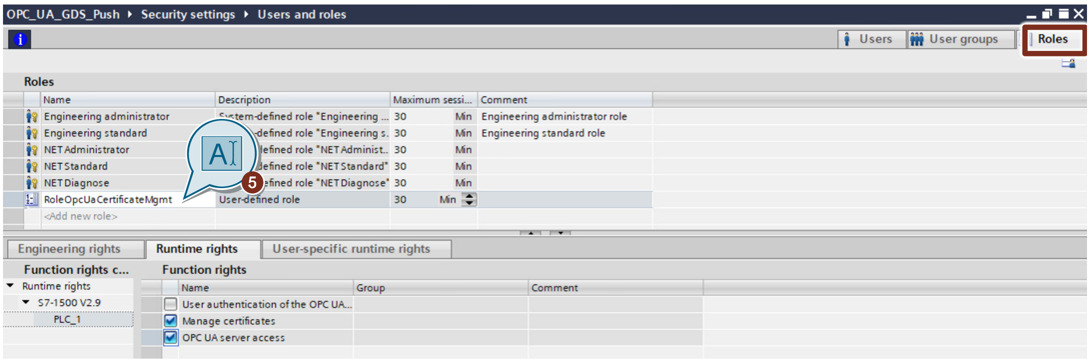
Define credentials for the project administrator

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

4. A user can only set certificates via OPC UA if that user has the permission to manage certificates. To create this user, double-click "Users and roles" in the "Security settings" area of the project tree.



5. Create a new role in the "Roles" tab.
   - Click "Add new role".
   - Enter a name for the role, such as "RoleOpcUaCertificateMgmt".



OPC_UA_GDS_Push ▸ Security settings ▸ Users and roles
Users
User groups
Roles
5
Engineering rights
Runtime rights
User-specific runtime rights

Roles

Name	Description	Maximum sessi...		Comment
Engineering administrator	System-defined role "Engineering ...	30	Min	Engineering administrator role
Engineering standard	-defined role "Engineering s.	30	Min	Engineering standard role
NET Administrator	defined role "NET Administ..	30	Min	
NET Standard	defined role "NET Standard"	30	Min	
NET Diagnose	efined role "NET Diagnose"	30	Min	
RoleOpcUaCertificateMgmt	User-defined role	30	Min	
<Add new role>				

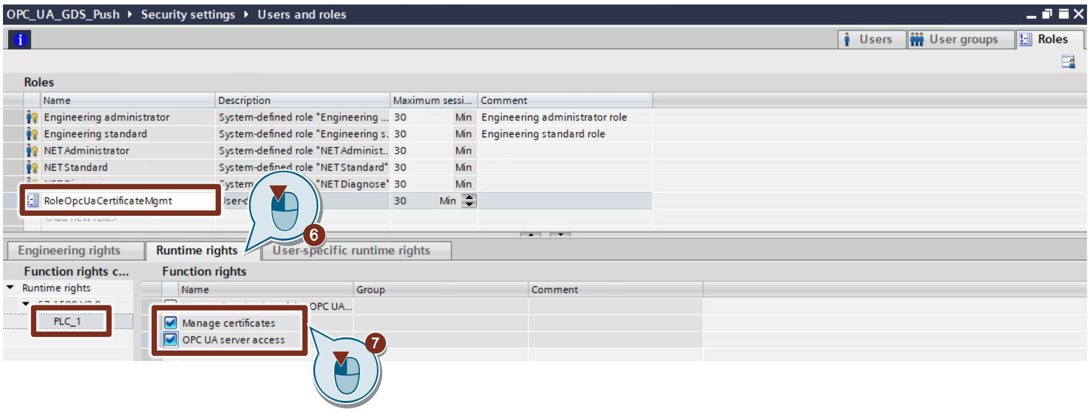
Function rights c...

- Runtime rights
  - S7-1500 V2.9
    - PLC_1

Function rights

	Name	Group	Comment
□	User authentication of the OPC UA...		
☑	Manage certificates		
☑	OPC UA server access		

6. Select the role you just created and open the "Runtime rights" tab in the lower pane.
7. Assign the following function rights:
   - "Manage certificates"
   - "OPC UA server access"



OPC_UA_GDS_Push ▸ Security settings ▸ Users and roles

Roles

Name	Description	Maximum sessi...		Comment
Engineering administrator	System-defined role "Engineering ...	30	Min	Engineering administrator role
Engineering standard	System-defined role "Engineering s.	30	Min	Engineering standard role
NET Administrator	System-defined role "NET Administ..	30	Min	
NET Standard	System-defined role "NET Standard"	30	Min	
	System "NET Diagnose"	30	Min	
RoleOpcUaCertificateMgmt	User-d	30	Min	

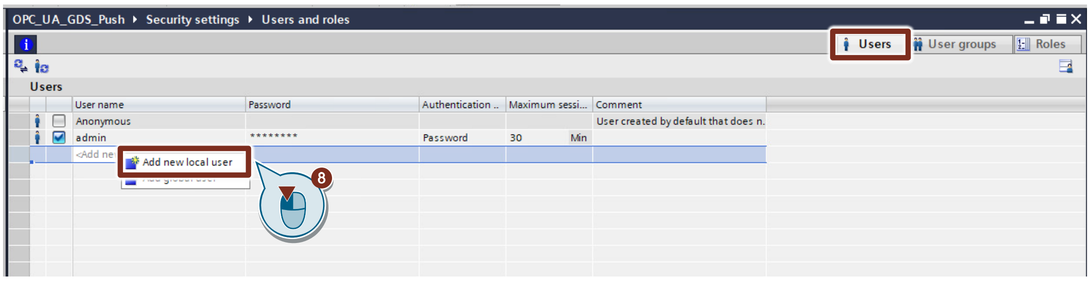
Function rights c...

- Runtime rights
  - PLC_1

Function rights

	Name	Group	Comment
		OPC UA...	
☑	Manage certificates		
☑	OPC UA server access		

8. In the "Users" tab, create a new local user.
   - Click "Add new user".
     A submenu will open where you can select the user type.
   - Click "Add new local user".

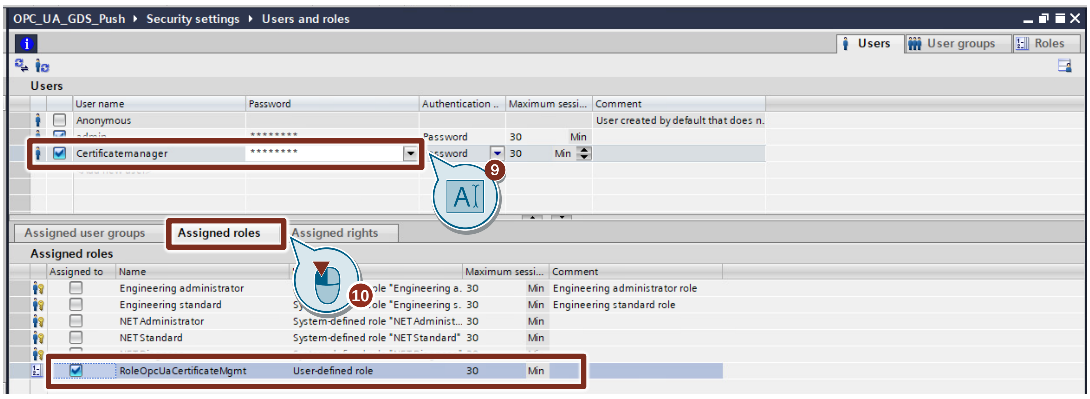


OPC_UA_GDS_Push ▸ Security settings ▸ Users and roles

Users

	User name	Password	Authentication ..	Maximum sessi...		Comment
☐	Anonymous					User created by default that does n.
☑	admin	********	Password	30	Min	
	<Add ne					

9. Assign a username and a password and select the newly created user.
10. In the lower pane, open the "Assigned roles" tab to link the user with the role created earlier.
    This user now has the necessary rights to connect with the CPU and manage certificates.



OPC_UA_GDS_Push ▸ Security settings ▸ Users and roles

Users

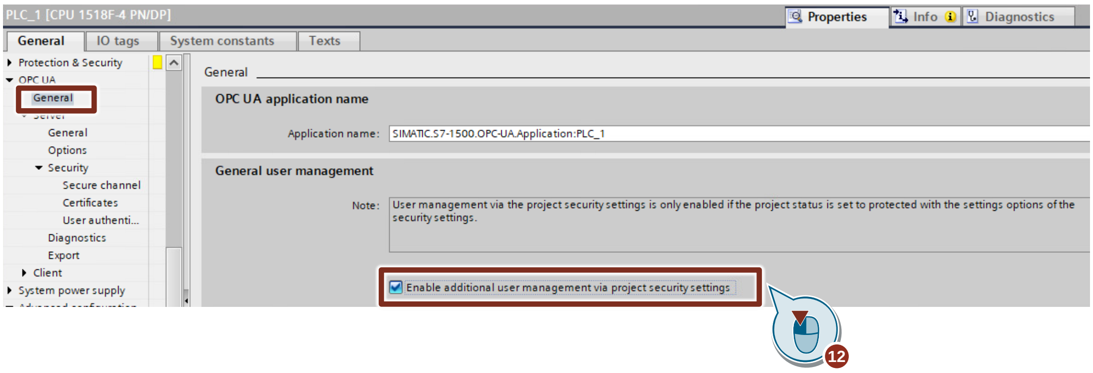
	User name	Password	Authentication ..	Maximum sessi...		Comment
☐	Anonymous					User created by default that does n.
☑	admin	********	Password	30	Min	
☑	Certificatemanager	********	Password	30	Min	

Assigned roles

Assigned to	Name		Maximum sessi...		Comment
☐	Engineering administrator	ole "Engineering a.	30	Min	Engineering administrator role
☐	Engineering standard	Sy ole "Engineering s.	30	Min	Engineering standard role
☐	NET Administrator	System-defined role "NET Administ...	30	Min	
☐	NET Standard	System-defined role "NET Standard"	30	Min	
☐					
☑	RoleOpcUaCertificateMgmt	User-defined role	30	Min	

11. The user created in the "Security settings" is currently still a global user, which cannot be used on the CPU. To use this user for the OPC UA server of the S7-1500 CPU, open the "Properties" of the configured S7-1500 CPU.

12. In the Inspector window, navigate to "OPC UA > General" and activate the function "Enable additional user management via project security settings".



PLC_1 [CPU 1518F-4 PN/DP]

General

OPC UA application name

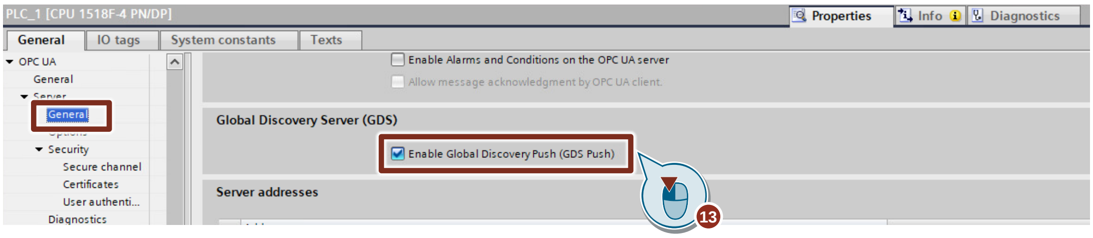
Application name: SIMATIC.S7-1500.OPC-UA.Application:PLC_1

General user management

Note: User management via the project security settings is only enabled if the project status is set to protected with the settings options of the security settings.

☑ Enable additional user management via project security settings

13. Navigate to "OPC UA > Server > General" and activate the function "Enable Global Discovery Push (GDS Push)". In this way you will have enabled dynamic certificate management for the OPC UA server.



PLC_1 [CPU 1518F-4 PN/DP]

□ Enable Alarms and Conditions on the OPC UA server

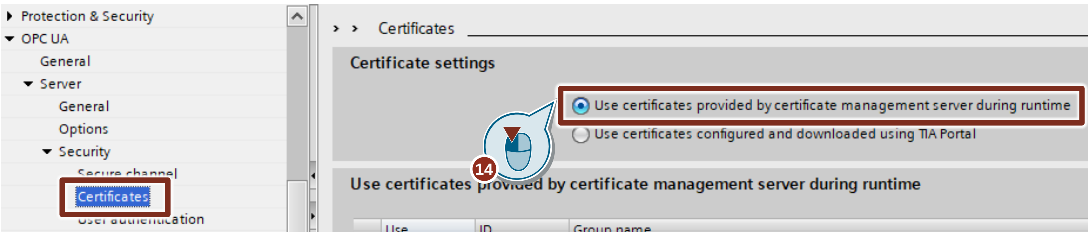
□ Allow message acknowledgment by OPC UA client.

Global Discovery Server (GDS)

☑ Enable Global Discovery Push (GDS Push)

Server addresses

14. Navigate to "OPC UA > Server >Security > Certificates". Activate the function "Use certificates provided by certificate management server during runtime".



Certificates

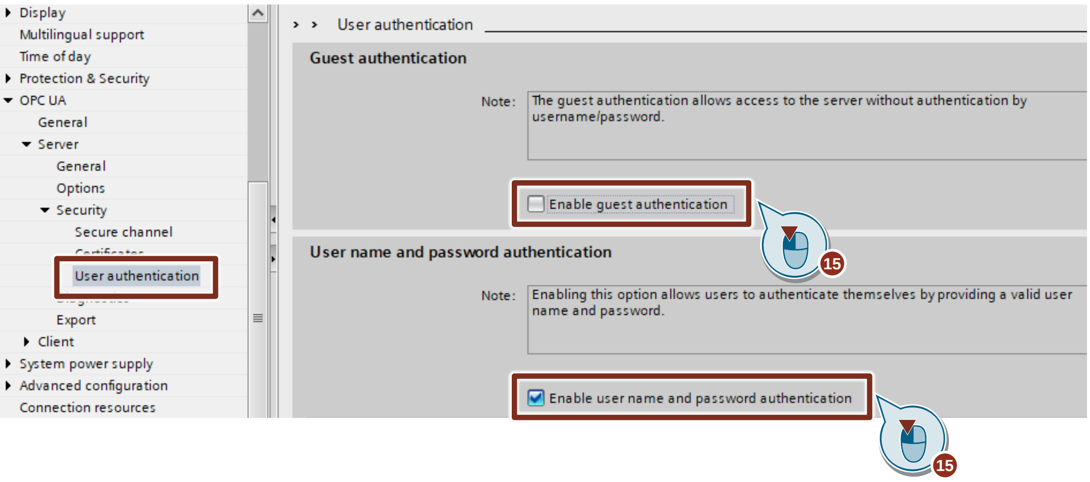
Certificate settings

● Use certificates provided by certificate management server during runtime

○ Use certificates configured and downloaded using TIA Portal

Use certificates provided by certificate management server during runtime

15. Navigate to "OPC UA > Server >Security > User authentication" and make the following settings:
    - Disable the function "Enable Guest Authentication".
    - Activate the function "Enable user name and password authentication".



Guest authentication

Note: The guest authentication allows access to the server without authentication by username/password.

□ Enable guest authentication

User name and password authentication

Note: Enabling this option allows users to authenticate themselves by providing a valid user name and password.

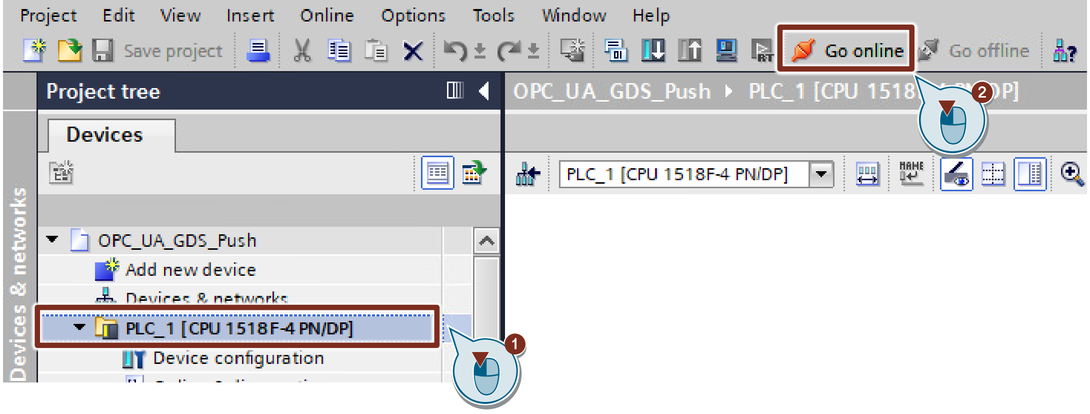
☑ Enable user name and password authentication

The functionality for dynamic certificate management is now enabled.

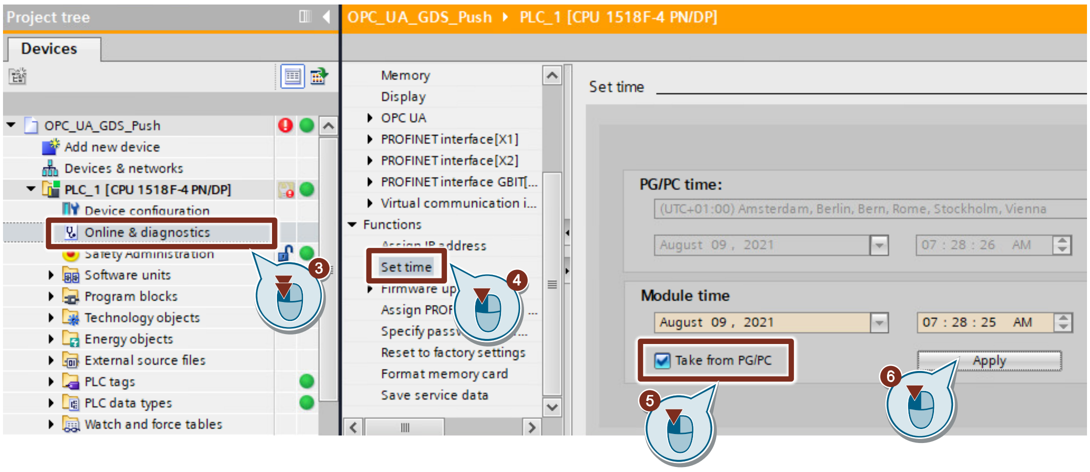
Set the time in the CPU

When working with certificates, it is important that the times in all devices in the system are set correctly and synchronized.

