APPLICATION NOTE

AC500 V3 - ENCRYPT AND SIGN YOUR APPLICATION

Contents

1 Introduction

1.1 Scope of the document

This Application Note describes how to protect the project and the running application in an AC500 V3 PLC.

To archive this a user management is used, the communication and the boot application are encrypted with a certificate from the controller in order to prevent unauthorized access and to make sure that it cannot be exchanged.

In addition, we want to sign the application on the controller.

It is not possible to just sign the application. It's always required to encrypt the application as well. It's possible to encrypt the application without sign it.

To do this, a corresponding certificate must be created on the controller and installed in the Windows Certificate Store of your computer.

Note: Be sure you have a battery plugged to you PLC. This is required to restore the date and time inside the PLC. Certificates have always an expiration date.

All available certificates are located in the Windows Certificate Store "certmgr" on your computer. There are two types of keys:

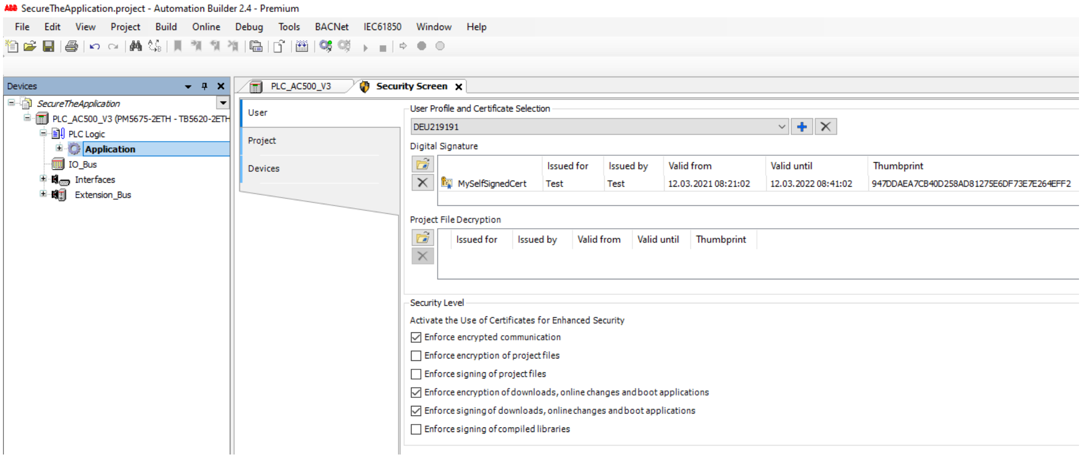
- Certificates with private keys
  - for file decryption
  - for digital signatures
- Certificates with public keys
  - for file encryption
  - for verifying digital signatures

1.2 Compatibility

The application example explained in this document have been used with the below engineering system versions. They should also work with other versions, nevertheless some small adaptations may be necessary, for future versions.

- AC500 V3 PLC
- Automation Builder V2.6.0 or newer

1.3 Overview


SecureTheApplication.project - Automation Builder 2.4 - Premium
File Edit View Project Build Online Debug Tools BACNet IEC61850 Window Help
Devices
SecureTheApplication
PLC_AC500_V3 (PM5675-2ETH - TB5620-2ETH
PLC Logic
Application
IO_Bus
Interfaces
Extension_Bus
PLC_AC500_V3
Security Screen
User
Project
Devices

User Profile and Certificate Selection

DEU219191

Digital Signature

	Issued for	Issued by	Valid from	Valid until	Thumbprint
MySelfSignedCert	Test	Test	12.03.2021 08:21:02	12.03.2022 08:41:02	947DDAEA7CB40D258AD81275E6DF73E7E264EFF2

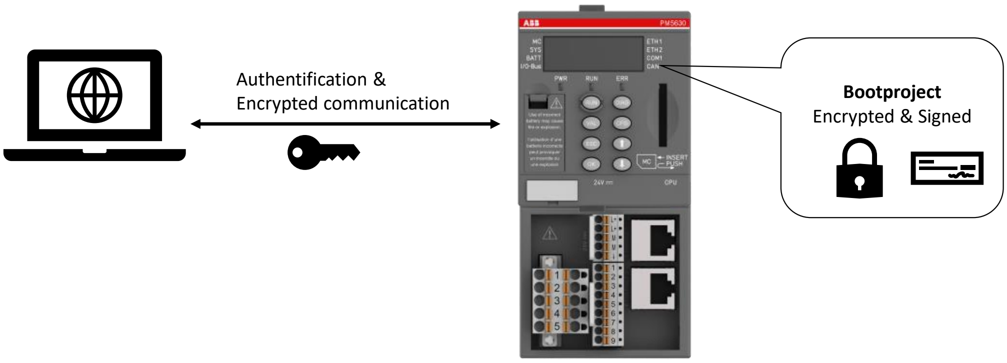
Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

- ☑ Enforce encrypted communication
- □ Enforce encryption of project files
- □ Enforce signing of project files
- ☑ Enforce encryption of downloads, online changes and boot applications
- ☑ Enforce signing of downloads, online changes and boot applications
- □ Enforce signing of compiled libraries



The steps described in this Application Note can be used to protect the Application. In the first step the communication between computer and AC500 V3 is authenticated and encrypted to make sure that no unauthorized person can access the PLC.

In the second step the download and boot application become encrypted and signed to make sure that nobody can replicate the boot application or load a not trusteed application.

2 User management and encrypted communication

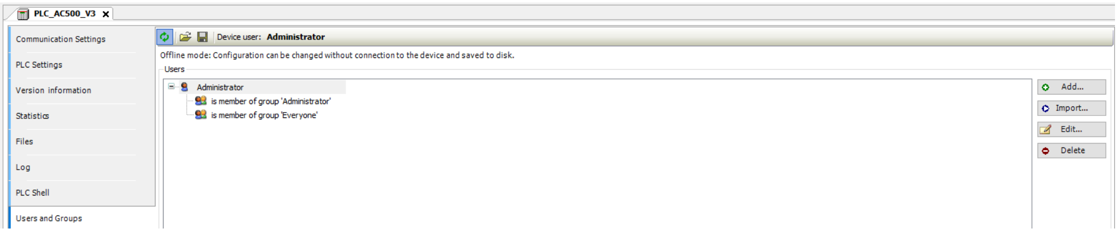
2.1 User management

To prevent that any unauthorized person can access the PLC, overwrite the Application, change the firmware or similar a User Management is needed.

How the User Management can be activated and configured is described in the Application Note AC500 User Management with V3 in chapter 2.2 in this example the default user Management is used.

⚠	CAUTION! **Please check and remember your Administrator password.** **There is also no workaround to login to the PLC without this password. If this happens, the PLC must be replaced!**

Only an Administrator has been added to the user management and the password has been set.



PLC_AC500_V3

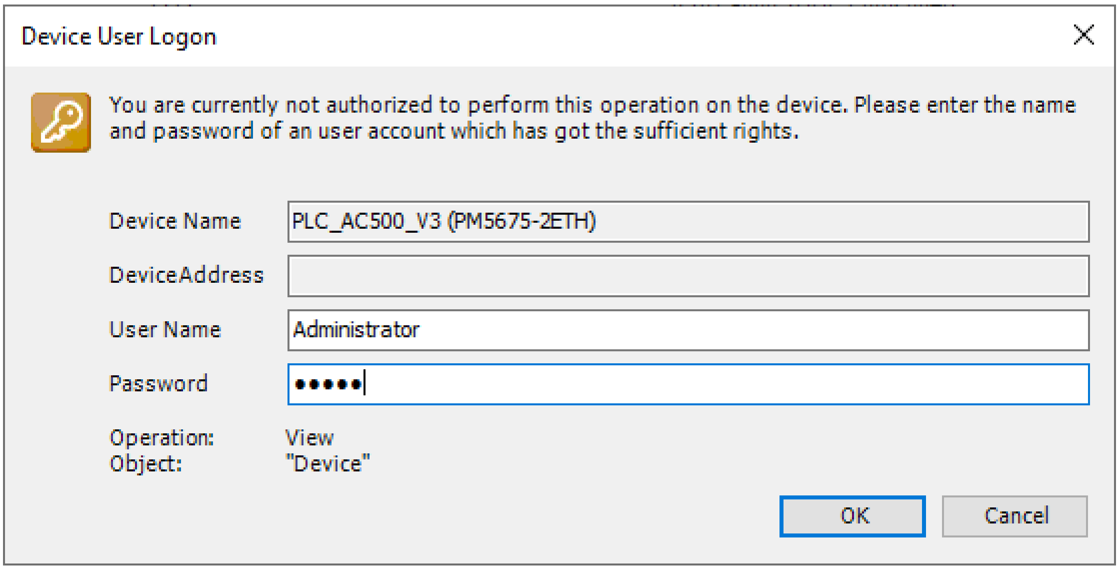
Device user: **Administrator**

Offline mode: Configuration can be changed without connection to the device and saved to disk.

Users

- Administrator
  - is member of group 'Administrator'
  - is member of group 'Everyone'

If now a project should be downloaded an authorized user needs to log in.



Device User Logon

You are currently not authorized to perform this operation on the device. Please enter the name and password of an user account which has got the sufficient rights.

Device Name: PLC_AC500_V3 (PM5675-2ETH)

DeviceAddress:

User Name: Administrator

Password: •••••

Operation: View

Object: "Device"

If a user who don’t has username and password tries to log in or update the firmware is not able to as he has insufficient rights. Each successful or failed login attempt will be tracked inside the Audit Log of the PLC.

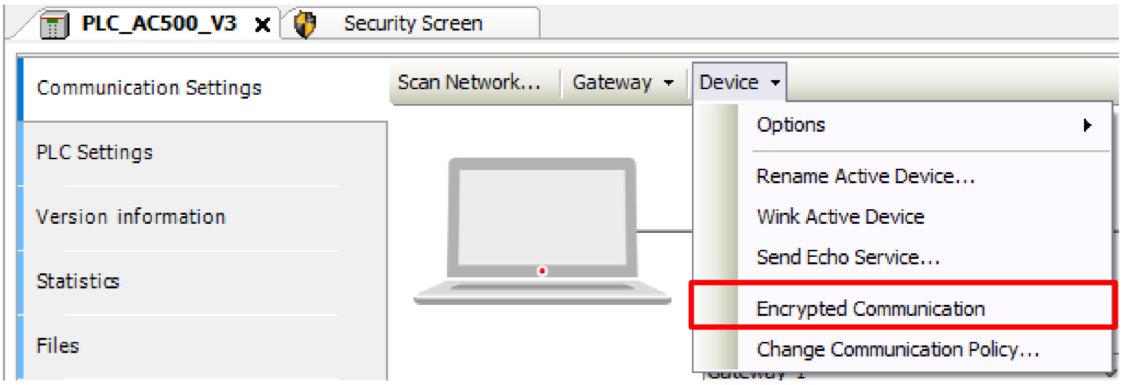
2.2 Encrypted communication

As described in the last chapter only authorized user can log in to the PLC.

To ensure that nobody can read the login data you sent from your computer to the PLC an encrypted communication must be used. The steps to archive this are also described in the Application Note AC500 User Management with V3 in the chapter 2.2.1.4.

Afterwards go to the Communication Settings.

1. In the tab “Device” choose “Encrypted Communication”

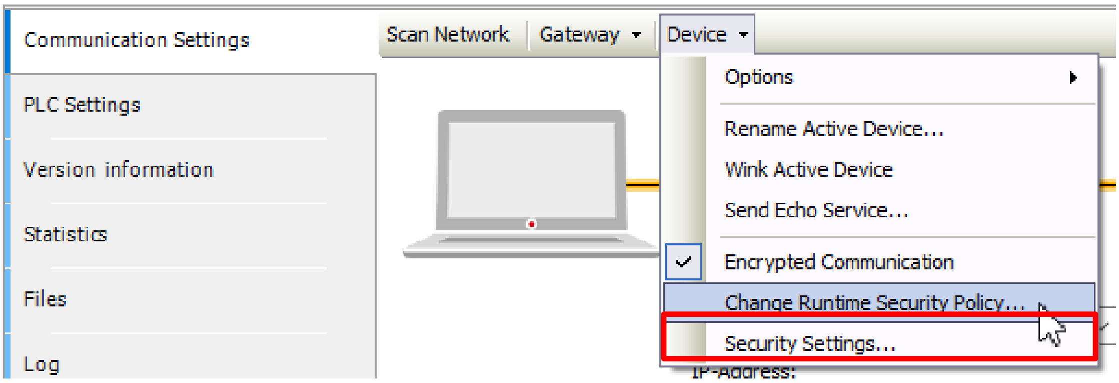


Now the communication between the PLC and the PC is encrypted so that nobody can get any log in information or read any system values. This setting is only done locally on your Automation Builder and will be saved within the project.

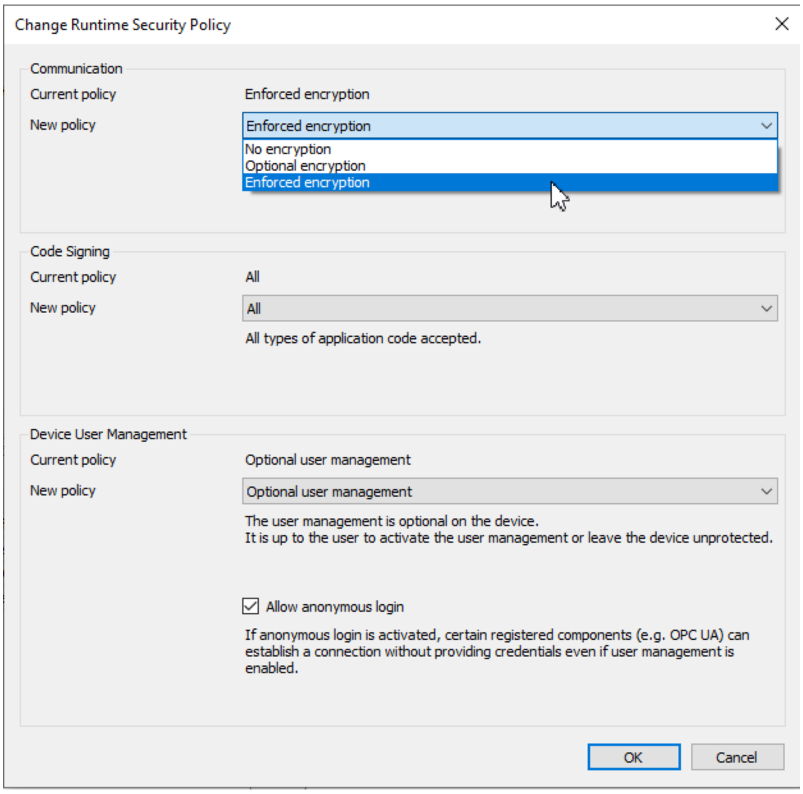
Note: In case you want to login from different computers to the controller, you will need the appropriate certificate for each computer. Otherwise the communication from other PCs is not encrypted and attackers could read confidential data.