1. In the project tree, select the device folder of the CPU.
2. In the function bar, click the "Go online" button.



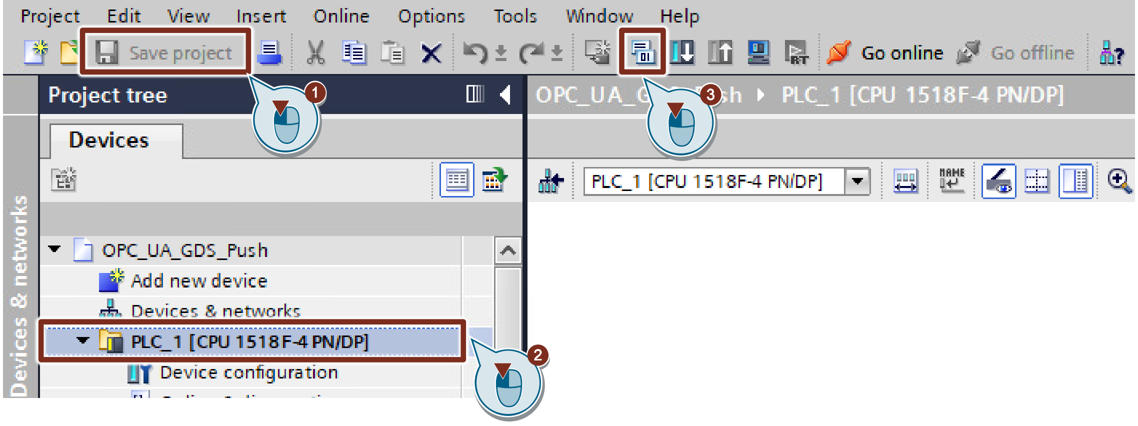
3. In the project tree, double-click on "Online & diagnostics" in the device folder of the CPU. The "Online & diagnostics" dialog will open.
4. Navigate to "Functions > Set Time".
5. Set the time in the module by activating the "Take from PG/PC" checkbox.
6. Save your settings with "Apply".



Save and compile the project

1. Save the project.
2. In the project tree, select the device folder of the CPU.
3. Click on the "Compile" button in the function bar.

Figure 2-5

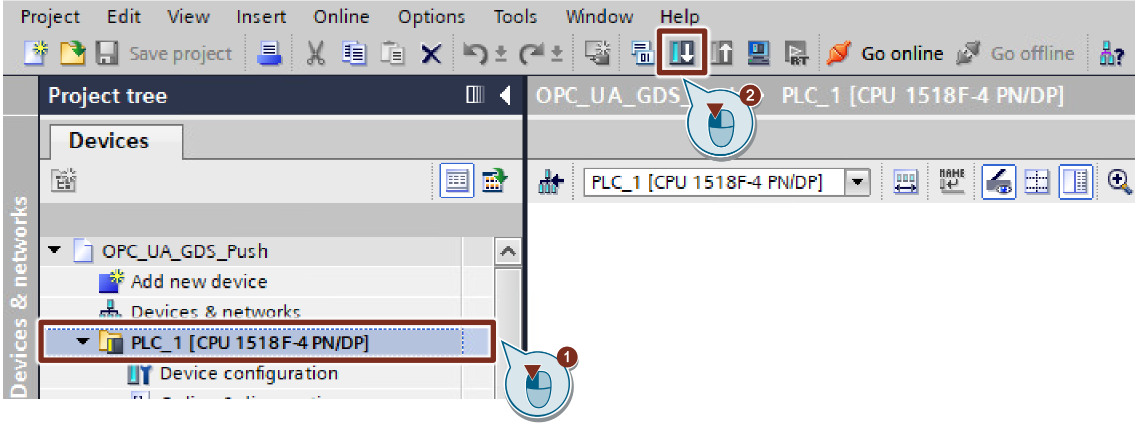


The configuration in TIA Portal will have been completed successfully once the project has compiled with no errors.

2.3.3 Download configuration to the CPU

1. In the project tree, select the device folder of the CPU.
2. Click on the "Download to device" button in the function bar.

Figure 2-6



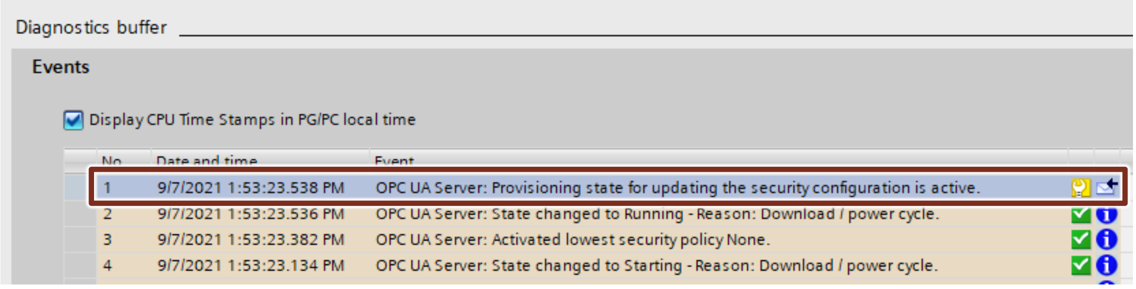
The download process will initialize and be executed.

2.3.4 "Provisioning state"

Once you have successfully completed the configuration in TIA Portal and downloaded the configuration to the CPU, the CPU will be in "Provisioning state".

The "provisioning state" will be displayed in the CPU's diagnostic buffer via an incoming message, and the MAINT LED of the CPU will illuminate yellow.

Figure 2-7


Diagnostics buffer

Events

☑ Display CPU Time Stamps in PG/PC local time

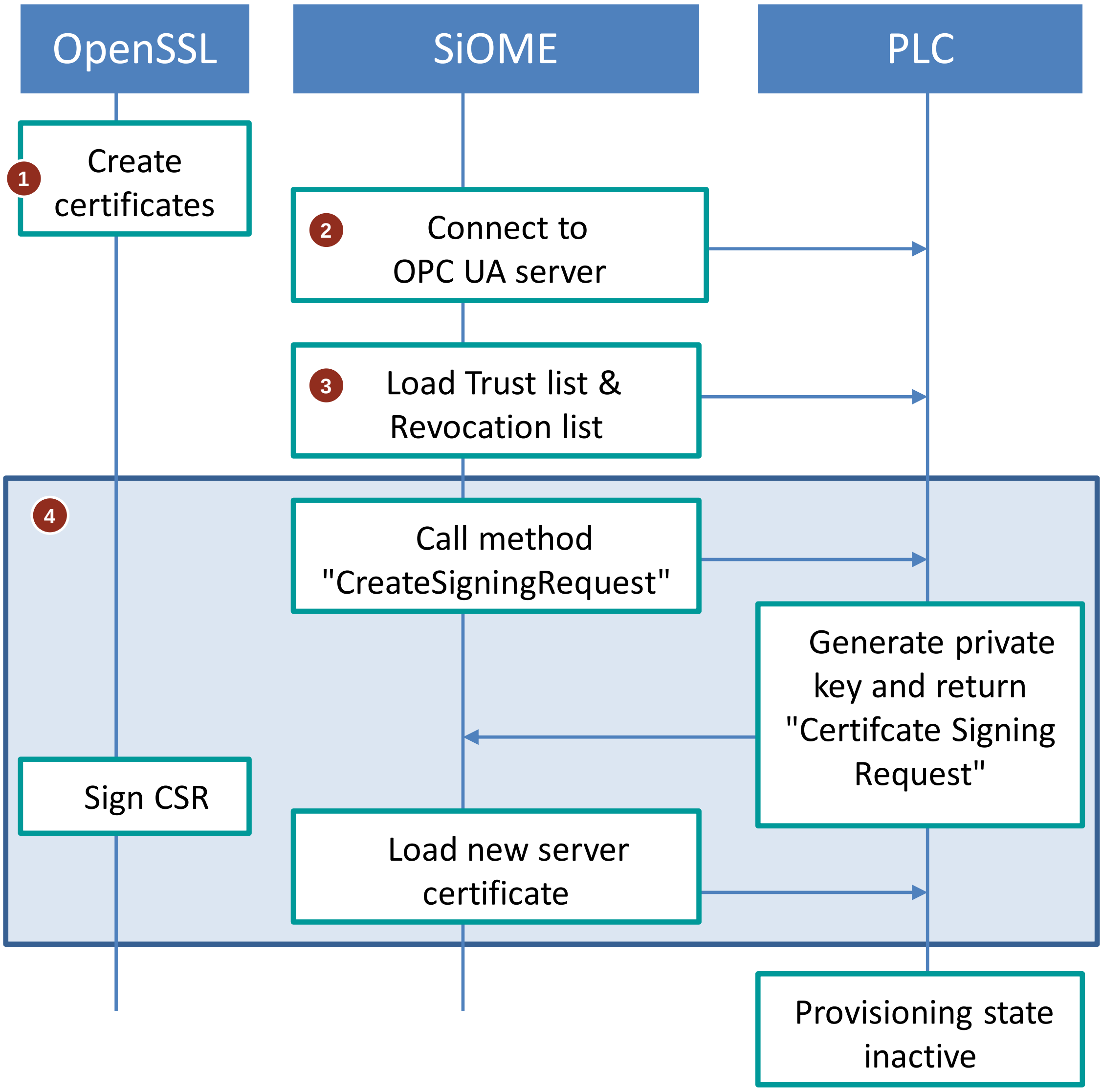
No.	Date and time	Event
1	9/7/2021 1:53:23.538 PM	OPC UA Server: Provisioning state for updating the security configuration is active.
2	9/7/2021 1:53:23.536 PM	OPC UA Server: State changed to Running - Reason: Download / power cycle.
3	9/7/2021 1:53:23.382 PM	OPC UA Server: Activated lowest security policy None.
4	9/7/2021 1:53:23.134 PM	OPC UA Server: State changed to Starting - Reason: Download / power cycle.

2.4 Actions and configuration steps with OpenSSL and "SiOME"

2.4.1 Overview

The following graphic shows the actions and configuration steps which are relevant in this section and the following sections.

Figure 2-8


OpenSSL
SiOME
PLC
1
Create certificates
2
Connect to OPC UA server
3
Load Trust list & Revocation list
4
Call method "CreateSigningRequest"
Generate private key and return "Certifcate Signing Request"
Sign CSR
Load new server certificate
Provisioning state inactive

1. Create certificates with OpenSSL (see chapter 2.4.2):
   - Generate private key for Certification Authority (CA)
   - Create certificate for CA
   - Generate private keys for client certificates ("SiOME" and "UA Expert")
   - Create client certificates for "SiOME" and "UA Expert"
   - Create empty Certificate Revocation List
2. Connect "SiOME" as OPC UA client with the OPC UA server of the S7-1500 CPU (see chapter 2.4.3)

3. Load Certificate Trust List from "SiOME" into the S7-1500 CPU (see chapter 2.4.4)

NOTE The Certificate Revocation List is loaded as part of the Certificate Trust List.

4. Replace server certificate of the OPC UA server (see chapter 2.4.5)
   - The OPC UA method "CreateSigningRequest" is called in the CPU via the "SiOME" interface.
   - When the method is called, the CPU starts generating a new private key. Accordingly, the CPU creates a "CertificateSigningRequest" which is returned to the OPC UA client as a return value from "SiOME".
   - The "CertificateSigningRequest" is signed by the CA by means of OpenSSL. This turns the "CertificateSigningRequest" into a valid server certificate for the CPU's OPC UA server.
   - The server certificate is loaded to the CPU via the "SiOME" interface. This replaces the temporary server certificate.

"Provisioning state" is exited if the following conditions are met:

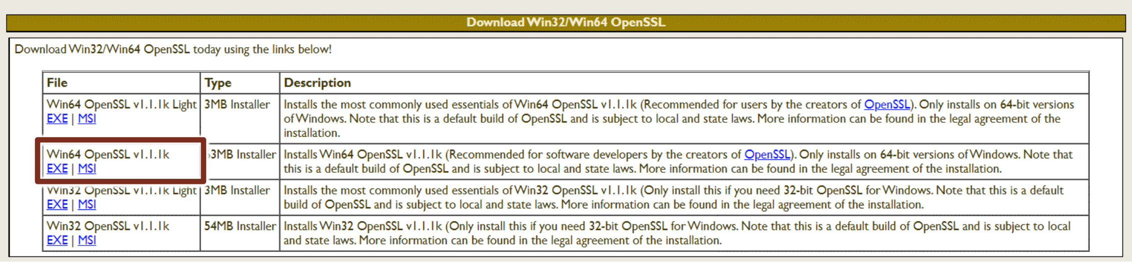
- The Certificate Trust List has been loaded into the S7-1500 CPU.
- The server certificate has been replaced.

When the S7-1500 CPU has left "Provisioning state", now only clients can establish a connection to the OPC UA server of the S7-1500 CPU in which a trust relationship exists.

Install and start OpenSSL

The OpenSSL installation is freely available and can be downloaded from several websites.

Figure 2-9



Download Win32/Win64 OpenSSL

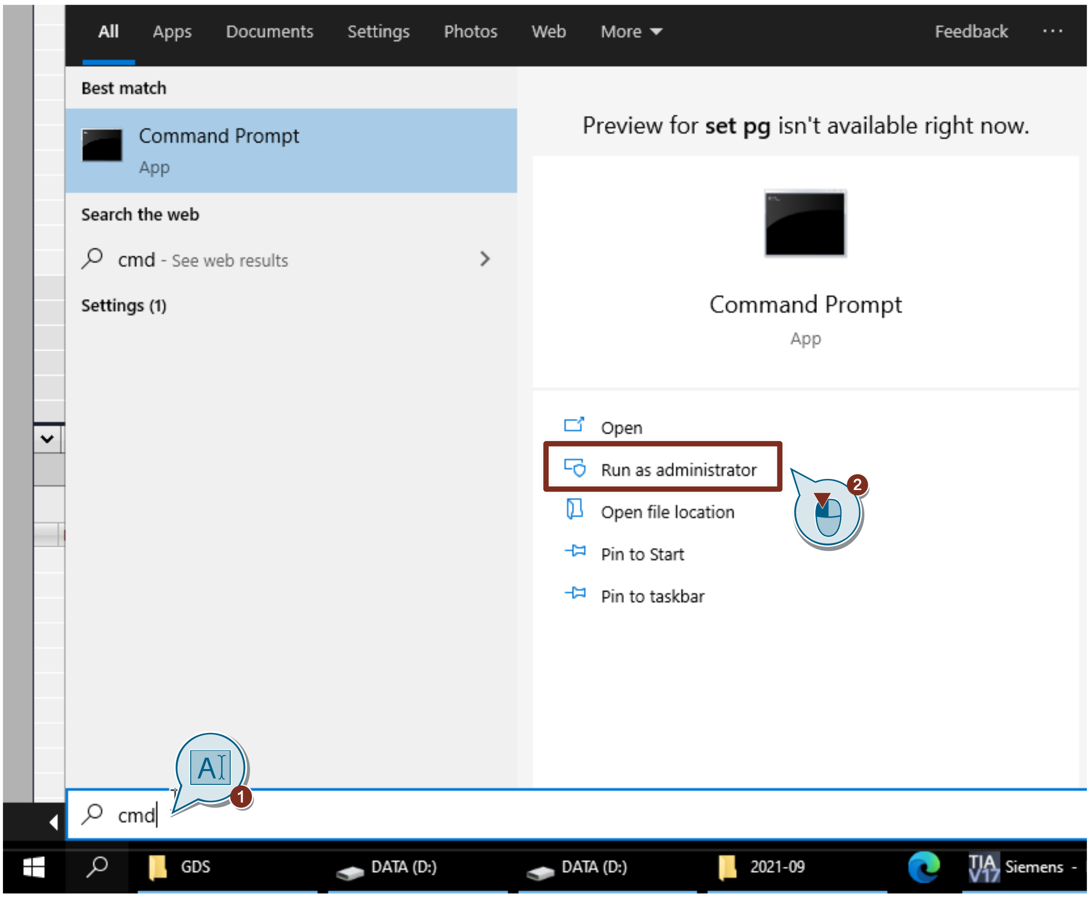
Download Win32/Win64 OpenSSL today using the links below!

File	Type	Description
Win64 OpenSSL v1.1.1k Light EXE | MSI	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1k (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.1k EXE | MSI	3MB Installer	Installs Win64 OpenSSL v1.1.1k (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1k Light EXE | MSI	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1k (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1k EXE | MSI	54MB Installer	Installs Win32 OpenSSL v1.1.1k (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

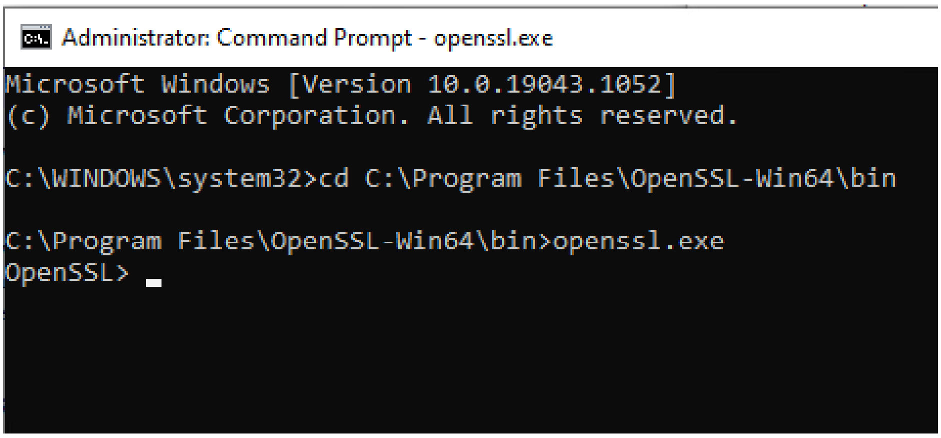
Install to the path: "C:\Program Files\OpenSSL-Win64\".

Start OpenSSL in the "Command Prompt". Proceed according to the instructions below:

1. Enter "cmd" into the Windows search.
2. Run the "Command Prompt" as an administrator.



3. Use the command below to switch to the path where the OpenSSL.exe file is located:
`cd C:\Program Files\OpenSSL-Win64\bin`
4. Launch OpenSSL with the following command:
`openssl.exe`

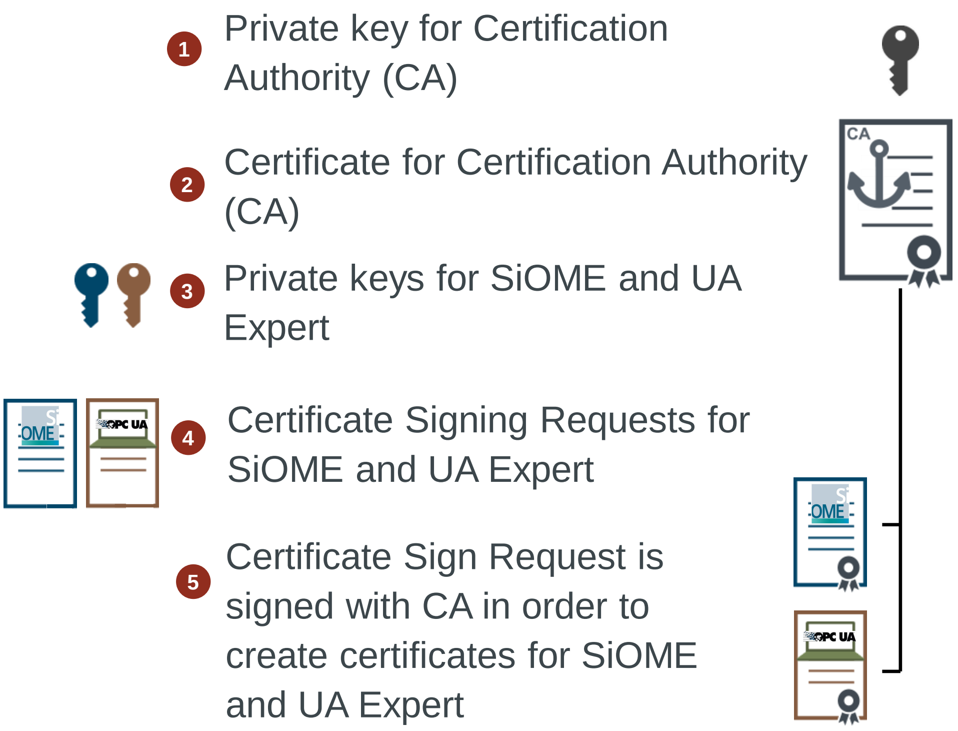

Administrator: Command Prompt - openssl.exe

```
Microsoft Windows [Version 10.0.19043.1052]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> _
```

2.4.2 Creating certificates with OpenSSL

The following section demonstrates how to create the necessary certificates for this application example with the help of OpenSSL, as we will not use a GDS server.