In the next step the comunication policy from the device is changed to allow only encrypted communication. Then it is not possible to log in without an encrypted communication.

2. Click “Change Communication Policy”



3. Change the communication policy to “Enforced encryption”



Change Runtime Security Policy

Communication

Current policy: Enforced encryption

New policy: Enforced encryption

No encryption
Optional encryption
Enforced encryption

Code Signing

Current policy: All

New policy: All

All types of application code accepted.

Device User Management

Current policy: Optional user management

New policy: Optional user management

The user management is optional on the device.
It is up to the user to activate the user management or leave the device unprotected.

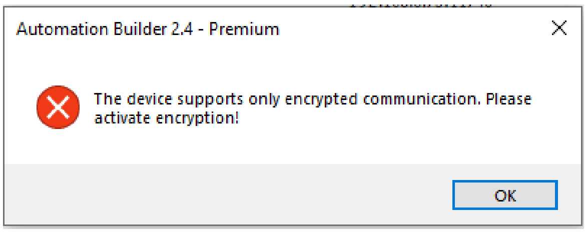
☑ Allow anonymous login

If anonymous login is activated, certain registered components (e.g. OPC UA) can establish a connection without providing credentials even if user management is enabled.

It is also possible to force the usermanagement here. Then it is not possible to delete the usermanagement from the PLC. The settings to force the signing of an application is described in chapter 5.2.

In the next step the communication from another PC to this PLC shall be established.

4. When trying to log in without encrypted communication following error will pop up

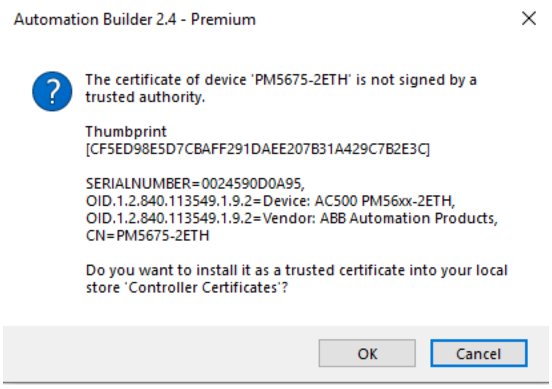


Automation Builder 2.4 - Premium

The device supports only encrypted communication. Please activate encryption!

5. Use also on the second computer encrypted communication like shown in step 1

6. With the next login the certificate for the encrypted communication will be stored in your certificate manager on your PC. Click “OK” to confirm



Automation Builder 2.4 - Premium

The certificate of device 'PM5675-2ETH' is not signed by a trusted authority.

Thumbprint
[CF5ED98E5D7CBAFF291DAEE207B31A429C7B2E3C]

SERIALNUMBER=0024590D0A95,
OID.1.2.840.113549.1.9.2=Device: AC500 PM56xx-2ETH,
OID.1.2.840.113549.1.9.2=Vendor: ABB Automation Products,
CN=PM5675-2ETH

Do you want to install it as a trusted certificate into your local store 'Controller Certificates'?

3 Encrypt the application with certificate

In addition to secure the communication to the PLC also the stored boot application can be encrypted to make sure that nobody who could access the PLC is able to duplicate the existing boot application for other PLCs.

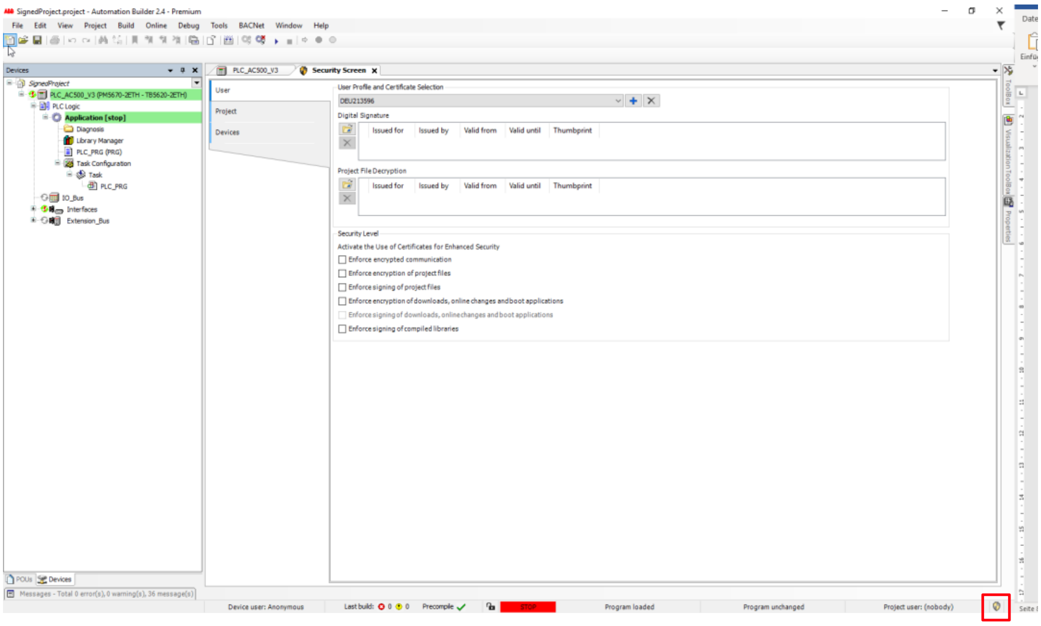
In this chapter, the boot application, Download and Online Change gets encrypted.

There is a project with an application that must be downloaded to the controller as an encrypted boot application. In the Windows Certificate Store of a computer, the certificate of this controller for encrypting the application will be installed.

☝	Note: In case you want to download the application to different controllers, you will need the appropriate certificate for each controller.