Figure 2-10



1 Private key for Certification Authority (CA)

2 Certificate for Certification Authority (CA)

3 Private keys for SiOME and UA Expert

4 Certificate Signing Requests for SiOME and UA Expert

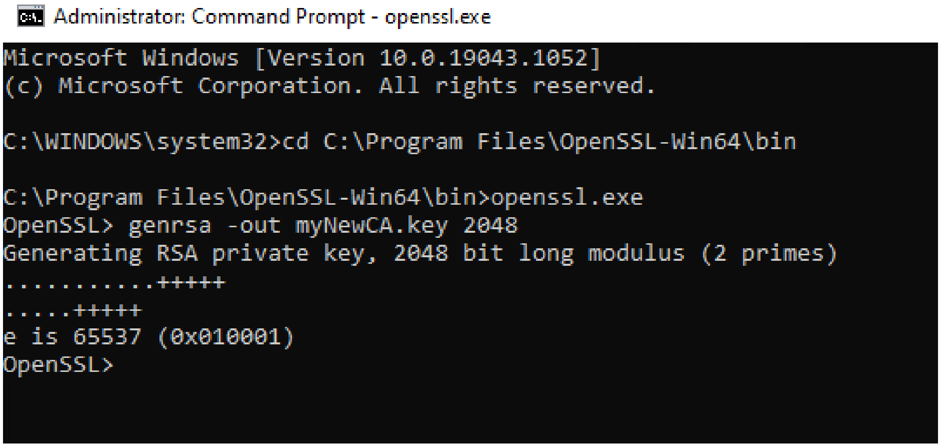
5 Certificate Sign Request is signed with CA in order to create certificates for SiOME and UA Expert

If your IT department has already provided you with certificates, you can skip this step and proceed directly to chapter 2.4.3 and load the existing certificates to the S7-1500 CPU.

Generate private key and create certificate for CA

Create a root certificate with the associated private key for the CA.

1. To generate the private key, enter the following command:
   `genrsa -out myNewCA.key 2048`



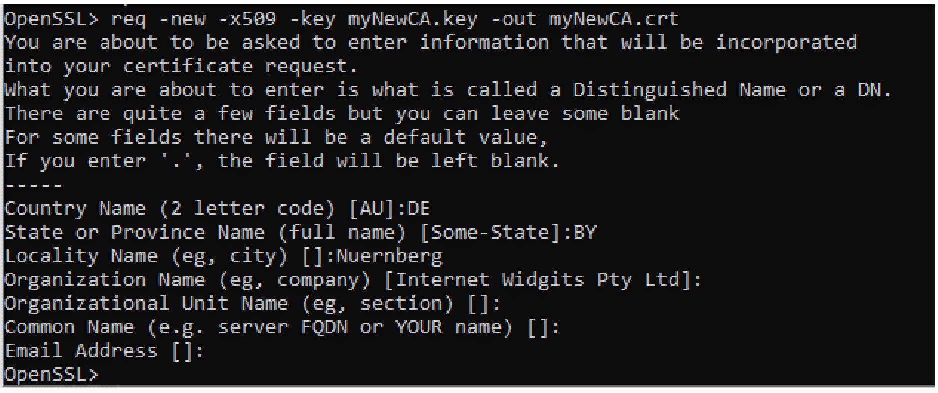
Administrator: Command Prompt - openssl.exe

```
Microsoft Windows [Version 10.0.19043.1052]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> genrsa -out myNewCA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...........+++++
.....+++++
e is 65537 (0x010001)
OpenSSL>
```

   You will generate a 2048-bit RSA key. You can choose any name you like for the key.
   Note the "*.key" file extension.
   The new key can be found in the folder "C:\Program Files\OpenSSL-Win64\bin".

2. Use the new key to create a certificate for the CA. Enter the following command:
   `req -new -x509 -key myNewCa.key -out myNewCA.crt`
   You can choose any name for the new certificate.
   Note the "*.crt" file extension. After the "-key" option, the key generated in the previous step must be entered.

3. To create the key, you will be prompted to specify information that will be carried over to the certificate.
   Enter at least the country. Other data are optional.
   The new "*.crt" file can be found in the folder "C:\Program Files\OpenSSL-Win64\bin".



```
OpenSSL> req -new -x509 -key myNewCA.key -out myNewCA.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:BY
Locality Name (eg, city) []:Nuernberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
OpenSSL>
```

4. To be able to later reuse the root certificate of the CA, the "*.der" format is necessary.
   Enter the following command for the conversion:
   `x509 -outform der -in myNewCA.crt -out myNewCA.der`
   The "myNewCA.der" certificate can be found in the folder "C:\Program Files\OpenSSL-Win64\bin". You can choose any name.

You have created the following files:

- the private key ("*.key")
- the certificate for your own CA ("*.crt", "*.der")

Generate private key and generate client certificate for "SiOME" and "UA Expert"

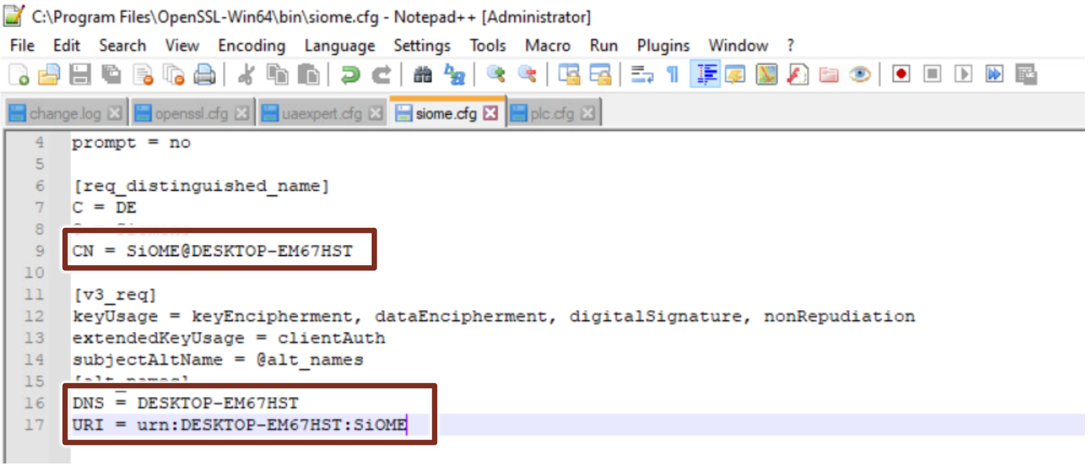
In this application example, you will create the client certificate and the associated private key for the following client applications:

- "SiOME":
  The certificates are loaded to the S7-1500 CPU with the "SiOME" GDS Push View.
- "UA Expert"
  You will use the OPC UA client "UA Expert" to test your configuration.

For the OPC UA server to accept the client certificates, it is necessary to define some attributes with OpenSSL. You can use the "*.cfg" files included in this download to set the attributes. The attributes are already set in the "*.cfg" files for the systems; they will be carried over to the certificates when OpenSSL is used.

The Figure in Step 1 shows, for example, the value for the "Common Name" (CN) in the certificate for "SiOME".

1. Open the "siome.cfg" file for "SiOME" with an ASCII text editor and modify the configuration:
   - Replace the PC name "DESKTOP-EM67HST" with the name of the PC that is running your client application.

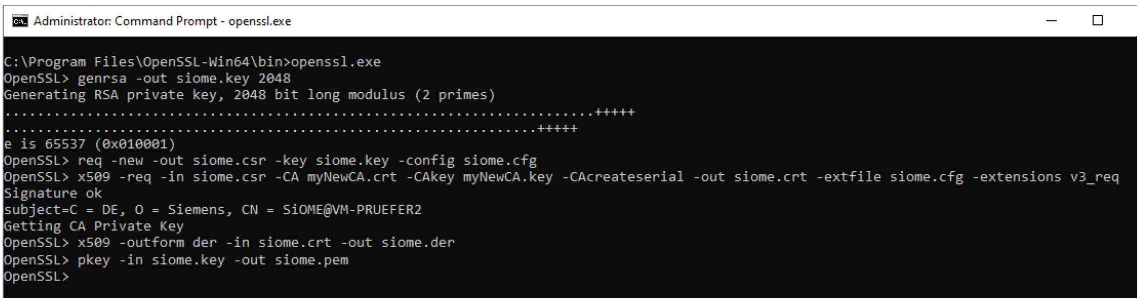

C:\Program Files\OpenSSL-Win64\bin\siome.cfg - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
openssl.cfg
uaexpert.cfg
siome.cfg
plc.cfg

```
prompt = no

[req_distinguished_name]
C = DE
O = Siemens
CN = SiOME@DESKTOP-EM67HST

[v3_req]
keyUsage = keyEncipherment, dataEncipherment, digitalSignature, nonRepudiation
extendedKeyUsage = clientAuth
subjectAltName = @alt_names
[alt_names]
DNS = DESKTOP-EM67HST
URI = urn:DESKTOP-EM67HST:SiOME
```

2. Open the "uaexpert.cfg" file for "UA Expert" with an ASCII text editor and modify the configuration:
   - Replace the PC name "DESKTOP-EM67HST" with the name of the PC that is running your client application.
   - You can use an OPC UA client of your choosing. If you are using an OPC UA client other than "UA Expert", then replace the application name.
3. Generate a new RSA key for the client application "SiOME".
   `genrsa -out siome.key 2048`
4. The client certificate must be signed by the CA. Therefore, it cannot be created directly. To create a client certificate from a CA with OpenSSL, it is necessary to create a "Certificate Signing Request".
   `req -new -out siome.csr -key siome.key -config siome.cfg`
5. The "Certificate Signing Request" is signed by the CA to obtain the certificate for the OPC UA client.
   `x509 -req -in siome.csr -CA myNewCA.crt -CAkey myNewCA.key -CAcreateserial -out siome.crt -extfile siome.cfg -extensions v3_req`
   For the files "siome.csr", "myNewCA.crt" and "myNewCA.key", use the files that you created in the previous steps. The extensions "-extfile" and "-extensions" are important so that the parameters "SubjectAlternativeName" and "KeyUsage" match in the certificate.

6. The "Certificate Signing Request" is no longer needed once the certificate is generated. The certificate and the key are necessary for the connection with the client. The certificate must be in the "*.der" file format and the private key must be in the "*.pem" file format.
   - Convert the certificate with the following command.
     `x509 -outform der -in siome.crt -out siome.der`
   - Convert the private key with the following command.
     `pkey -in siome.key -out siome.pem`
7. Proceed in the same manner for the certificate of the OPC UA client "UA Expert". Assign new file names and use the file "uaexpert.cfg" or modify the file "siome.cfg".

Figure 2-11



```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> genrsa -out siome.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.......................................................................+++++
.................................................................+++++
e is 65537 (0x010001)
OpenSSL> req -new -out siome.csr -key siome.key -config siome.cfg
OpenSSL> x509 -req -in siome.csr -CA myNewCA.crt -CAkey myNewCA.key -CAcreateserial -out siome.crt -extfile siome.cfg -extensions v3_req
Signature ok
subject=C = DE, O = Siemens, CN = SiOME@VM-PRUEFER2
Getting CA Private Key
OpenSSL> x509 -outform der -in siome.crt -out siome.der
OpenSSL> pkey -in siome.key -out siome.pem
OpenSSL>
```

You have created the following files for each client:

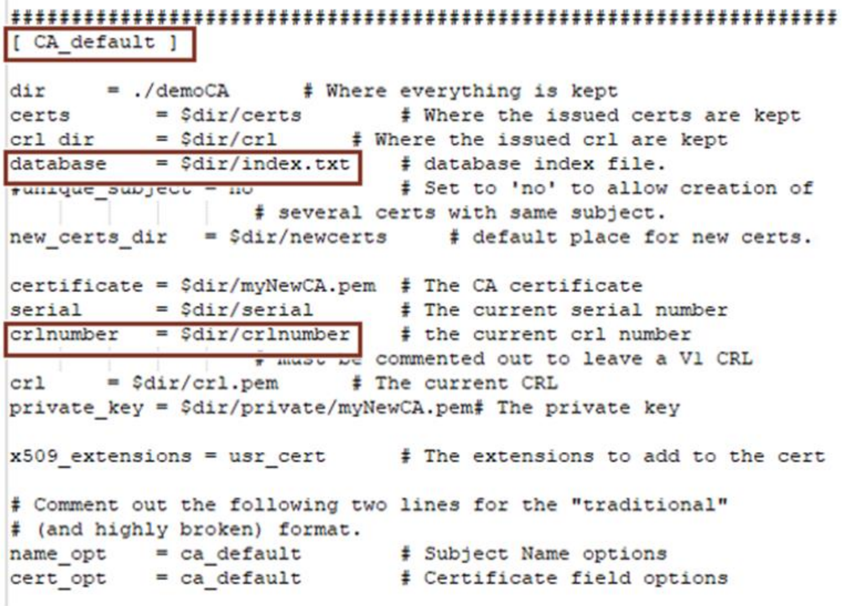
- the private key ("*.key", "*.pem")
- a "Certificate Signing Request" ("*.csr")
- the certificate ("*.crt", "*.der")

Create the Certificate Revocation List

If a CA certificate is added to the list of trusted clients (Certificate Trust List, CTL) for the OPC UA server of the S7-1500 CPU, then a Certificate Revocation List for this CA must also be added. Individual client certificates for a CA can be revoked in the Certificate Revocation List. This list can be exported from OpenSSL to various file formats. SiOME requires the "*.der" file format.

In this example, the Certificate Revocation List will initially remain empty, i. e. no CA certificates will be revoked.

1. In the folder "C\Program Files\OpenSSL-Win64\bin", search for the file "OpenSSL.cfg" and open it in an ASCII text editor. This file contains the general configuration options for your OpenSSL installation.
2. Look for the section entitled "[CA_default]" and the entries "database" and "crlnumber" below it.



```
####################################################################
[ CA_default ]

dir     = ./demoCA      # Where everything is kept
certs       = $dir/certs        # Where the issued certs are kept
crl_dir     = $dir/crl      # Where the issued crl are kept
database    = $dir/index.txt    # database index file.
#unique_subject = no           # Set to 'no' to allow creation of
                    # several certs with same subject.
new_certs_dir   = $dir/newcerts     # default place for new certs.

certificate = $dir/myNewCA.pem  # The CA certificate
serial      = $dir/serial       # The current serial number
crlnumber   = $dir/crlnumber    # the current crl number
                    # must be commented out to leave a V1 CRL
crl     = $dir/crl.pem      # The current CRL
private_key = $dir/private/myNewCA.pem# The private key

x509_extensions = usr_cert      # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt    = ca_default        # Subject Name options
cert_opt    = ca_default        # Certificate field options
```

3. Check what path the entries point to.
   In the example here, $dir is: "C\Program Files\OpenSSL-Win64\bin\demoCA".
   If this folder does not exist, create it now.
   If the files "index.txt" and "crlnumber" don't yet exist, create them as well. Create the file "crlnumber" without a file extension.
   Write "00" in the "crlnumber" file.
   You can leave the "index.txt" file empty.

   Now create a new, empty Certificate Revocation List.
   ```
   ca -gencrl -keyfile myNewCA.key -cert myNewCA.crt -out
   emptylist.pem
   ```
   The new, empty Certificate Revocation List can be found in the folder "C:\Program Files\OpenSSL-Win64\bin" with the name "emptylist.pem".
4. To load the Certificate Revocation List to the S7-1500 CPU with SiOME, the "*.der" file format is necessary.
   Convert the list to the "*.pem" format.
   ```
   crl -outform der -in emptylist.pem -out emptylist.der
   ```

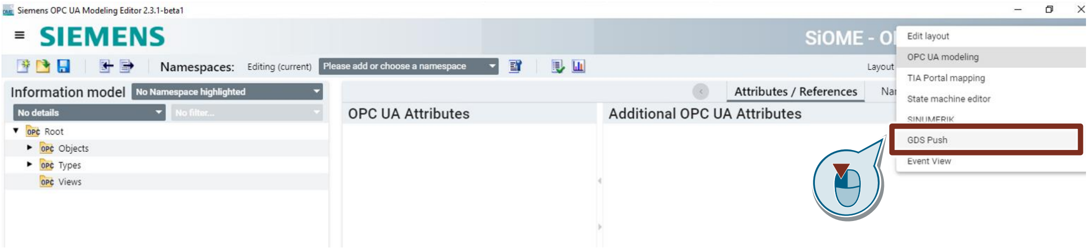
2.4.3 Connecting "SiOME" as an OPC UA client with the OPC UA server of the S7-1500 CPU

The certificates you created are loaded to the S7-1500 CPU with the help of the GDS Push plugin in "SiOME". This is part of the initial commissioning of the S7-1500 CPU, once dynamic certificate management has been enabled.

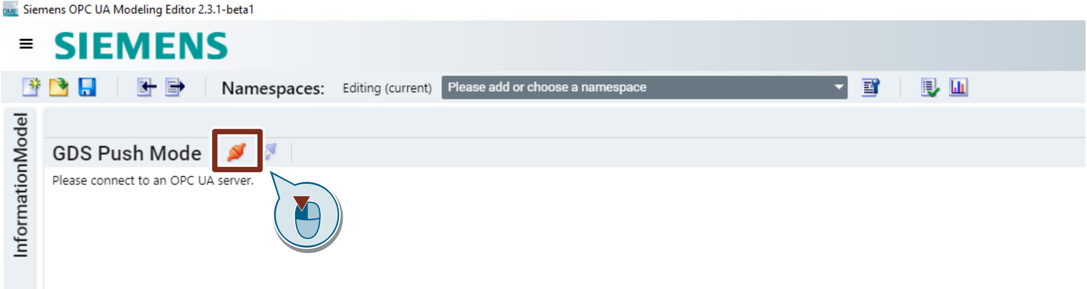
If all client certificates are present, then a connection to the OPC UA server of the S7-1500 CPU can be established.

The certificates are now initialized. The OPC UA server of the S7-1500 CPU can exits its "Provisioning state".

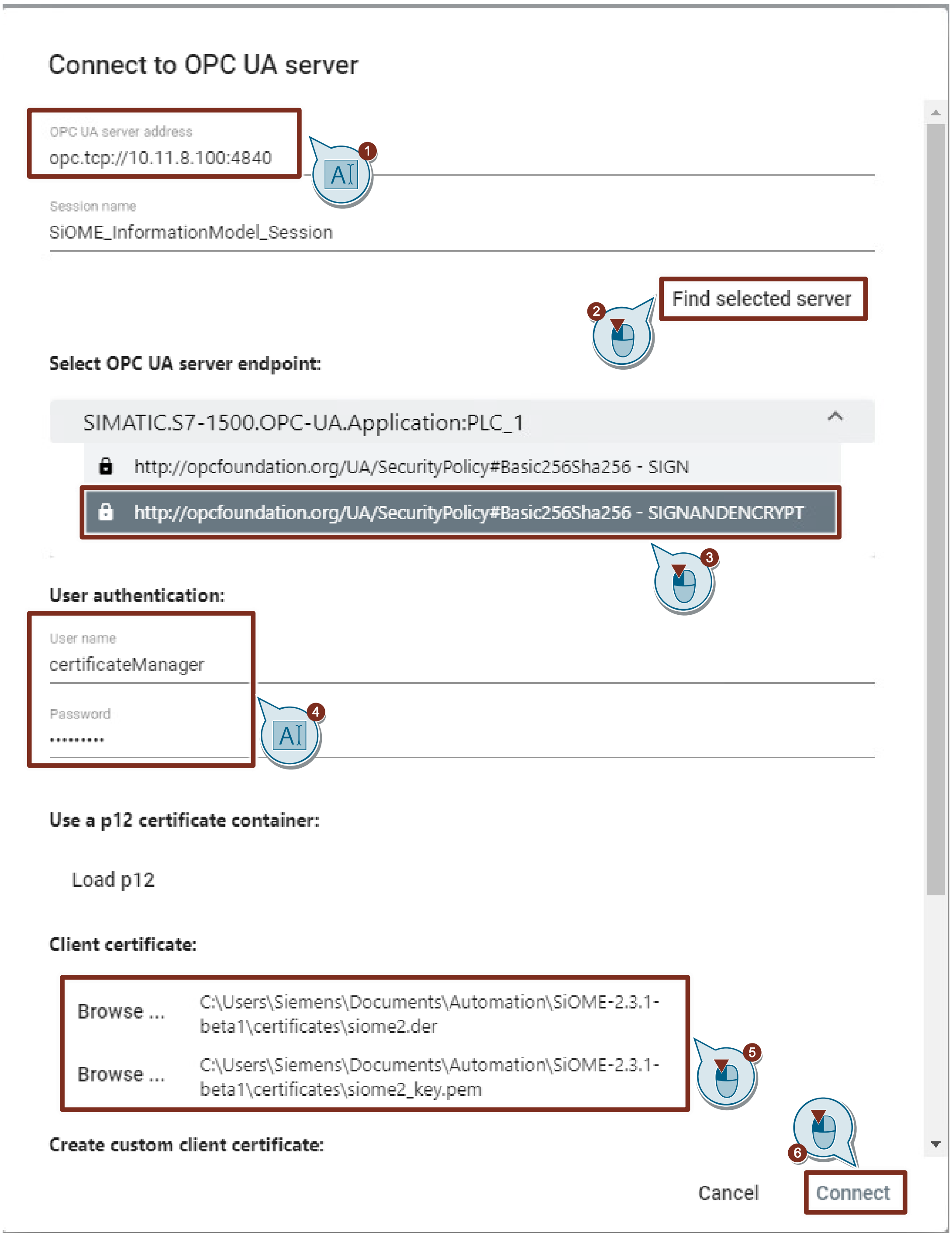
1. Download SiOME in version 2.3.1 or higher from SIOS (https://support.industry.siemens.com/cs/ww/en/view/109755133) and extract the "*.zip" file.
2. Start "SiOME" with the "SiOME-2.3.6.exe" file.
3. Select the "GDS Push" layout to open the GDS Push plugin.



4. Click the icon for "Connect to OPC UA server" to connect "SiOME" with the OPC UA server of the S7-1500 CPU.
   The "Connect to OPC UA server" dialog will open.


Siemens OPC UA Modeling Editor 2.3.1-beta1
SIEMENS
Namespaces:
Editing (current)
Please add or choose a namespace
InformationModel
GDS Push Mode
Please connect to an OPC UA server.

5. Make the following settings:
   - Enter the address of the OPC UA server of the S7-1500 CPU.
   - Click on "Find selected server".
   - Select the encrypted and signed endpoint. Use of the encrypted and signed endpoint is a requirement for certificate management with OPC UA.
   - Enter the username and the password of the user to whom you assigned the runtime right in TIA Portal for certificate management. This user was created while configuring the S7-1500 CPU and is named "certificateManager" in this application example.
   - Select the certificate and the private key that you created with OpenSSL for the client application "SiOME" ("siome.der", "siome.pem").
   - Click "Connect".



Connect to OPC UA server

OPC UA server address: opc.tcp://10.11.8.100:4840

Session name: SiOME_InformationModel_Session

Select OPC UA server endpoint:

SIMATIC.S7-1500.OPC-UA.Application:PLC_1

- http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256 - SIGN
- http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256 - SIGNANDENCRYPT

User authentication:

User name: certificateManager

Password: •••••••••

Use a p12 certificate container:

Client certificate:

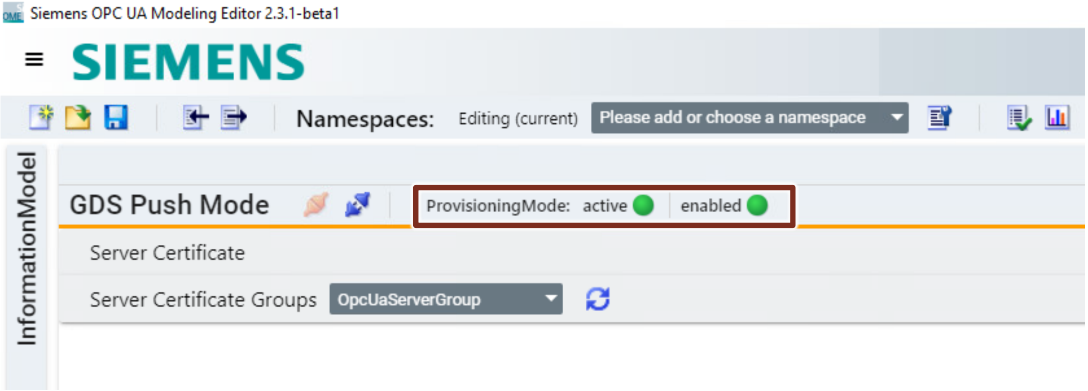
Browse ... C:\Users\Siemens\Documents\Automation\SiOME-2.3.1-beta1\certificates\siome2.der

Browse ... C:\Users\Siemens\Documents\Automation\SiOME-2.3.1-beta1\certificates\siome2_key.pem

Create custom client certificate:

Result

- "SiOME" is connected to the OPC UA server of the S7-1500 CPU as an OPC UA client.
- The status bar in "SiOME" shows you that the CPU is still in "Provisioning state". This means that no list of trusted certificates has been loaded and therefore that the temporary server certificate has not yet been replaced.


Siemens OPC UA Modeling Editor 2.3.1-beta1

Namespaces: Editing (current) Please add or choose a namespace

GDS Push Mode

ProvisioningMode: active ● enabled ●

Server Certificate

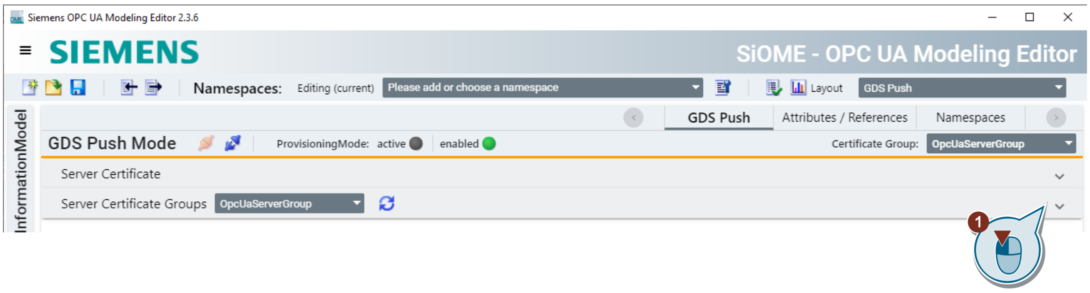
Server Certificate Groups OpcUaServerGroup

2.4.4 Loading the Certificate Trust List from "SiOME" into the S7-1500 CPU

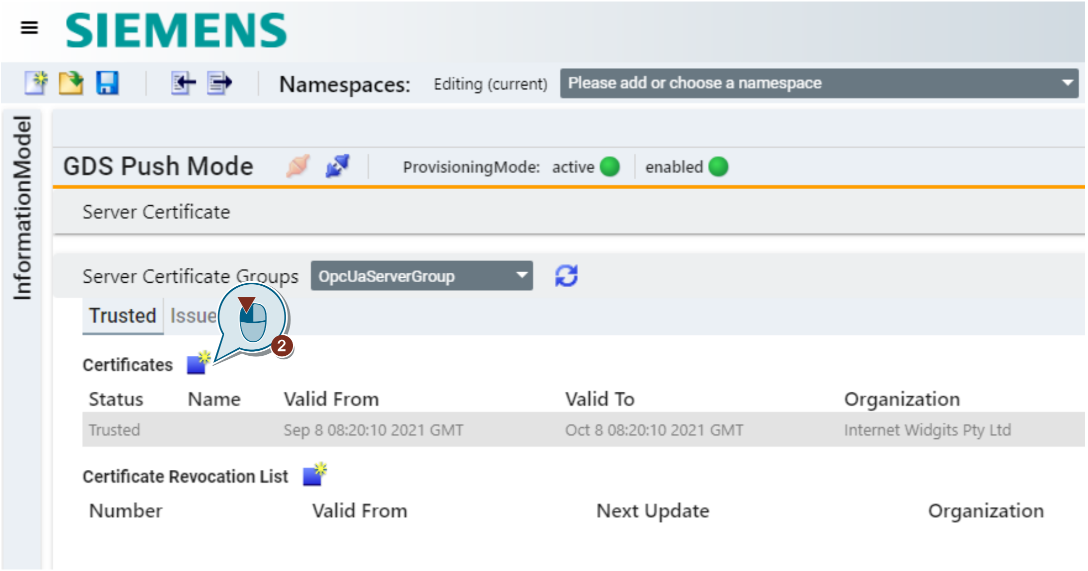
Once the connection is established, the Certificate Trust List is loaded to the S7-1500 CPU. This determines which clients the S7-1500 CPU trusts. In this application example, at first all clients of the self-created CA are trusted.

Add CA certificate to the Certificate Trust List

1. In the GDS Push plugin, open the "Server Certificate Groups" view.



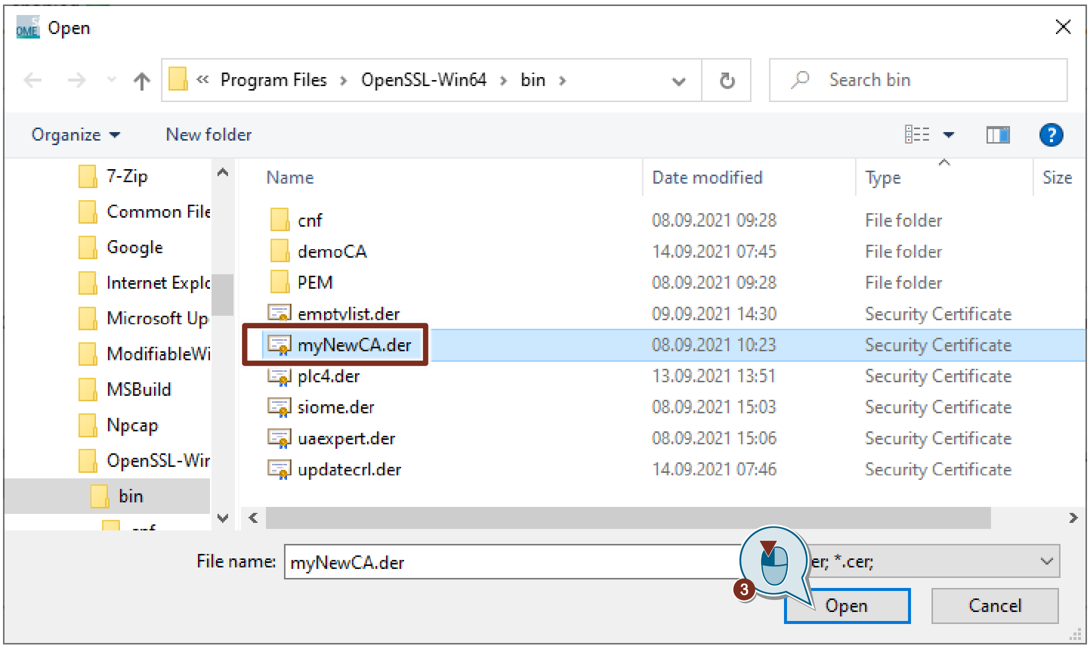
2. In the "Certificates" section, click the icon for "Add New TrustList Entry". The "Open" dialog will open.



Status	Name	Valid From	Valid To	Organization
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd

Number	Valid From	Next Update	Organization

3. Select the self-created CA certificate "MyNewCA.der" and click on "Open".
   The CA certificate "MyNewCA.der" can be found in this application example in the folder "C:\Program Files\OpenSSL-Win64\bin".



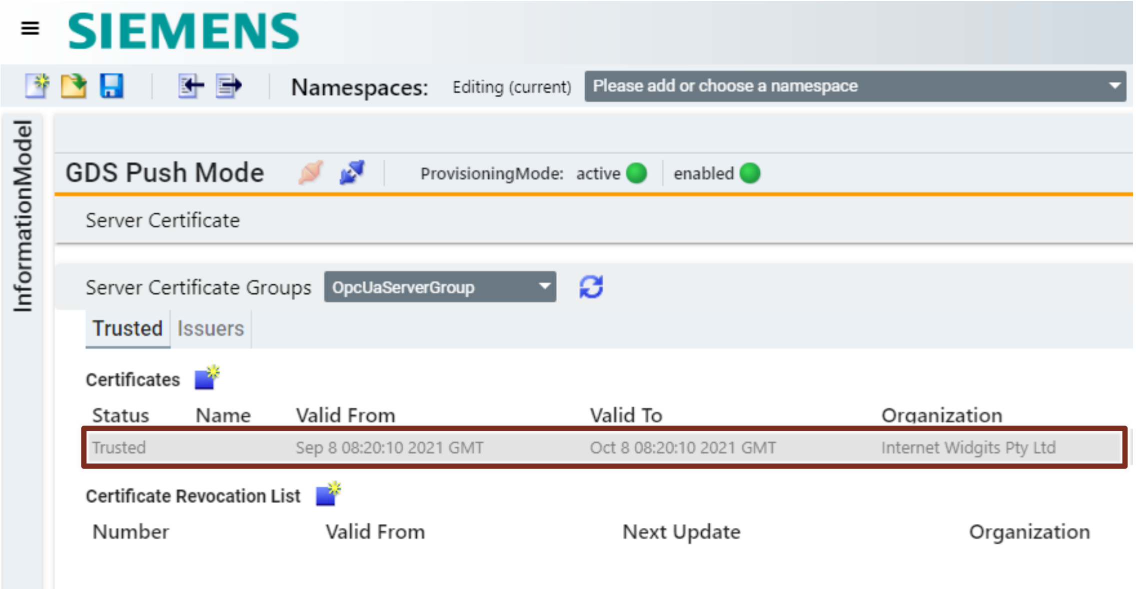
Name	Date modified	Type	Size
cnf	08.09.2021 09:28	File folder	
demoCA	14.09.2021 07:45	File folder	
PEM	08.09.2021 09:28	File folder	
emptylist.der	09.09.2021 14:30	Security Certificate	
myNewCA.der	08.09.2021 10:23	Security Certificate	
plc4.der	13.09.2021 13:51	Security Certificate	
siome.der	08.09.2021 15:03	Security Certificate	
uaexpert.der	08.09.2021 15:06	Security Certificate	
updatecrl.der	14.09.2021 07:46	Security Certificate	

File name: myNewCA.der

er; *.cer;

The CA certificate "MyNewCA.der" will be added to the Certificate Trust List. The file will appear in "SiOME" with a gray background. This means that the file has not yet been transferred to the S7-1500 CPU.

Figure 2-12



Namespaces: Editing (current) Please add or choose a namespace

ProvisioningMode: active ● enabled ●

Server Certificate Groups OpcUaServerGroup

Certificates

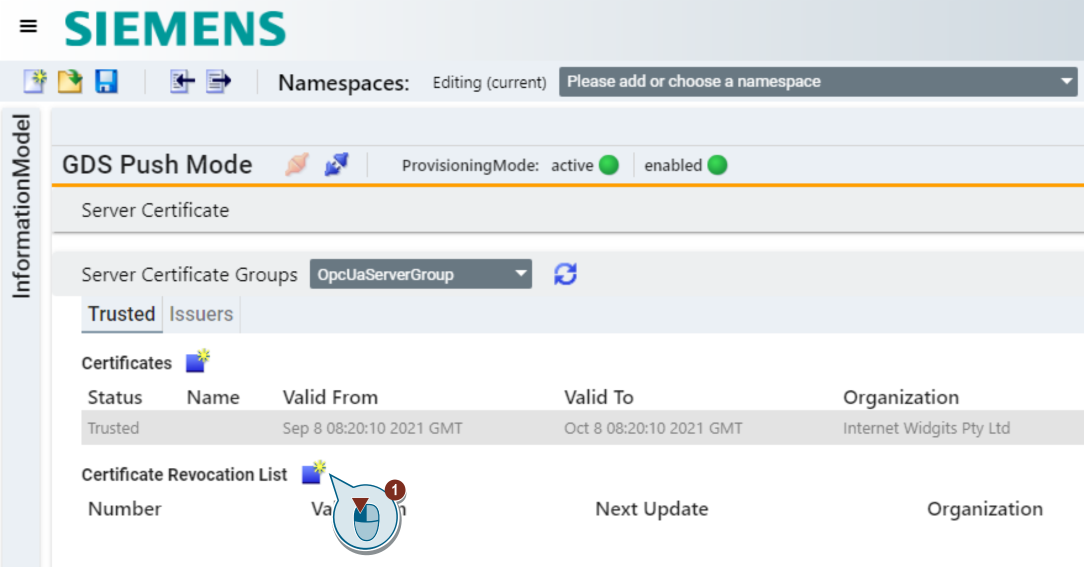
Status	Name	Valid From	Valid To	Organization
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd

Certificate Revocation List

Number	Valid From	Next Update	Organization

Add Certificate Revocation List

1. In the "Certificate Revocation List" section, click the icon for "Add New RevocationList Entry".
   The "Open" dialog will open.