1. Login to your PLC

2. Open the “Security-Screen” view by double-clicking the 🛡 symbol in the status bar or by clicking “View → Security-Screen”



User Profile and Certificate Selection

DEU213596

Digital Signature

Project File Decryption

Security Level

Activate the Use of Certificates for Enhanced Security

☐ Enforce encrypted communication

☐ Enforce encryption of project files

☐ Enforce signing of project files

☐ Enforce encryption of downloads, online changes and boot applications

☐ Enforce signing of downloads, online changes and boot applications

☐ Enforce signing of compiled libraries

Messages - Total 0 error(s), 0 warning(s), 36 message(s)

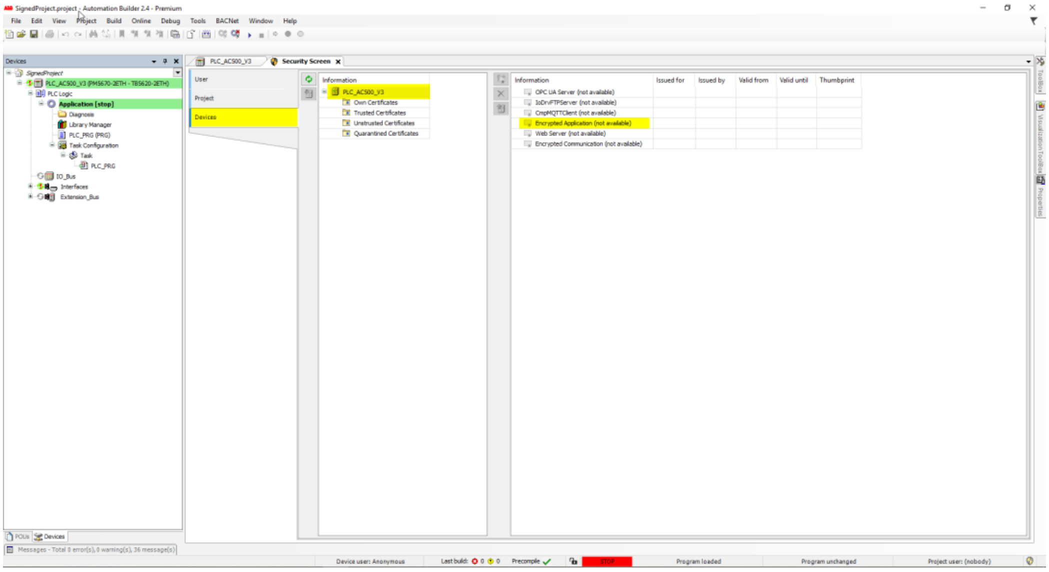
Device user: Anonymous

Last build: 0 0

Precompile ✓

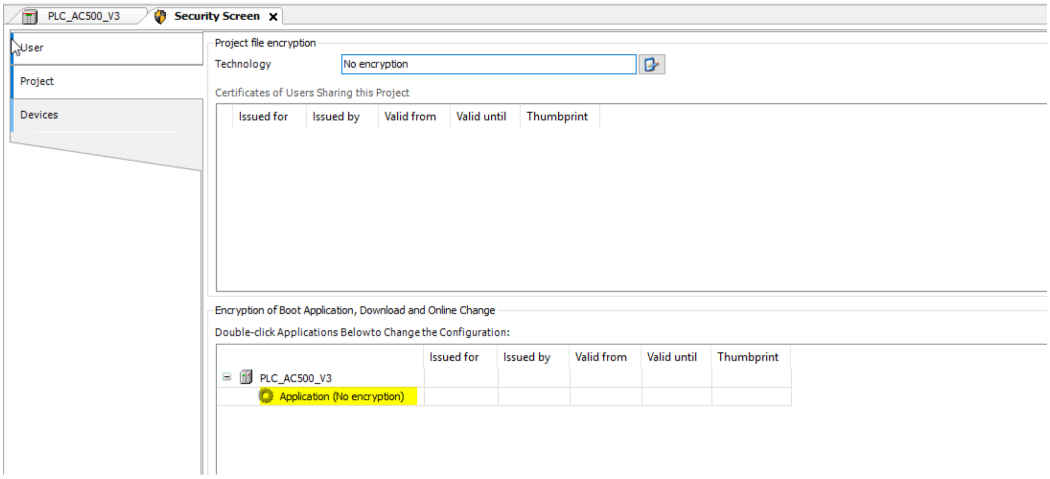
Project user: (nobody)

3. Go to “Devices” tab and click the ⟳ button to refresh the list of available devices and their certificate store
   You can see that there are no certificates available. If the certificate already exists,
   some of the steps below can be skipped.



Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
IoDrvFTPServer (not available)					
CmpMQTTClient (not available)					
Encrypted Application (not available)					
Web Server (not available)					
Encrypted Communication (not available)					

4. Open the “Project” tab and double-click the “Application” entry in the area “Encryption of boot application, download, and online change”



Project file encryption

Technology: No encryption

Certificates of Users Sharing this Project

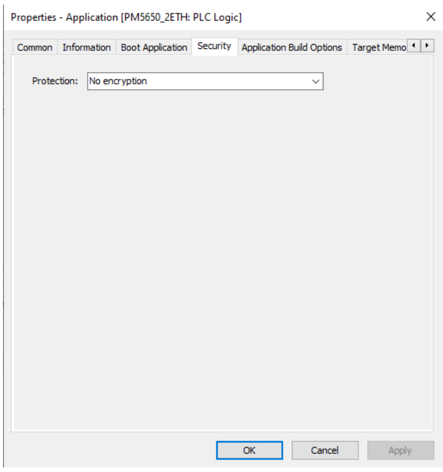
Issued for	Issued by	Valid from	Valid until	Thumbprint

Encryption of Boot Application, Download and Online Change

Double-click Applications Belowto Change the Configuration:

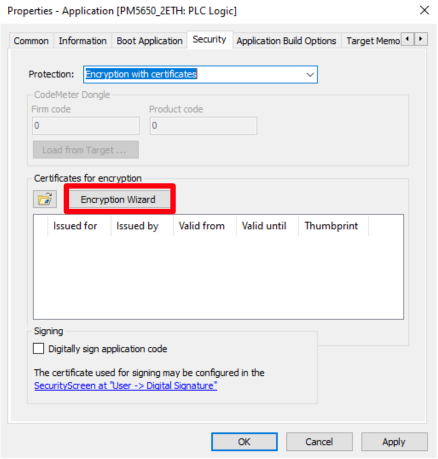
	Issued for	Issued by	Valid from	Valid until	Thumbprint
PLC_AC500_V3					
Application (No encryption)					

5. The “Properties” dialog of the Application opens


Properties - Application [PM5650_2ETH: PLC Logic]
Common
Information
Boot Application
Security
Application Build Options
Target Memo
OK
Cancel
Apply

Protection: No encryption

6. Select the “Security” tab and select “Encryption with certificates” as the “Protection”.



Properties - Application [PM5650_2ETH: PLC Logic]

Protection: Encryption with certificates

CodeMeter Dongle

Firm code: 0

Product code: 0

Certificates for encryption

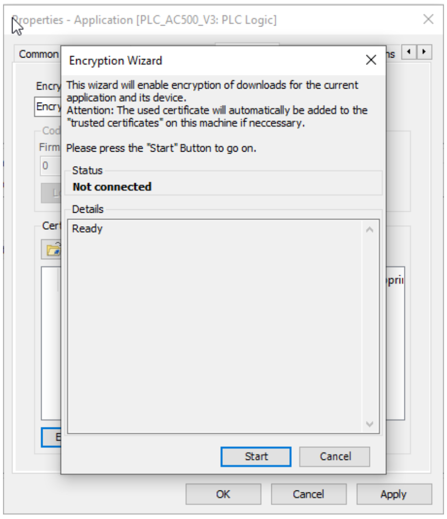
Issued for	Issued by	Valid from	Valid until	Thumbprint

Signing

☐ Digitally sign application code

The certificate used for signing may be configured in the SecurityScreen at "User -> Digital Signature"

7. Click on the “Encryption Wizard” button



Properties - Application [PLC_AC500_V3: PLC Logic]

Encryption Wizard

This wizard will enable encryption of downloads for the current application and its device.
Attention: The used certificate will automatically be added to the "trusted certificates" on this machine if neccessary.

Please press the "Start" Button to go on.

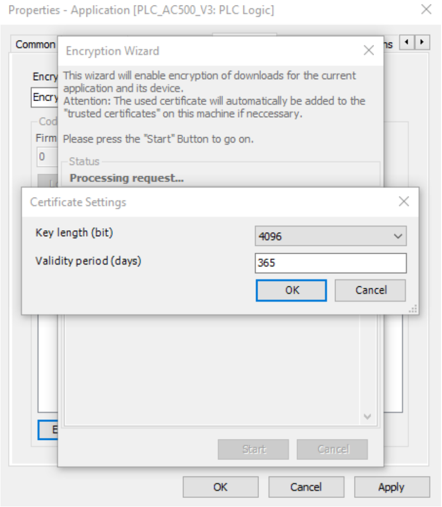
Status

Not connected

Details

Ready

8. Click on “Start” and select the Key Length “4096” and the Validity period in days:



Properties - Application [PLC_AC500_V3: PLC Logic]

Encryption Wizard

This wizard will enable encryption of downloads for the current application and its device.
Attention: The used certificate will automatically be added to the "trusted certificates" on this machine if neccessary.

Please press the "Start" Button to go on.

Status

Processing request...

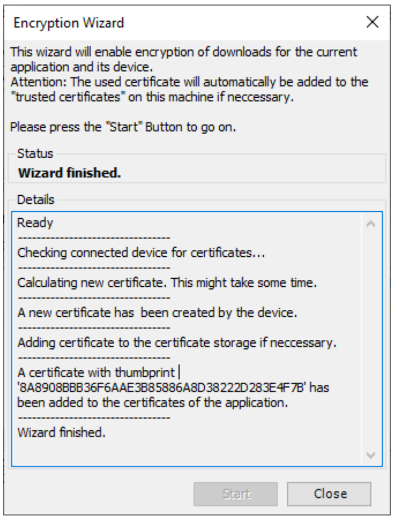
Certificate Settings

Key length (bit): 4096

Validity period (days): 365

9. Confirm with “OK”

10. The server certificate on the PLC will be created. Also, the certificate will be installed on the Cert store in Windows.



Encryption Wizard

This wizard will enable encryption of downloads for the current application and its device.
Attention: The used certificate will automatically be added to the "trusted certificates" on this machine if neccessary.

Please press the "Start" Button to go on.

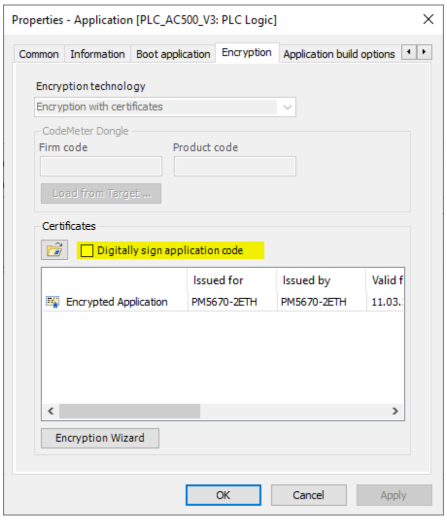
Status
Wizard finished.

Details

```
Ready
--------------------------------
Checking connected device for certificates...
--------------------------------
Calculating new certificate. This might take some time.
--------------------------------
A new certificate has  been created by the device.
--------------------------------
Adding certificate to the certificate storage if neccessary.
--------------------------------
A certificate with thumbprint |
'8A8908BBB36F6AAE3B85886A8D38222D283E4F7B' has
been added to the certificates of the application.
--------------------------------
Wizard finished.
```

11. Click “Close”

12. The certificate is automatically added for the encrypted application. Please remove the checkbox for “Digitally signing application code” if it is set.
    This will be handled in chapter 5.



Properties - Application [PLC_AC500_V3: PLC Logic]

Encryption technology: Encryption with certificates

CodeMeter Dongle

Firm code

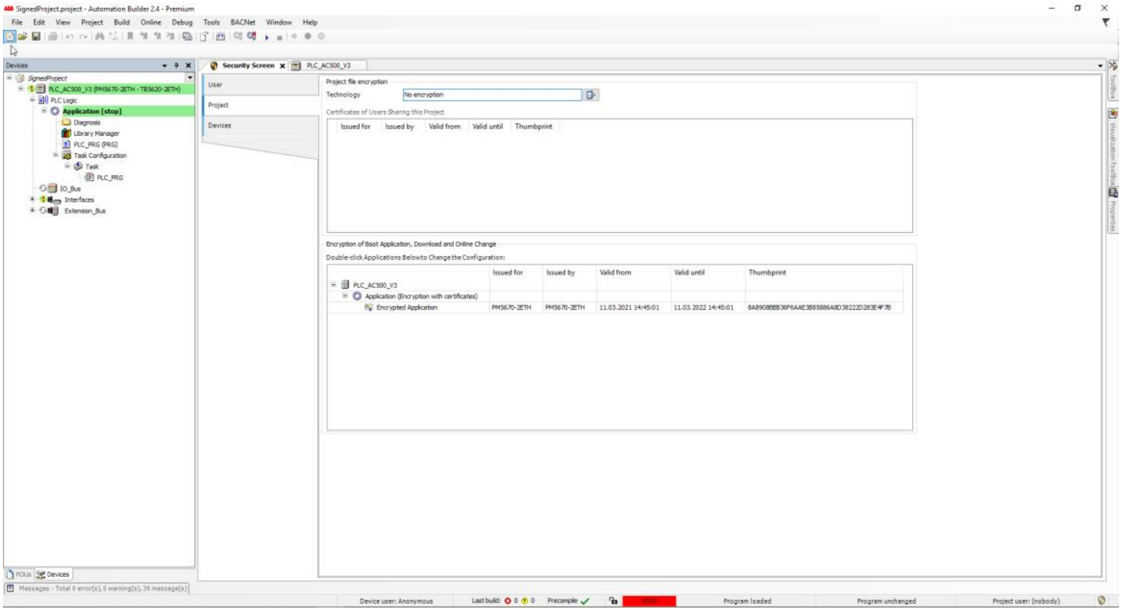
Product code

Certificates

□ Digitally sign application code

	Issued for	Issued by	Valid f
Encrypted Application	PM5670-2ETH	PM5670-2ETH	11.03.