Namespaces: Editing (current) Please add or choose a namespace

ProvisioningMode: active ● enabled ●

Server Certificate

Server Certificate Groups OpcUaServerGroup

Trusted Issuers

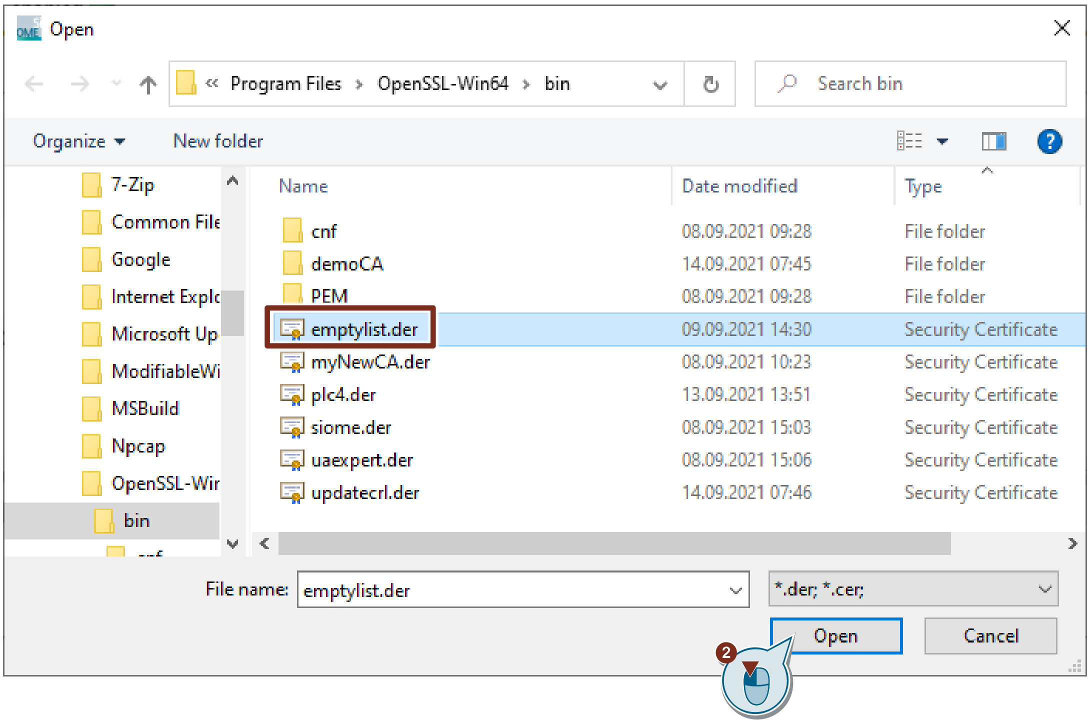
Certificates

Status	Name	Valid From	Valid To	Organization
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd

Certificate Revocation List

Number	Va[illegible]n	Next Update	Organization

2. Select the self-created, empty Certificate Revocation List (CRL) "emptylist.der" and click the "Open" button.
   The empty Certificate Revocation List "emptylist.der" can be found in this application example in the folder "C:\Program Files\OpenSSL-Win64\bin".



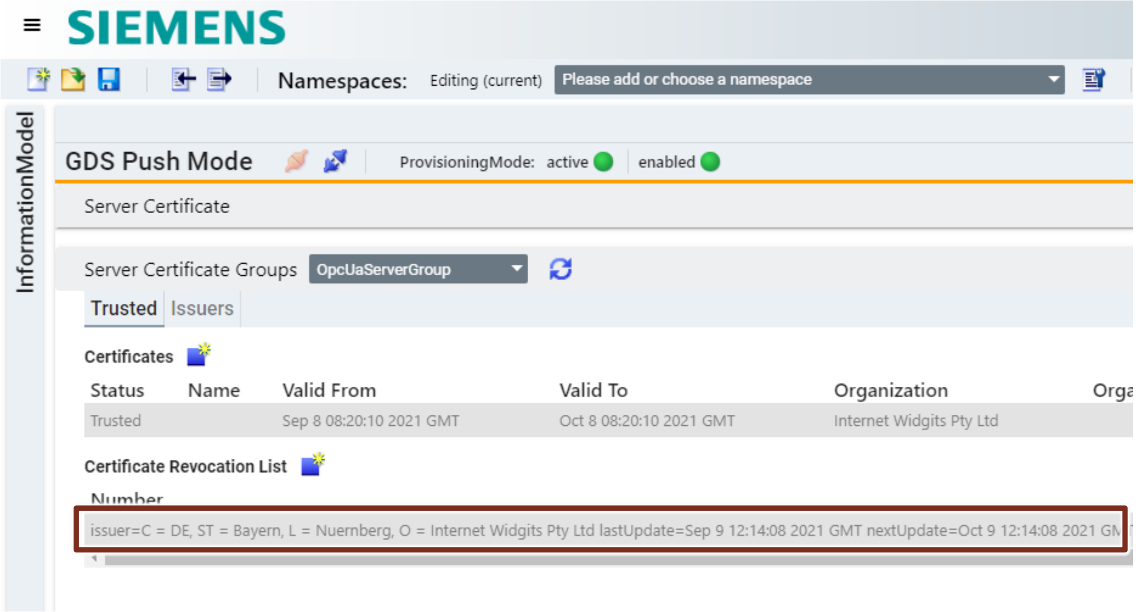
Name	Date modified	Type
cnf	08.09.2021 09:28	File folder
demoCA	14.09.2021 07:45	File folder
PEM	08.09.2021 09:28	File folder
emptylist.der	09.09.2021 14:30	Security Certificate
myNewCA.der	08.09.2021 10:23	Security Certificate
plc4.der	13.09.2021 13:51	Security Certificate
siome.der	08.09.2021 15:03	Security Certificate
uaexpert.der	08.09.2021 15:06	Security Certificate
updatecrl.der	14.09.2021 07:46	Security Certificate

File name: emptylist.der

*.der; *.cer;

The empty Certificate Revocation List "emptylist.der" will be added. The file will appear in "SiOME" with a gray background. This means that the file has not yet been transferred to the S7-1500 CPU.

Figure 2-13



ProvisioningMode: active ● enabled ●

Server Certificate Groups: OpcUaServerGroup

Status	Name	Valid From	Valid To	Organization	Orga
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd	

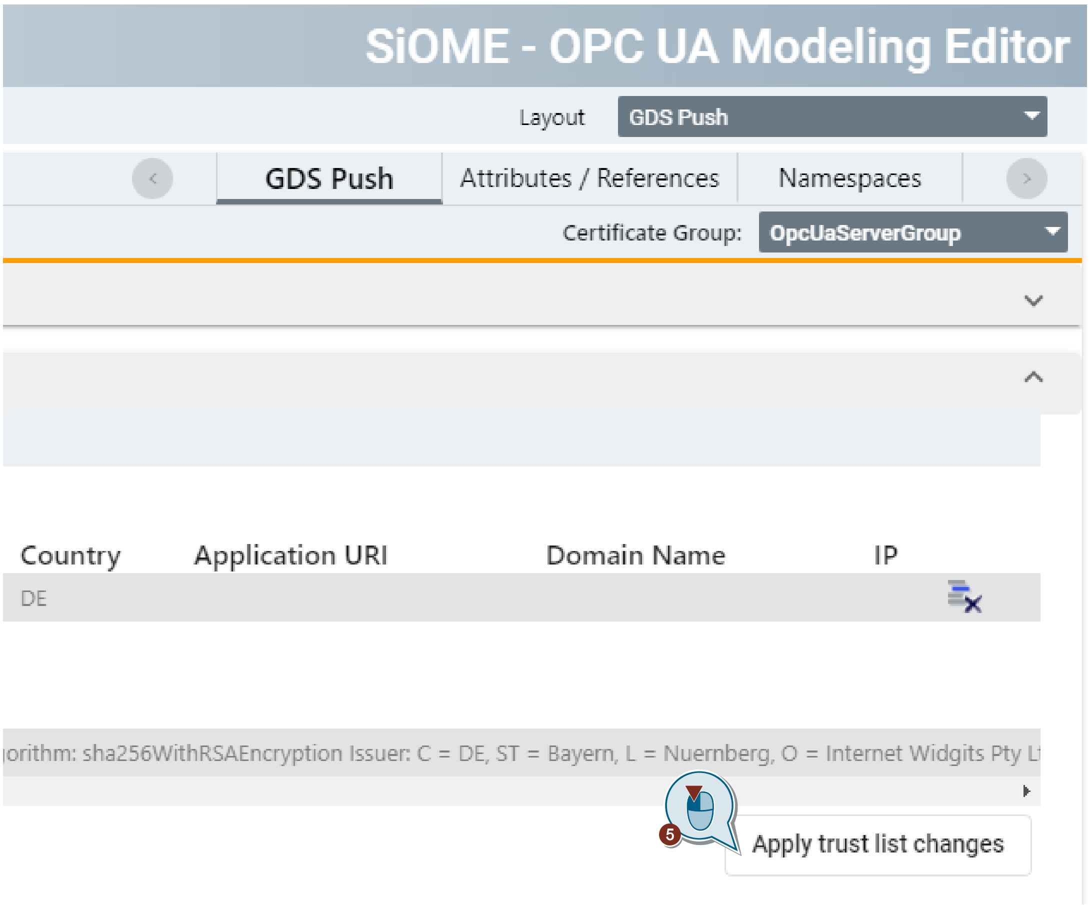
Number

issuer=C = DE, ST = Bayern, L = Nuernberg, O = Internet Widgits Pty Ltd lastUpdate=Sep 9 12:14:08 2021 GMT nextUpdate=Oct 9 12:14:08 2021 GM

Load Certificate Trust List to the S7-1500 CPU

You need to transfer the self-created CA certificate "MyNewCA.der" and the empty Certificate Revocation List (CRL) "emptylist.der" to the S7-1500 CPU to place them in the Trust List of the S7-1500 CPU. This is necessary for trusting all clients of this CA.

1. Click the icon "Apply trust list changes".
   The Certificate Trust List will be transferred to the S7-1500 CPU. The Certificate Revocation List is loaded as part of the Certificate Trust List.



|orithm: sha256WithRSAEncryption Issuer: C = DE, ST = Bayern, L = Nuernberg, O = Internet Widgits Pty Lt

Result

The CA certificate "MyNewCA.der" and the empty Certificate Revocation List are set within the Trust List of the S7-1500 CPU. One of the two conditions necessary for the S7-1500 CPU to exit "Provisioning state" has thus been met.

The second condition that still needs to be met is the replacement of the server certificate.

2.4.5 Replacing the server certificate of the OPC UA server

Now that the certificates for the CA and all clients have been created, the certificate of the OPC UA server of the S7-1500 CPU still needs to be replaced, as the temporary server certificate that the S7-1500 CPU generated is still in use.

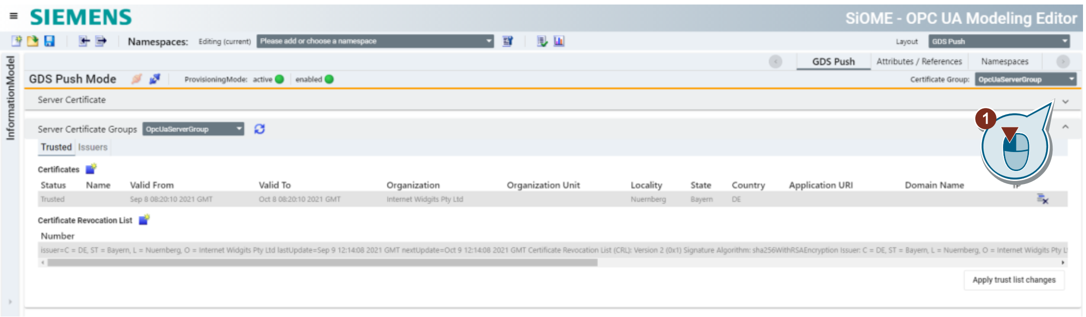
The server certificate can be replaced in two different ways:

1. The certificate, including the private key, is loaded to the S7-1500 CPU.
2. The S7-1500 CPU sends a "Certificate Signing Request" via the OPC UA method "Request CSR". To do this, the S7-1500 CPU first generates a private key and then returns a "Certificate Signing Request" to the client. The request is signed by the CA and then loaded to the S7-1500 CPU.

The second method offers additional security compared to the first method, as the private key never leaves the end device. Therefore, the following section will explain the second method. Figure 2-4 shows the flowchart corresponding to the second method.

Create certificate request "*.csr" file

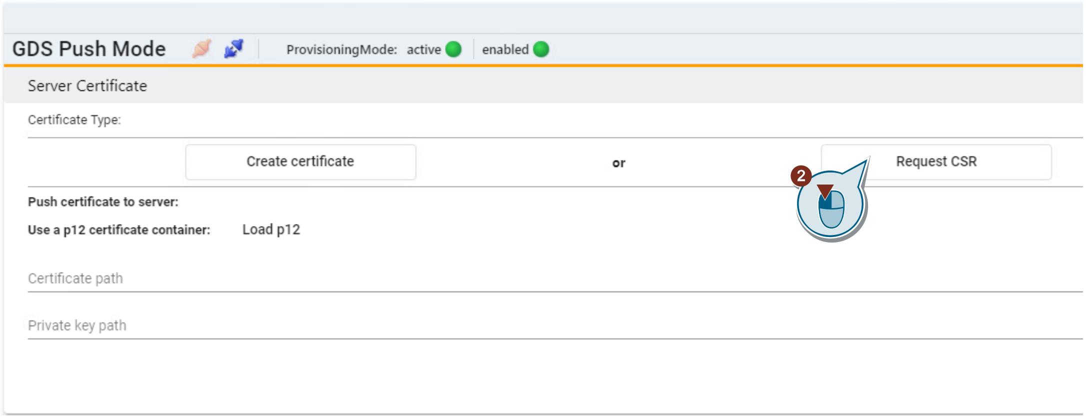
1. Open the area for handling the server certificate ("Server Certificate").



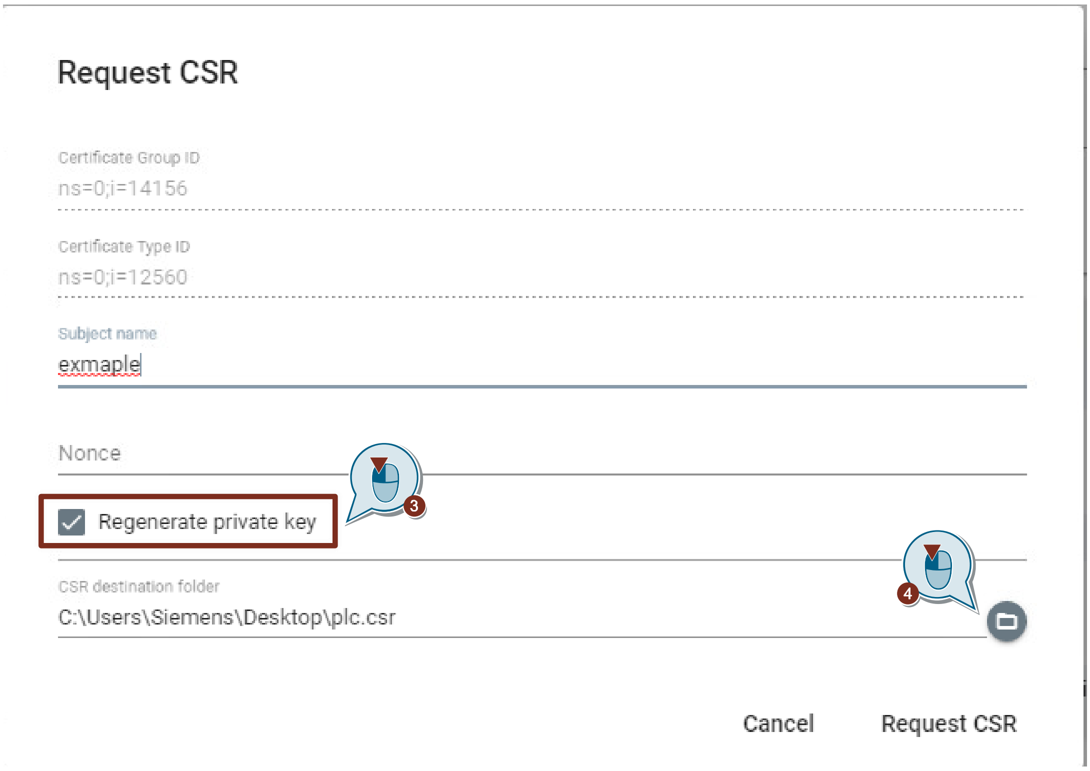
Status	Name	Valid From	Valid To	Organization	Organization Unit	Locality	State	Country	Application URI	Domain Name
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd		Nuernberg	Bayern	DE		

Number
issuer=C = DE, ST = Bayern, L = Nuernberg, O = Internet Widgits Pty Ltd lastUpdate=Sep 9 12:14:08 2021 GMT nextUpdate=Oct 9 12:14:08 2021 GMT Certificate Revocation List (CRL): Version 2 (0x1) Signature Algorithm: sha256WithRSAEncryption Issuer: C = DE, ST = Bayern, L = Nuernberg, O = Internet Widgits Pty L

2. Click on "Request CSR" to create a certificate request ("*.csr" file).
   The "Request CSR" dialog will open.



3. Enable the function "Regenerate private key".
4. Click the "folder" icon to define the storage path and file name for the certificate request ("*.csr" file).
   The "Save" dialog will open.