13. Confirm with “OK” and find then encrypted application added



Project file encryption

Technology: No encryption

Certificates of Users Sharing this Project

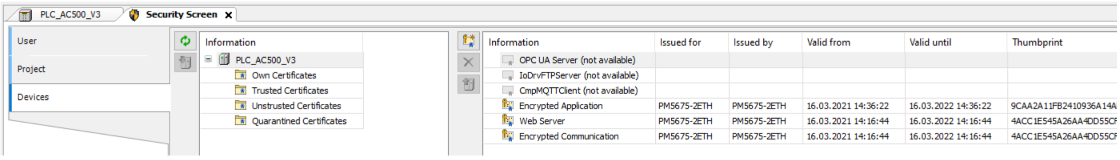
Issued for	Issued by	Valid from	Valid until	Thumbprint

Encryption of Boot Application, Download and Online Change

Double-click Applications Belowto Change the Configuration:

	Issued for	Issued by	Valid from	Valid until	Thumbprint
PLC_AC500_V3					
Application (Encryption with certificates)					
Encrypted Application	PM5670-2ETH	PM5670-2ETH	11.03.2021 14:45:01	11.03.2022 14:45:01	8A89088BB36F6AAE3B85886A8D38222D283E4F7B

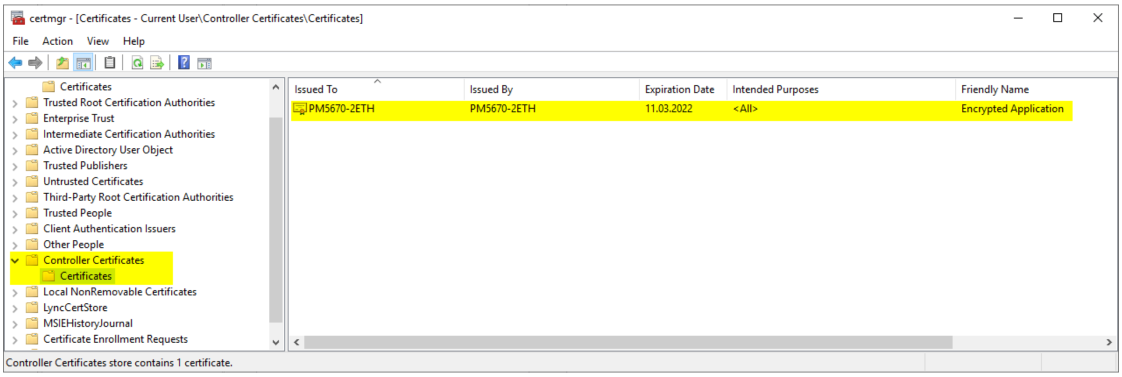
14. Go to “Devices” tab and click the ♻ button to refresh the list of available devices and their certificate store
    You can see that the certificate is available



Information
PLC_AC500_V3
Own Certificates
Trusted Certificates
Unstrusted Certificates
Quarantined Certificates

Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
IoDrvFTPServer (not available)					
CmpMQTTClient (not available)					
Encrypted Application	PM5675-2ETH	PM5675-2ETH	16.03.2021 14:36:22	16.03.2022 14:36:22	9CAA2A11FB2410936A14A
Web Server	PM5675-2ETH	PM5675-2ETH	16.03.2021 14:16:44	16.03.2022 14:16:44	4ACC1E545A26AA4DD55CF
Encrypted Communication	PM5675-2ETH	PM5675-2ETH	16.03.2021 14:16:44	16.03.2022 14:16:44	4ACC1E545A26AA4DD55CF

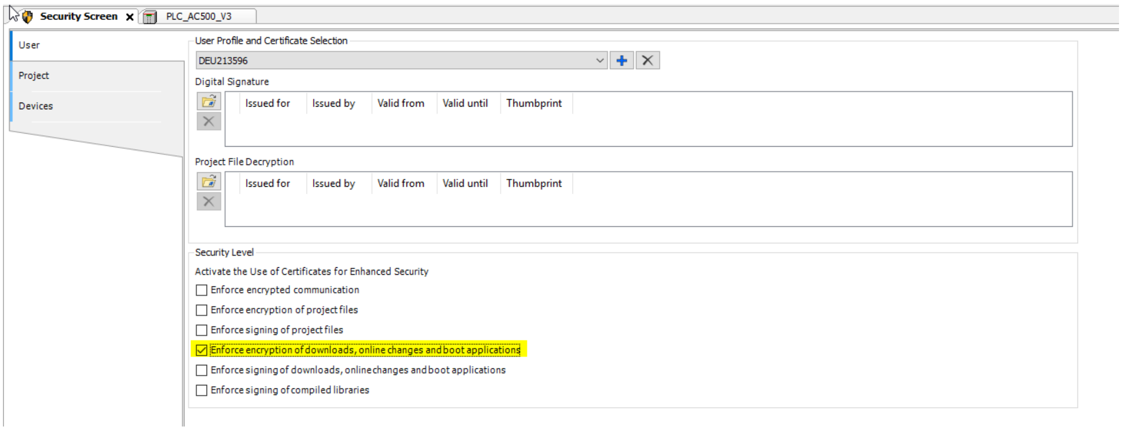
15. When you go to your **certmgr.msc**, see chapter 4 step 4, navigate to “Controller Certificates” you can see the installed certificate on your Certificate Store on Windows


certmgr - [Certificates - Current User\Controller Certificates\Certificates]
File
Action
View
Help
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Controller Certificates
Certificates
Local NonRemovable Certificates
LyncCertStore
MSIEHistoryJournal
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
PM5670-2ETH	PM5670-2ETH	11.03.2022	<All>	Encrypted Application

Controller Certificates store contains 1 certificate.

16. Open the “Users” tab in the “Security-Screen”.
Activate the option “Enforce encryption of downloads, online changes, and boot applications” in the “Security-Level” area.



User Profile and Certificate Selection

DEU213596

Digital Signature

Issued for	Issued by	Valid from	Valid until	Thumbprint

Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

☐ Enforce encrypted communication
☐ Enforce encryption of project files
☐ Enforce signing of project files
☑ Enforce encryption of downloads, online changes and boot applications
☐ Enforce signing of downloads, online changes and boot applications
☐ Enforce signing of compiled libraries

17. Logout of the PLC

18. Select Build → Clean All

19. Login to the PLC

20. The certificate is now used to encrypt the application.

4 Create self-signed certificates with Win10

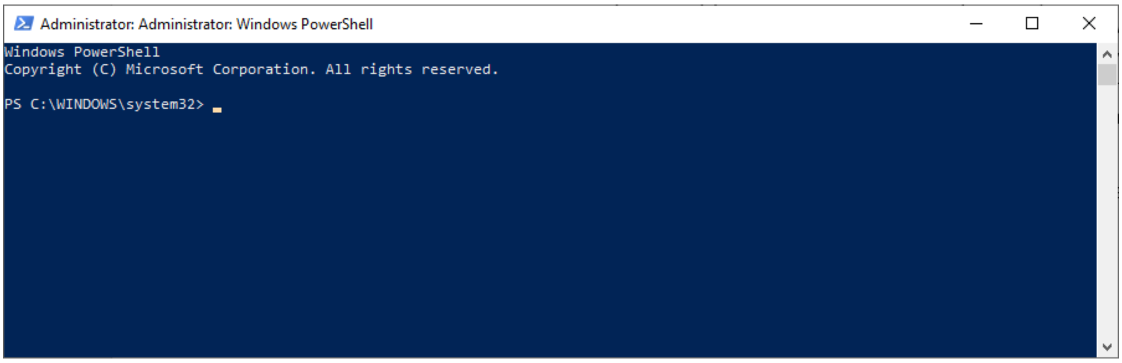
In the face of increasing security precautions and security issues, it has become of fundamental importance to websites and services to be implemented with always activated security. Various service providers now need secure connections, also for development environments. In most cases it is not possible to use cryptographic certificates for the local development environment any developer, but you can easily get self-signed certificates for free.

These certificates can be used in local environments and cover the security requirements during the development of the solution.

⚠	CAUTION! **Self-signed certificates should NEVER be used on production or public websites and networks.**

PowerShell in Windows 10 includes the command **New-SelfSignedCertificate**. This command can be used to create self-signed certificates.

1. Open a PowerShell window in Administrator mode



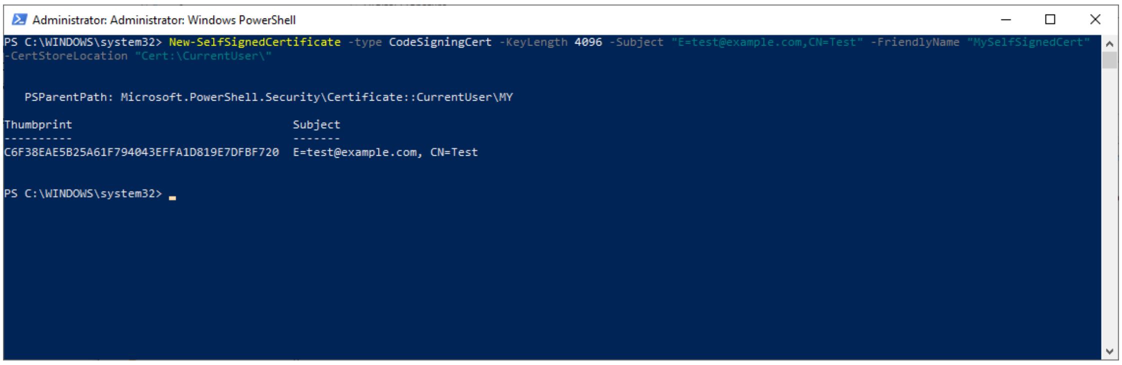
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> _
```

2. Enter the following command:

New-SelfSignedCertificate -type CodeSigningCert -KeyLength 4096 -Subject "E=test@example.com,CN=Test" -FriendlyName "SelfSignedCertForSigning" -CertStoreLocation "Cert:\CurrentUser\"

3. The result will be a Thumbprint



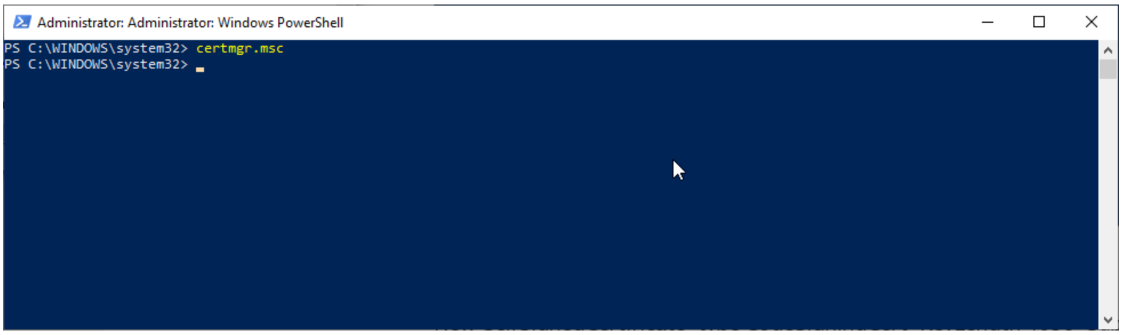
```
PS C:\WINDOWS\system32> New-SelfSignedCertificate -type CodeSigningCert -KeyLength 4096 -Subject "E=test@example.com,CN=Test" -FriendlyName "MySelfSignedCert"
-CertStoreLocation "Cert:\CurrentUser\"


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\MY

Thumbprint                                Subject
----------                                -------
C6F38EAE5B25A61F794043EFFA1D819E7DFBF720  E=test@example.com, CN=Test


PS C:\WINDOWS\system32> _
```

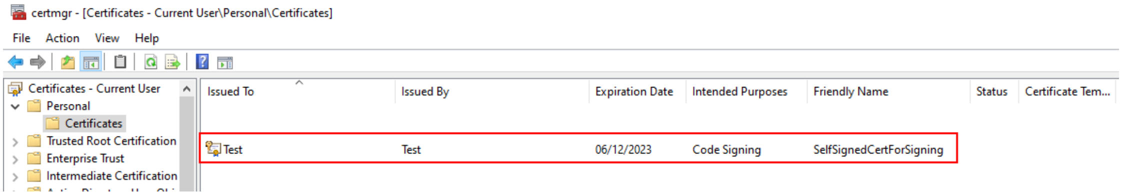
4. Start the **certmgr.msc** via PowerShell



Administrator: Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> certmgr.msc
PS C:\WINDOWS\system32> _
```

5. A new window will open
   Navigate to Personal→ Certificates
   Here you can see the currently created self-signed certificate with private key



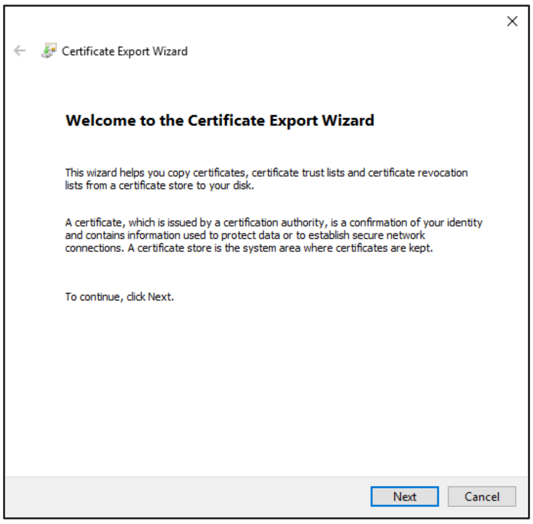
certmgr - [Certificates - Current User\Personal\Certificates]

File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Test	Test	06/12/2023	Code Signing	SelfSignedCertForSigning		