Request CSR

Certificate Group ID
ns=0;i=14156

Certificate Type ID
ns=0;i=12560

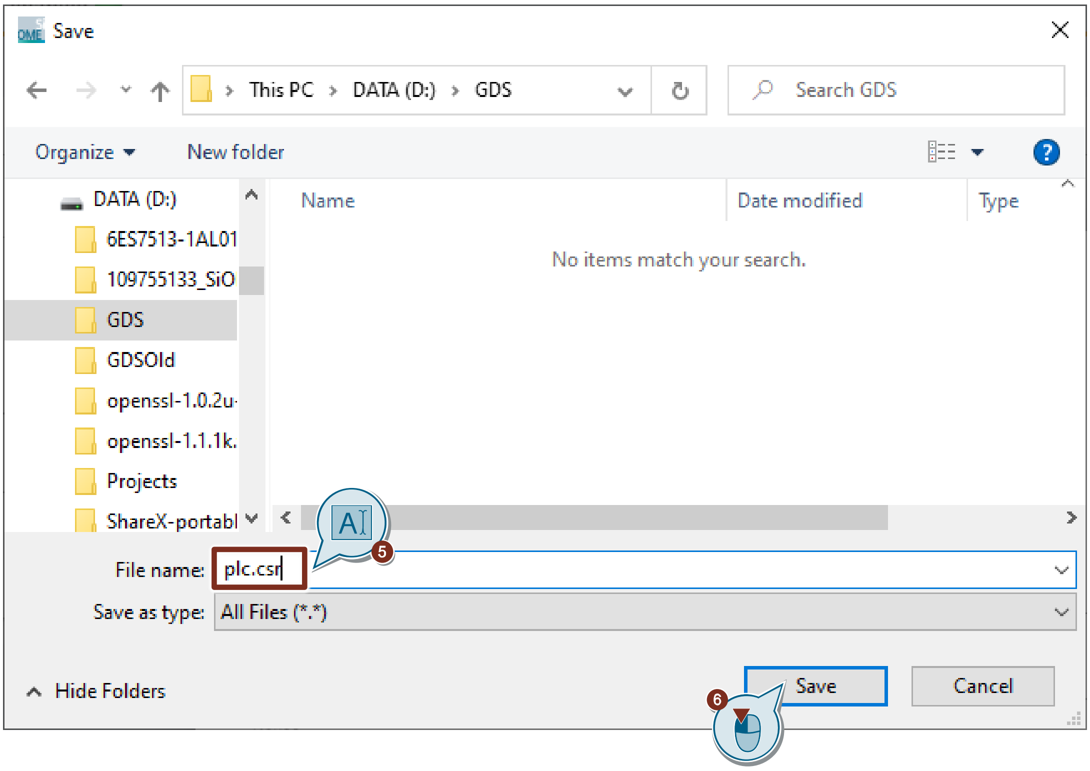
Subject name
exmaple

Nonce

☑ Regenerate private key

CSR destination folder
C:\Users\Siemens\Desktop\plc.csr

5. Select a storage location for the "*.csr" file and enter a file name for the "*.csr" file, for example "plc.csr".
6. Click "Save".

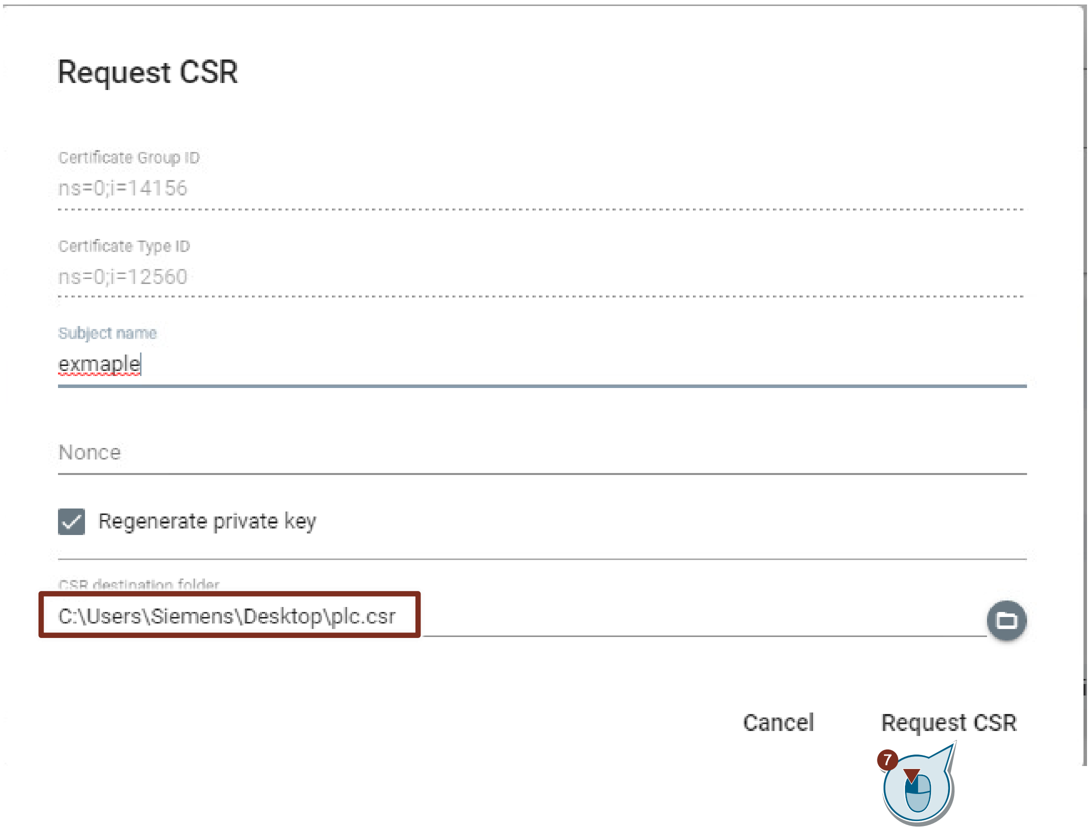


File name: plc.csr

Save as type: All Files (*.*)

No items match your search.

7. Click "Request CSR".
   The certificate request will be created, i. e. the "plc.csr" file will be saved in the selected save location.



Request CSR

Certificate Group ID
ns=0;i=14156

Certificate Type ID
ns=0;i=12560

Subject name
exmaple

Nonce

☑ Regenerate private key

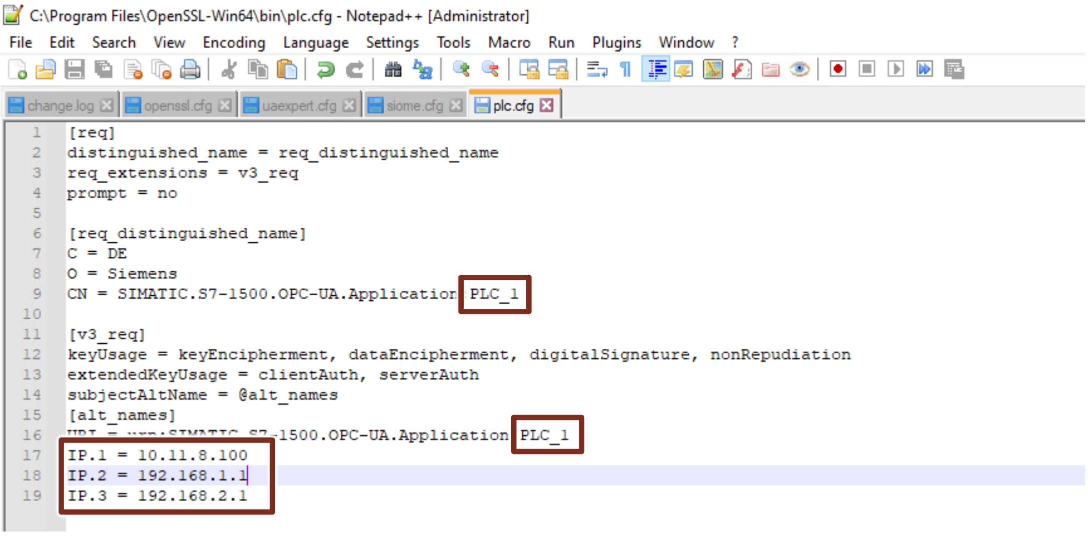
CSR destination folder
C:\Users\Siemens\Desktop\plc.csr

8. Copy the "plc.csr" file to the "\bin" folder of OpenSSL.

CA-signed certificate request "*.csr" file

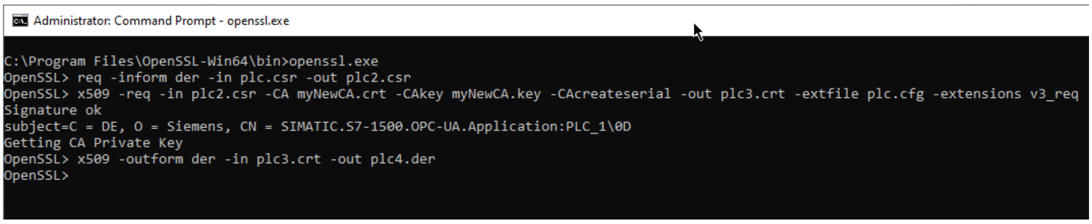
To turn the certificate request "plc.csr" into a certificate, the CA must sign the certificate request with the help of OpenSSL.

1. To properly set the necessary attributes in the certificate, it is possible to use a "*.cfg" file. Modify the file "plc.cfg" from this download to match your configuration. Open the "plc.cfg" file in an ASCII text editor.
   Change the name of the CPU and the IP addresses. Then save the file.


C:\Program Files\OpenSSL-Win64\bin\plc.cfg - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
openssl.cfg
uaexpert.cfg
siome.cfg
plc.cfg

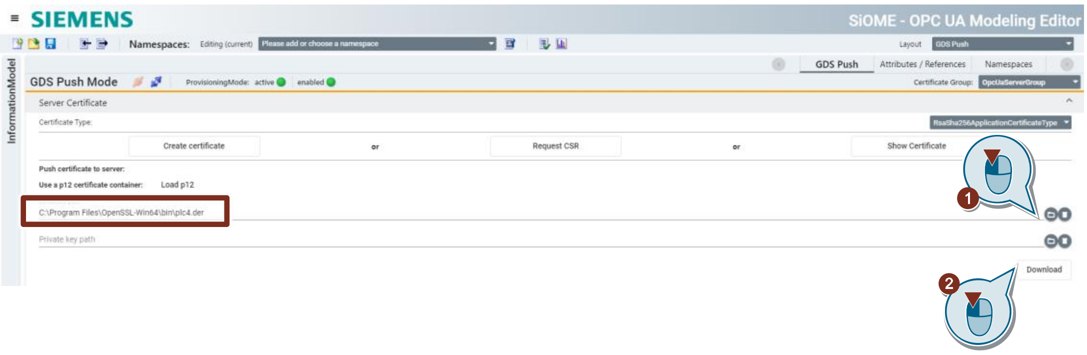
```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no

[req_distinguished_name]
C = DE
O = Siemens
CN = SIMATIC.S7-1500.OPC-UA.Application:PLC_1

[v3_req]
keyUsage = keyEncipherment, dataEncipherment, digitalSignature, nonRepudiation
extendedKeyUsage = clientAuth, serverAuth
subjectAltName = @alt_names
[alt_names]
URI = urn:SIMATIC.S7-1500.OPC-UA.Application:PLC_1
IP.1 = 10.11.8.100
IP.2 = 192.168.1.1
IP.3 = 192.168.2.1
```

2. Convert the "*.der"-based file into a "*.pem"-based file via the OpenSSL console.
   `req -inform der -in plc.csr -out plc2.csr`
3. Sign the file with the CA.
   `x509 -req -in plc2.csr -CA myNewCA.crt -CAkey myNewCA.key -CAcreateserial -out plc3.crt -extfile plc.cfg -extensions v3_req`
4. The certificate must be in the "*.der" file format to load it to the S7-1500 CPU. Convert the certificate.
   `x509 -outform der -in plc3.crt -out -plc4.der`



```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -inform der -in plc.csr -out plc2.csr
OpenSSL> x509 -req -in plc2.csr -CA myNewCA.crt -CAkey myNewCA.key -CAcreateserial -out plc3.crt -extfile plc.cfg -extensions v3_req
Signature ok
subject=C = DE, O = Siemens, CN = SIMATIC.S7-1500.OPC-UA.Application:PLC_1\0D
Getting CA Private Key
OpenSSL> x509 -outform der -in plc3.crt -out plc4.der
OpenSSL>
```

5. Load the "*.der" file to the CPU with SiOME.
   - Select the created "*.der" file.
   - Click the "Download" button.



SiOME - OPC UA Modeling Editor

Namespaces: Editing (current) Please add or choose a namespace

Layout: GDS Push

GDS Push Mode — ProvisioningMode: active ● enabled ●

Certificate Group: OpcUaServerGroup

Server Certificate

Certificate Type: RsaSha256ApplicationCertificateType

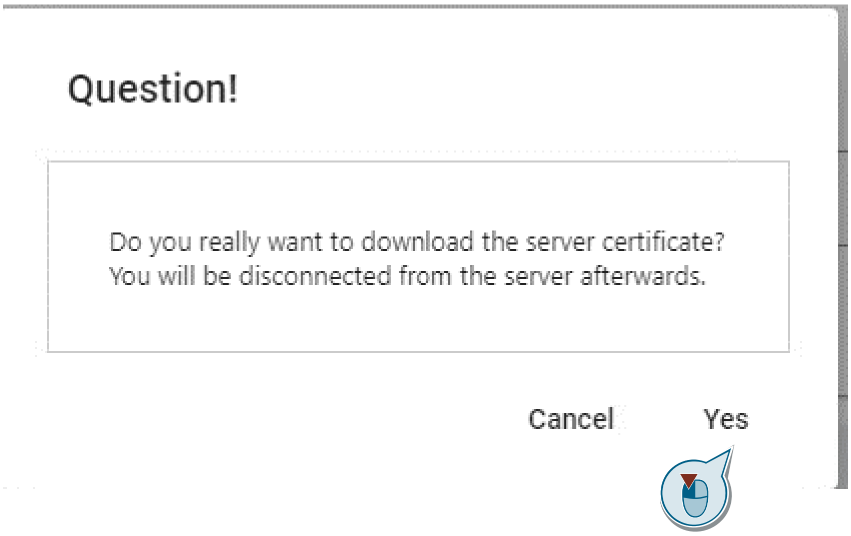
Push certificate to server:

Use a p12 certificate container: Load p12

C:\Program Files\OpenSSL-Win64\bin\plc4.der

Private key path

6. Start the download process with "Yes".
   Once the server certificate is loaded, the endpoints of the OPC UA server of the S7-1500 CPU will be shut down. This will cause SiOME to lose the connection.



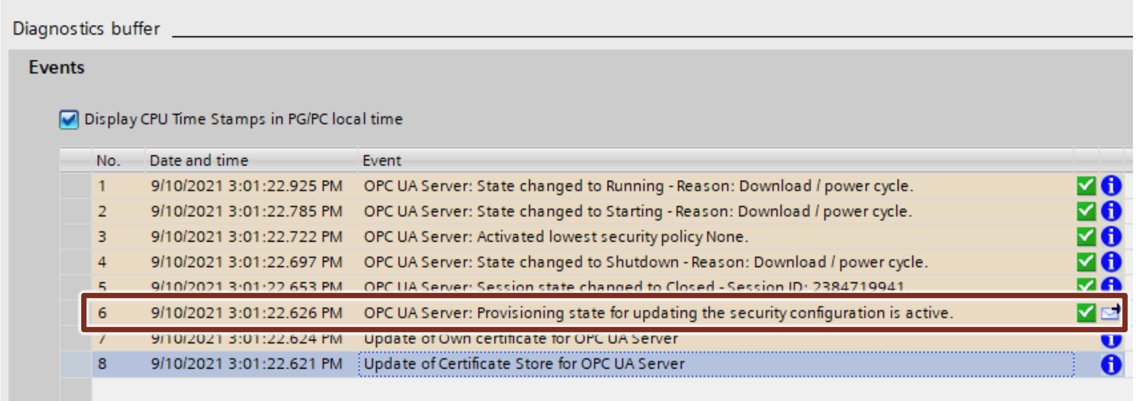
Question!

Do you really want to download the server certificate?
You will be disconnected from the server afterwards.

Result

Once the Certificate Trust List has been loaded and the server certificate has been replaced, both conditions are met for the CPU to terminate "Provisioning state". You can see this on the CPU when the yellow MAINT LED no longer lights up. In the diagnostic buffer of the S7-1500 CPU, the "Provisioning state" is displayed as an outgoing message.

Figure 2-14



☑ Display CPU Time Stamps in PG/PC local time

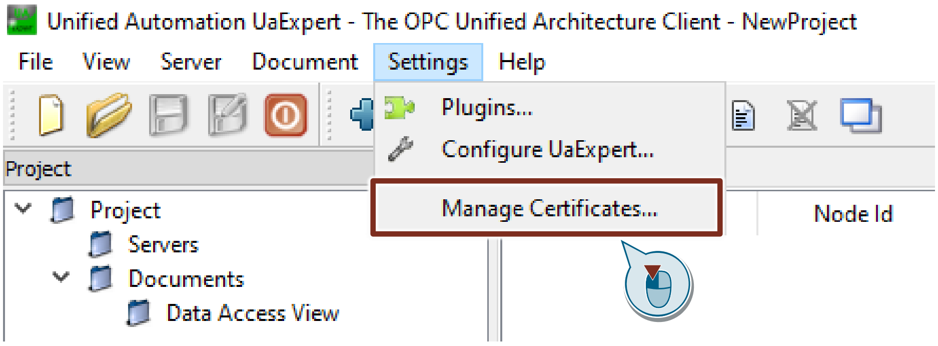
No.	Date and time	Event		
1	9/10/2021 3:01:22.925 PM	OPC UA Server: State changed to Running - Reason: Download / power cycle.	✓	ℹ
2	9/10/2021 3:01:22.785 PM	OPC UA Server: State changed to Starting - Reason: Download / power cycle.	✓	ℹ
3	9/10/2021 3:01:22.722 PM	OPC UA Server: Activated lowest security policy None.	✓	ℹ
4	9/10/2021 3:01:22.697 PM	OPC UA Server: State changed to Shutdown - Reason: Download / power cycle.	✓	ℹ
5	9/10/2021 3:01:22.653 PM	OPC UA Server: Session state changed to Closed - Session ID: 2384719941	✓	ℹ
6	9/10/2021 3:01:22.626 PM	OPC UA Server: Provisioning state for updating the security configuration is active.	✓	✉
7	9/10/2021 3:01:22.624 PM	Update of Own certificate for OPC UA Server		ℹ
8	9/10/2021 3:01:22.621 PM	Update of Certificate Store for OPC UA Server		ℹ

Now OPC UA clients can only establish a connection to the CPU if they have an existing trust relationship. In this example, these are all clients whose certificates are signed by the CA.

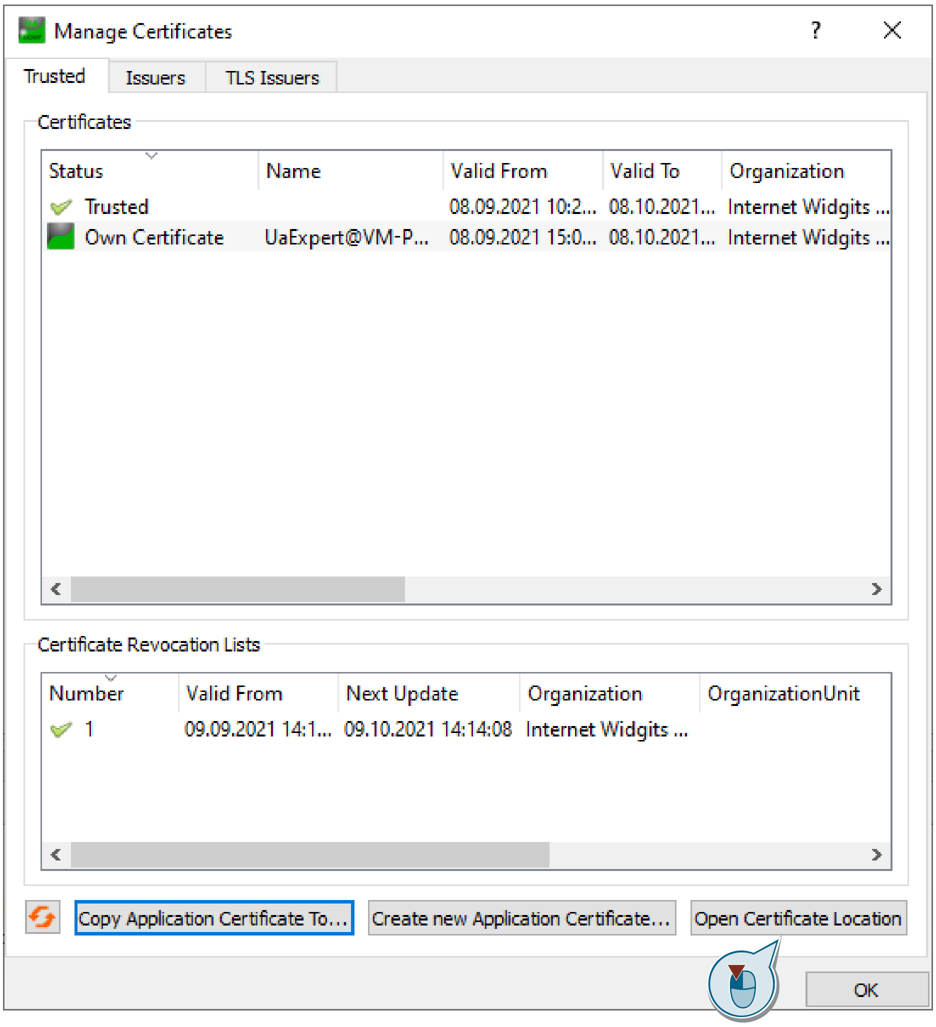
2.5 Testing the OPC UA connection to the S7-1500 CPU

In this chapter, you will test opening a connection from an OPC UA client to the OPC UA server of the S7-1500 CPU. The OPC UA client "UA Expert" will be used for the test. In chapter 2.4.2, you already created a certificate and a private key for the OPC UA client "UA Expert". These now must be imported.

1. Launch the OPC UA client "UA Expert".
2. Select the menu "Settings > Manage Certificates".
   The "Manage Certificates" dialog will open.



3. Click the "Open Certificate Location" button.
   You will be taken to the storage directory of the certificates.


Manage Certificates
?
Trusted
Issuers
TLS Issuers
Certificates

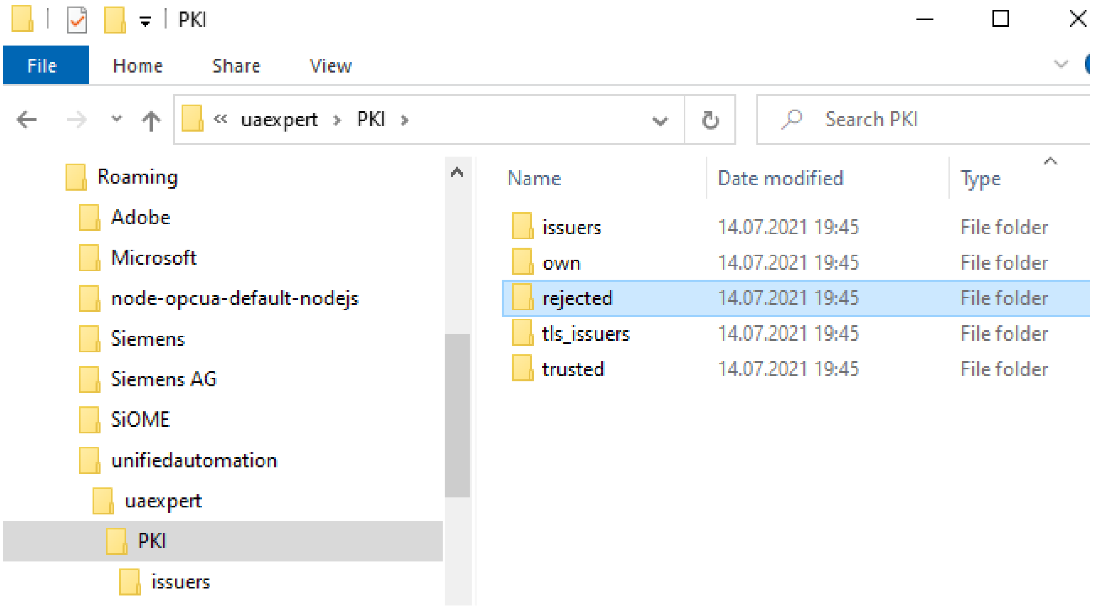
Status	Name	Valid From	Valid To	Organization
✓ Trusted		08.09.2021 10:2...	08.10.2021...	Internet Widgits ...
Own Certificate	UaExpert@VM-P...	08.09.2021 15:0...	08.10.2021...	Internet Widgits ...

Certificate Revocation Lists

Number	Valid From	Next Update	Organization	OrganizationUnit
✓ 1	09.09.2021 14:1...	09.10.2021 14:14:08	Internet Widgits ...	

Copy Application Certificate To...
Create new Application Certificate...
Open Certificate Location
OK

4. Navigate to the folder "PKI" one level up.



Name	Date modified	Type
issuers	14.07.2021 19:45	File folder
own	14.07.2021 19:45	File folder
rejected	14.07.2021 19:45	File folder
tls_issuers	14.07.2021 19:45	File folder
trusted	14.07.2021 19:45	File folder

5. Place the certificates created for the OPC UA client "UA Expert" in chapter 2.4.2 in the corresponding directories and delete the existing files.

File	Storage location
Client certificate of UA Expert (*.der)	.\pki\own\certs
Private key of UA Expert	.\pki\own\private
CA root certificate	.\pki\trusted\certs
Certificate Revocation List (CRL)	.\pki\trusted\crl

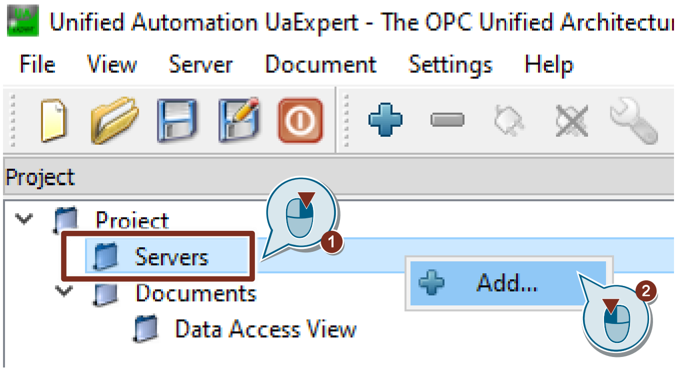
NOTE

The Certificate Revocation List requires the file format "*.crl". Rename the Certificate Revocation List so that it has the "*.crl" extension.

Rename the client certificate of UA Expert to "uaexpert.der".

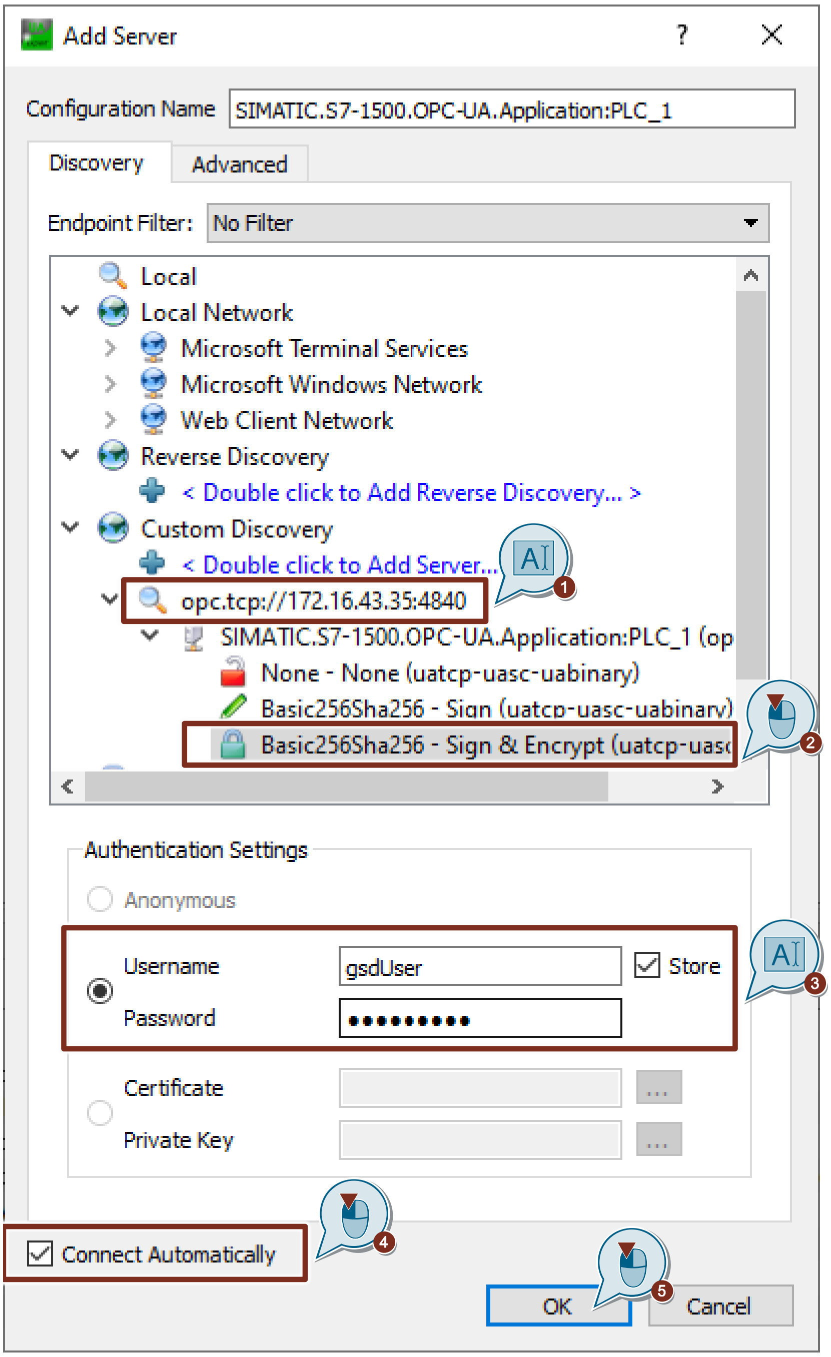
Rename the private key of UA Expert to "uaexpert_key.pem".

6. With "UA Expert", establish a connection to the OPC UA server of the S7-1500 CPU.
   - In the "Project" window under "Project", right-click "Servers".
   - Select "Add..." in the context menu.
     The "Add Server" dialog will open.



Unified Automation UaExpert - The OPC Unified Architectur
File
View
Server
Document
Settings
Help
Project
Project
Servers
Documents
Data Access View
Add...
1
2

- Enter the address of the OPC UA server of the S7-1500 CPU.
- Select the encrypted and signed endpoint.
- Enter the username and password of the user to whom you gave the runtime right for access to the OPC UA server in TIA Portal. This user was created while configuring the S7-1500 CPU and is named "certificateManager" in this application example.
- Enable the "Connect Automatically" function so that OPC UA Expert automatically establishes the connection to the OPC UA server of the S7-1500 CPU. Because both connection partners trust the CA, it is possible to establish the connection automatically.
- Click "OK".



Add Server

Configuration Name: SIMATIC.S7-1500.OPC-UA.Application:PLC_1

Endpoint Filter: No Filter

- Local
- Local Network
  - Microsoft Terminal Services
  - Microsoft Windows Network
  - Web Client Network
- Reverse Discovery
  - < Double click to Add Reverse Discovery... >
- Custom Discovery
  - < Double click to Add Server...
  - 1 opc.tcp://172.16.43.35:4840
    - SIMATIC.S7-1500.OPC-UA.Application:PLC_1 (op
      - None - None (uatcp-uasc-uabinary)
      - Basic256Sha256 - Sign (uatcp-uasc-uabinary)
      - 2 Basic256Sha256 - Sign & Encrypt (uatcp-uasc

Authentication Settings

○ Anonymous

3 ● Username: gsdUser ☑ Store
Password: ●●●●●●●●●●

○ Certificate
Private Key

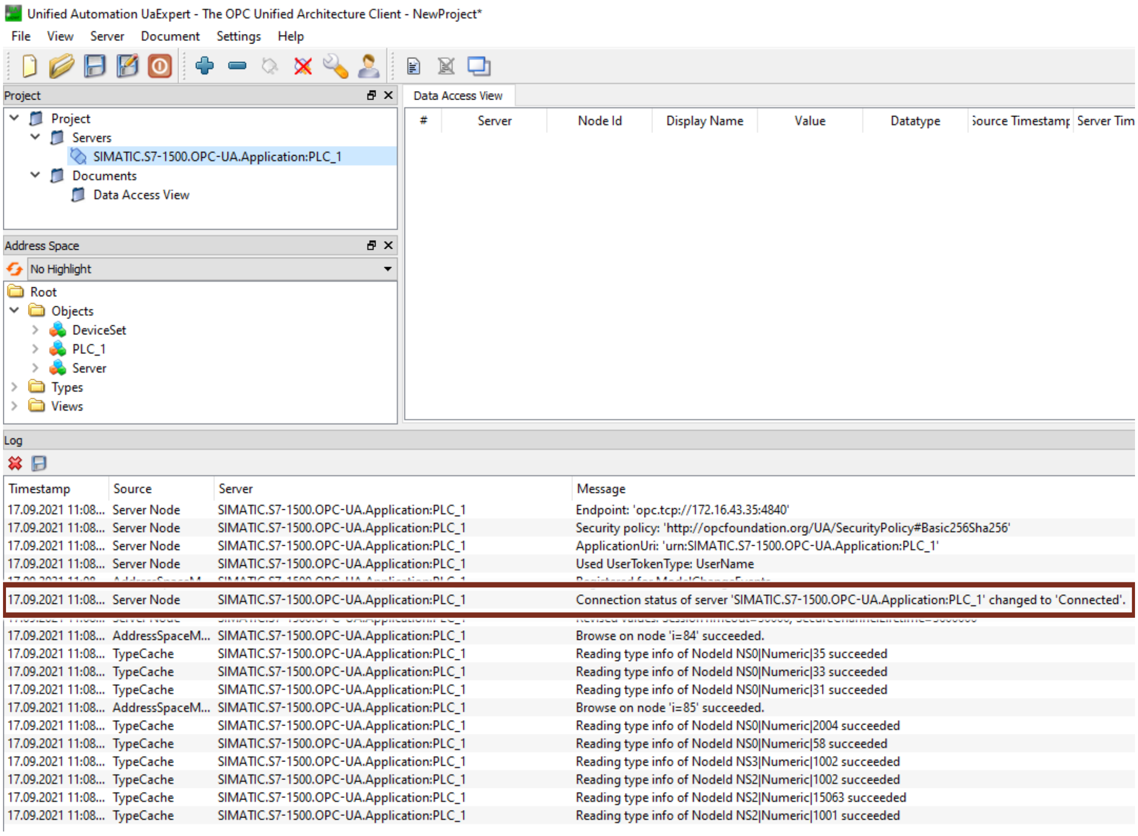
4 ☑ Connect Automatically

Result

The connection between the OPC UA client "UA Expert" and the OPC UA server of the S7-1500 CPU has been established.

The connection status appears in the "Log" window. If the connection status "Connected" appears, then the connection is online.

Figure 2-15



Timestamp	Source	Server	Message
17.09.2021 11:08...	Server Node	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Endpoint: 'opc.tcp://172.16.43.35:4840'
17.09.2021 11:08...	Server Node	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Security policy: 'http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256'
17.09.2021 11:08...	Server Node	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	ApplicationUri: 'urn:SIMATIC.S7-1500.OPC-UA.Application:PLC_1'
17.09.2021 11:08...	Server Node	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Used UserTokenType: UserName
17.09.2021 11:08...	Server Node	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Connection status of server 'SIMATIC.S7-1500.OPC-UA.Application:PLC_1' changed to 'Connected'.
17.09.2021 11:08...	AddressSpaceM...	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Browse on node 'i=84' succeeded.
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS0|Numeric|35 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS0|Numeric|33 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS0|Numeric|31 succeeded
17.09.2021 11:08...	AddressSpaceM...	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Browse on node 'i=85' succeeded.
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS0|Numeric|2004 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS0|Numeric|58 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS3|Numeric|1002 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS2|Numeric|1002 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS2|Numeric|15063 succeeded
17.09.2021 11:08...	TypeCache	SIMATIC.S7-1500.OPC-UA.Application:PLC_1	Reading type info of NodeId NS2|Numeric|1001 succeeded

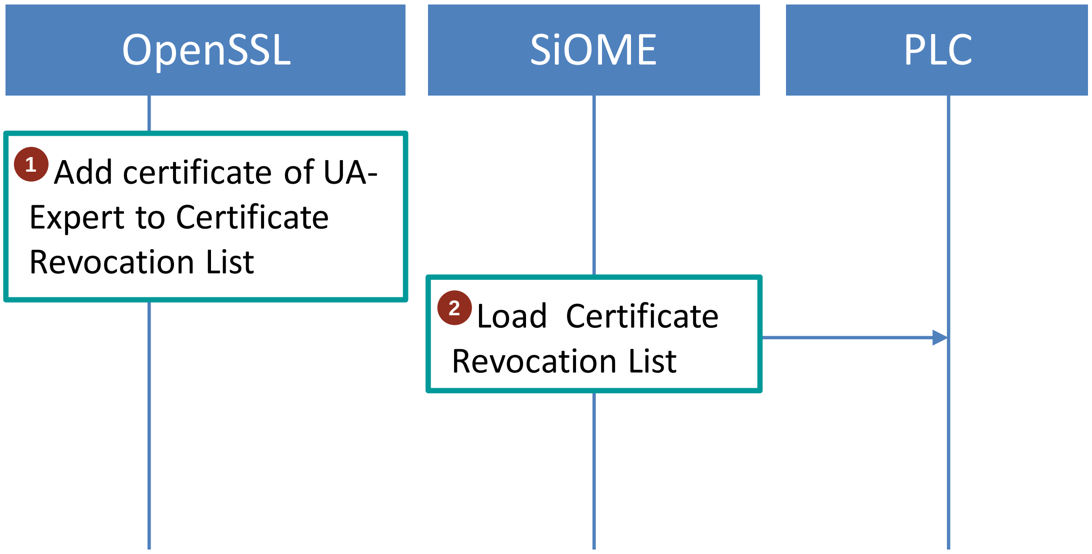
2.6 Updating the Certificate Revocation List

2.6.1 Overview

When using a CA, there are scenarios in which certificates are considered compromised. In this case it is important that these can be revoked. In this example, the certificate of the OPC client "UA Expert" will be considered compromised. At the same time, however, SiOME should still be able to connect with the OPC UA server of the S7-1500 CPU. The trust relationship of SiOME to the CA will therefore be retained and only the certificate of the OPC UA client "UA Expert" will be declared invalid.

The following graphic shows an overview of the procedure.

Figure 2-16

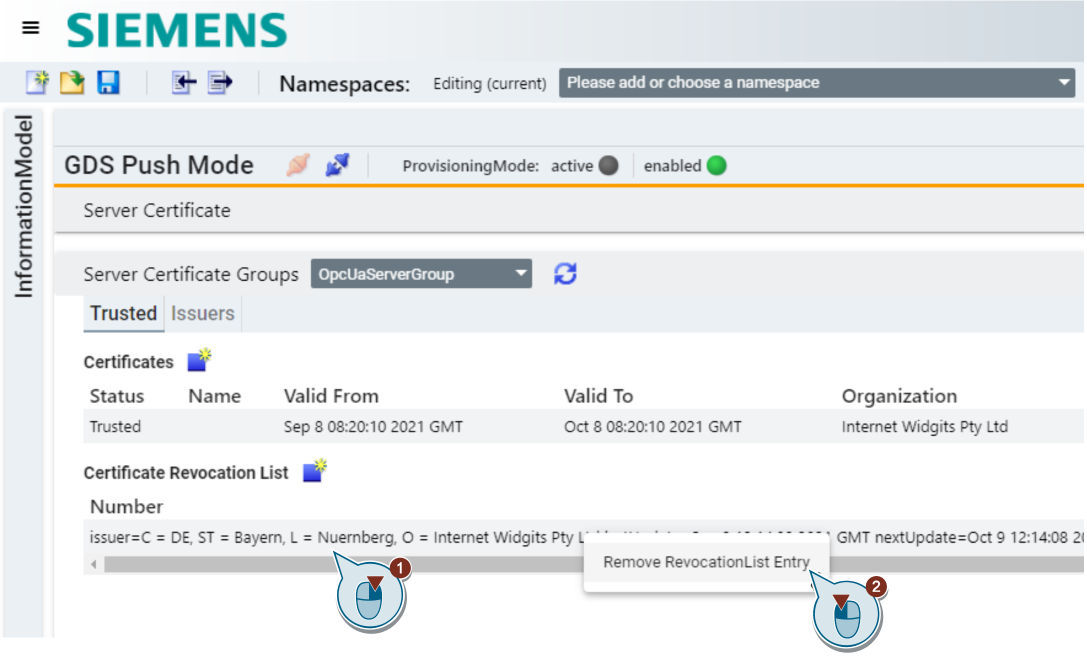

OpenSSL
SiOME
PLC
1 Add certificate of UA-Expert to Certificate Revocation List
2 Load Certificate Revocation List

2.6.2 Adding the certificate of the OPC client "UA Expert" to the Certificate Revocation List

1. Declare the certificate of the OPC UA client "UA Expert" invalid by adding it to the Certificate Revocation List with OpenSSL.
   ```
   ca -revoke uaexpert.crt -keyfile myNewCA.key -cert myNewCA.crt
   ```
2. Generate an updated Certificate Revocation List (CRL).
   ```
   ca -gencrl -keyfile myNewCA.key -cert myNewCA.crt -out
   updatecrl.pem
   ```
3. Convert the "*.crl" file to the "*.der" file format so that it can be loaded to the S7-1500 CPU.
   ```
   crl -outform der -in updatecrl.pem -out updatecrl.der
   ```

2.6.3 Loading the Certificate Revocation List

1. Open "SiOME".
   If "SiOME" is no longer connected to the CPU, reconnect.
2. In the "Certificate Revocation List" section, right-click on the existing empty Certificate Revocation List and select the context menu "Remove RevocationList Entry" to delete it.


SIEMENS
Namespaces:
Editing (current)
Please add or choose a namespace
InformationModel
GDS Push Mode
ProvisioningMode: active ●
enabled ●
Server Certificate
Server Certificate Groups
OpcUaServerGroup
Trusted
Issuers
Certificates
Certificate Revocation List
Remove RevocationList Entry
1
2

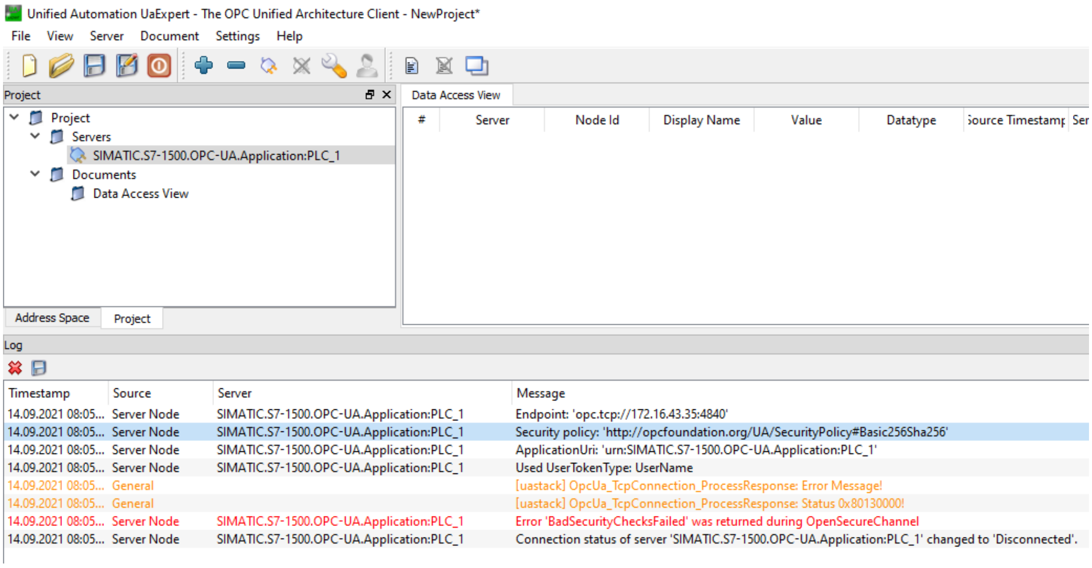
Status	Name	Valid From	Valid To	Organization
Trusted		Sep 8 08:20:10 2021 GMT	Oct 8 08:20:10 2021 GMT	Internet Widgits Pty Ltd

Number
issuer=C = DE, ST = Bayern, L = Nuernberg, O = Internet Widgits Pty L GMT nextUpdate=Oct 9 12:14:08 2(

3. Add the new Certificate Revocation List, "updatedcrl.der".
4. Click on the icon for "Apply trust list changes" to load the new Certificate Revocation List "updatedcrl.der" to the S7-1500 CPU.
   The connection to the client whose certificate has been revoked remains for the time being.

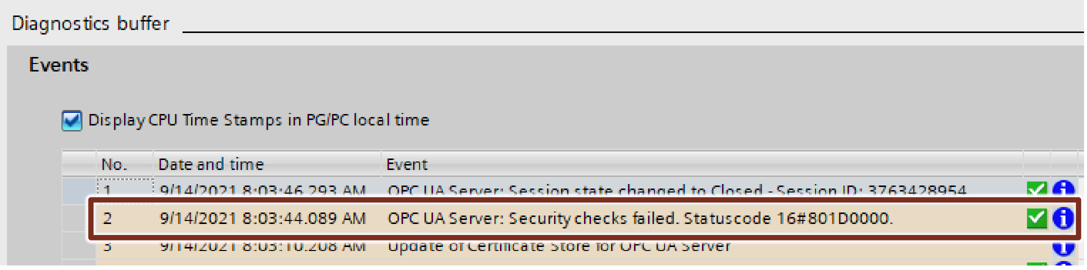
2.6.4 Testing the OPC UA connection to the S7-1500 CPU

1. Terminate the connection of the OPC UA client "UA Expert" and attempt to reestablish it. The OPC UA client "UA Expert" will show the error "BadSecurityChecksFailed".


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
Documents
Data Access View
Address Space
Project
Data Access View
# Server Node Id Display Name Value Datatype Source Timestamp Ser
Log

```
Timestamp            Source       Server                                     Message
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   Endpoint: 'opc.tcp://172.16.43.35:4840'
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   Security policy: 'http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256'
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   ApplicationUri: 'urn:SIMATIC.S7-1500.OPC-UA.Application:PLC_1'
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   Used UserTokenType: UserName
14.09.2021 08:05...  General                                                 [uastack] OpcUa_TcpConnection_ProcessResponse: Error Message!
14.09.2021 08:05...  General                                                 [uastack] OpcUa_TcpConnection_ProcessResponse: Status 0x80130000!
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   Error 'BadSecurityChecksFailed' was returned during OpenSecureChannel
14.09.2021 08:05...  Server Node  SIMATIC.S7-1500.OPC-UA.Application:PLC_1   Connection status of server 'SIMATIC.S7-1500.OPC-UA.Application:PLC_1' changed to 'Disconnected'.
```

2. In TIA Portal, establish an online connection to the S7-1500 CPU. In the "Online & diagnostics" view, navigate to "Diagnostics > Diagnostics buffer".
   In the diagnostic buffer you will see an entry for the failed connection attempt.



☑ Display CPU Time Stamps in PG/PC local time

No.	Date and time	Event
1	9/14/2021 8:03:46.293 AM	OPC UA Server: Session state changed to Closed - Session ID: 3763428954
2	9/14/2021 8:03:44.089 AM	OPC UA Server: Security checks failed. Statuscode 16#801D0000.
3	9/14/2021 8:03:10.208 AM	Update of Certificate Store for OPC UA Server

3 Useful information

3.1 Terms used

Table 3-1

Term/Abbreviation	Description
CA	Short for Certificate Authority. The CA is a trusted instance which issues digital certificates.
CRL	Certificate Revocation List This list enumerates invalid certificates. If a Certificate Authority declares a certificate to be invalid, it will enter the serial number of the certificate in the Certificate Revocation List.
CSR	A Certificate Signing Request is a digital certificate request. A digital signature and a public key are used to create a digital certificate.
"Provisioning state"	After the initial configuration of the S7-1500 CPU, no certificates are yet available for the OPC UA server. The server thus creates a temporary server certificate for itself and allows access for all clients. This state is known as "Provisioning state".

3.2 Basics of certificates

Description of certificates

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

A distinction is made between the following certificate types:

- self-signed certificates
- device certificates signed by a Certificate Authority (short: CA).

Self-signed certificate

Each participant generates its own certificate and signs it. All certificates from partner devices to which a connection needs to be established must therefore be stored beforehand.

Example applications are static configurations with a limited number of communication nodes.

Device certificate signed via a Certificate Authority

All certificates are created and signed by a certification authority. You must load the certificate from the Certificate Authority into a CPU. The Certificate Authority may generate new certificates.

Example applications include dynamically expanding systems.

Tree structures are possible within a CA. The root certificate of a CA has the capacity to sign other Sub-CA certificates, while the Sub-CA certificates have the capacity to sign other device certificates.

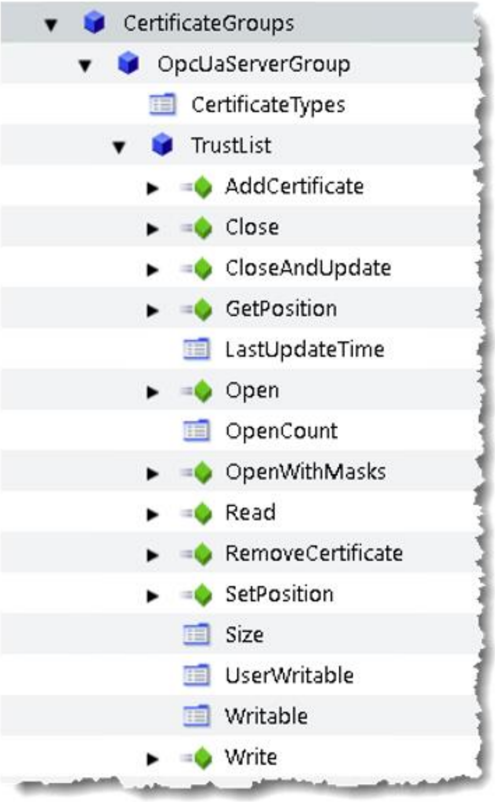
Example:

The root CA belongs to a specific company. The company operates two plants. Each plant in turn has a CA certificate signed by the root CA. The certificates of the devices can now be signed with the respective plant certificate. There may be other subordinate CA certificates, for example for the individual lines.

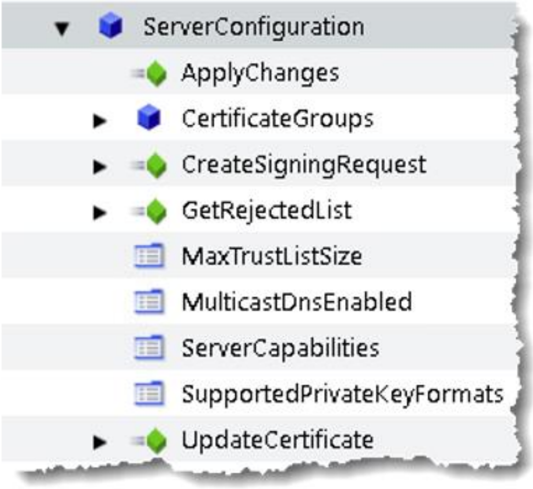
Within a CA it may be necessary to revoke certain certificates, for instance when an employee leaves the company. The Certificate Revocation List exists for this purpose. The number of the revoked certificate is noted in this list. If a device then attempts to establish a connection with this certificate, the connection partner will first check the certificate. The certificate is signed by the CA that the partner trusts. The partner then checks the revocation list of the CA and can then refuse the connection.

3.3 Information model

To dynamically set certificates for the OPC UA server, the Push Certificate Management Model has been implemented on the OPC UA server of the S7-1500 CPU per OPC UA specification. The following methods are in the address space of the OPC UA server underneath the server object; the methods can then be called by a GDS client:



- ▼ CertificateGroups
  - ▼ OpcUaServerGroup
    - CertificateTypes
    - ▼ TrustList
      - ▶ AddCertificate
      - ▶ Close
      - ▶ CloseAndUpdate
      - ▶ GetPosition
      - LastUpdateTime
      - ▶ Open
      - OpenCount
      - ▶ OpenWithMasks
      - ▶ Read
      - ▶ RemoveCertificate
      - ▶ SetPosition
      - Size
      - UserWritable
      - Writable
      - ▶ Write



- ▼ ServerConfiguration
  - ApplyChanges
  - ▶ CertificateGroups
  - ▶ CreateSigningRequest
  - ▶ GetRejectedList
  - MaxTrustListSize
  - MulticastDnsEnabled
  - ServerCapabilities
  - SupportedPrivateKeyFormats
  - ▶ UpdateCertificate

3.4 Tips in case of errors

Error loading the certificates

If it is not possible to load the certificates to the CPU, check the following points:

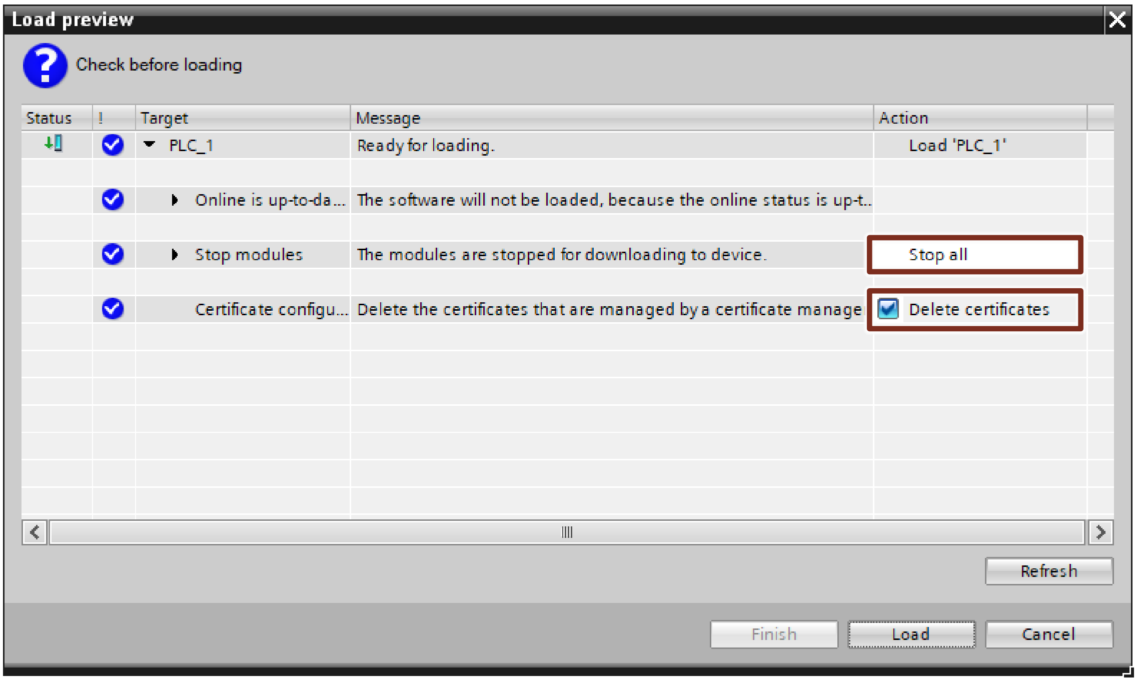
1. Is the time of the CPU or client PC set correctly?
2. Is there a message with an error number in the diagnostic buffer of the CPU?

Connection with a client no longer possible after loading certificates

If you wish to check why a client connection was rejected by the OPC UA server, open the "Online & diagnostics" view. The message in the diagnostic buffer will contain a status code which is explained in the Online Help.

It is also possible to lock yourself out with dynamic certificate handling. This happens when there is no longer any client that can establish a connection to the CPU. In this case, put the CPU back in "Provisioning state".
In the project tree, select the CPU and click "Download to device" in the function bar. In the "Load preview" dialog, enable the function "Delete certificates". In this case, downloading in "STOP" mode will be necessary.

Figure 3-1



Status	!	Target	Message	Action
	✓	PLC_1	Ready for loading.	Load 'PLC_1'
	✓	Online is up-to-da...	The software will not be loaded, because the online status is up-t..	
	✓	Stop modules	The modules are stopped for downloading to device.	Stop all
	✓	Certificate configu...	Delete the certificates that are managed by a certificate manage	☑ Delete certificates

3.5 Alternative solutions

1. In addition to the option of dynamically managing the certificates, TIA Portal V17 also makes it possible to download the certificates to the CPU statically via the hardware configuration.
2. OpenSSL is used in this example to create certificates. Other tools, such as existing company infrastructure, may also be used for this purpose.
3. SiOME provides a UI that internally calls the methods in the information model of the OPC UA server. This functionality can be used instead by other OPC UA clients. Other vendors also provide tools for the functionality of the GDS server and GDS client.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

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

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

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

support.industry.siemens.com

Technical Support

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

Please send queries to Technical Support via Web form:

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

Service offer

Our range of services includes the following:

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

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

support.industry.siemens.com/cs/sc

Industry Online Support app

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

support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109799888
\3\	Siemens OPC UA Modeling Editor (SiOME) https://support.industry.siemens.com/cs/ww/en/view/109755133

4.3 Change documentation

Table 4-2

Version	Date	Change
V1.0	09/2021	First edition