6. Select the Test certificate, right click and select:
   All Tasks -> Export...

7. Click Next



Certificate Export Wizard

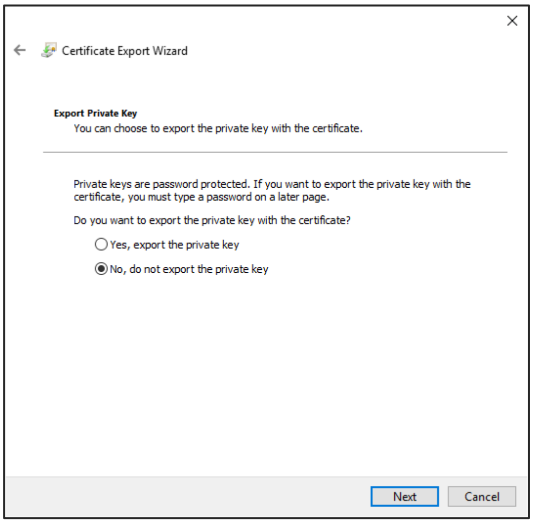
Welcome to the Certificate Export Wizard

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

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

To continue, click Next.

8. Select: **No, do not export the private key**



Export Private Key

You can choose to export the private key with the certificate.

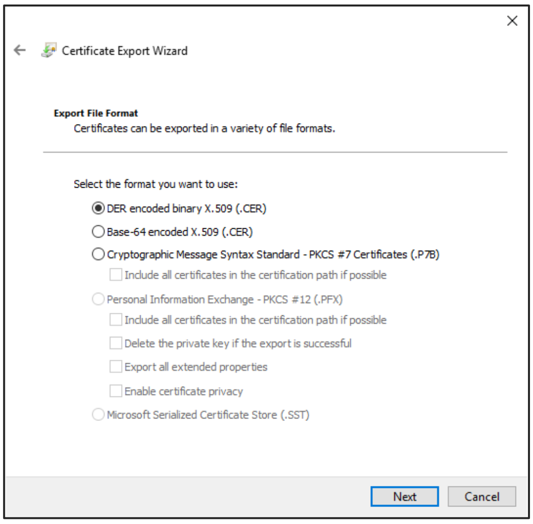
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

9. Select **DER encoded binary X.509 (.CER)**



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

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

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

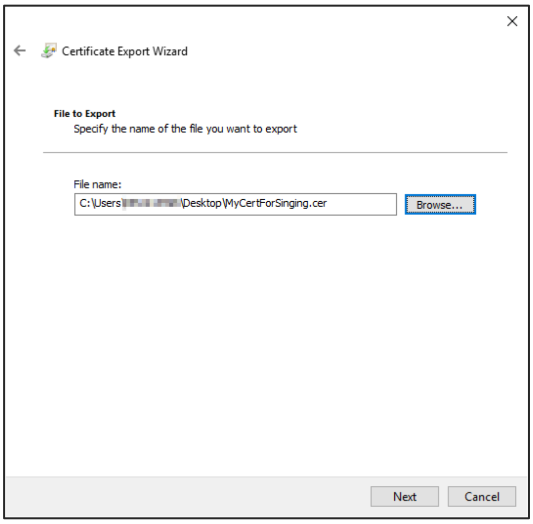
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

10. Choose a path and name e.g. **MyCertForSinging.cer** to store the certificate. Confirm with Next



Certificate Export Wizard

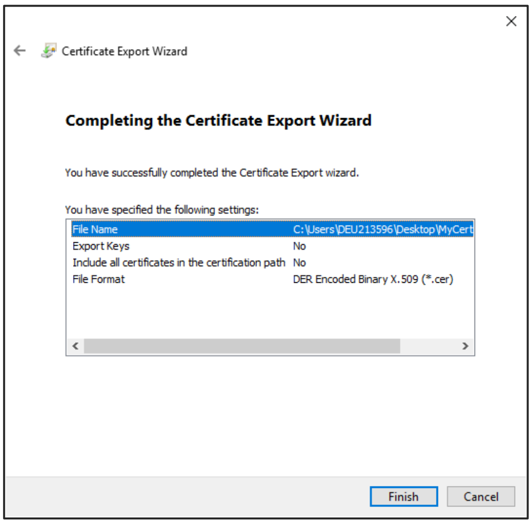
File to Export

Specify the name of the file you want to export

File name:

C:\Users\[redacted]\Desktop\MyCertForSinging.cer

11. The final result will be shown:



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\DEU213596\Desktop\MyCert
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

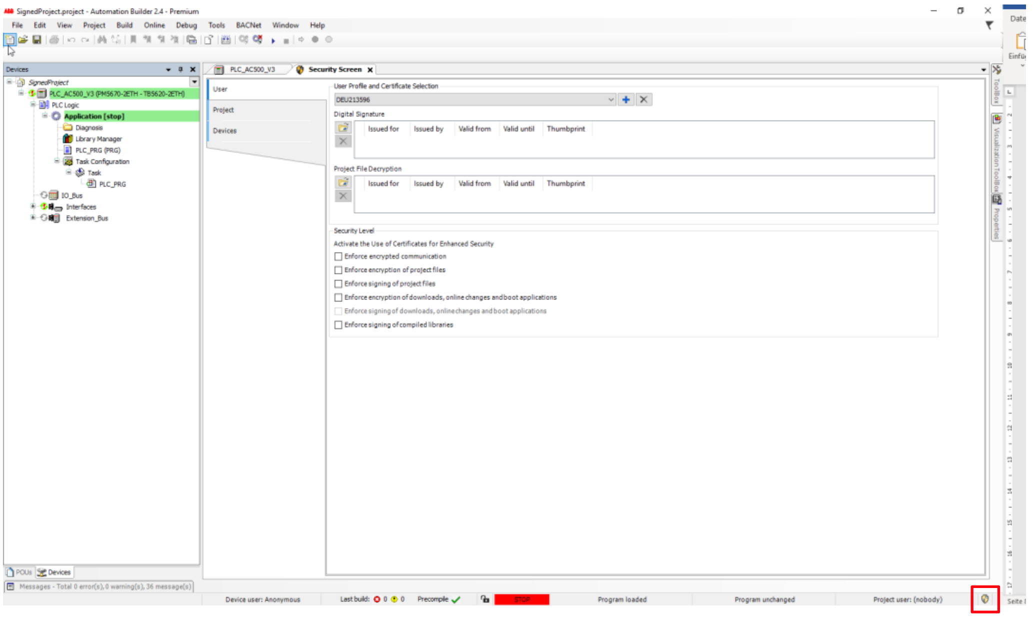
12. Confirm with Finish

5 Sign the application with certificate

In this step, boot application becomes signed. Currently AB allows only to sign the application, when you also encrypt the application. The encryption of the application was already handled in chapter 3.

5.1 Import Certificate into Automation Builder

1. Open the “Security-Screen” view by double-clicking the 🛡 symbol in the status bar or by clicking “View → Security-Screen”



User Profile and Certificate Selection

DEU213596

Digital Signature

Issued for	Issued by	Valid from	Valid until	Thumbprint

Project File Decryption

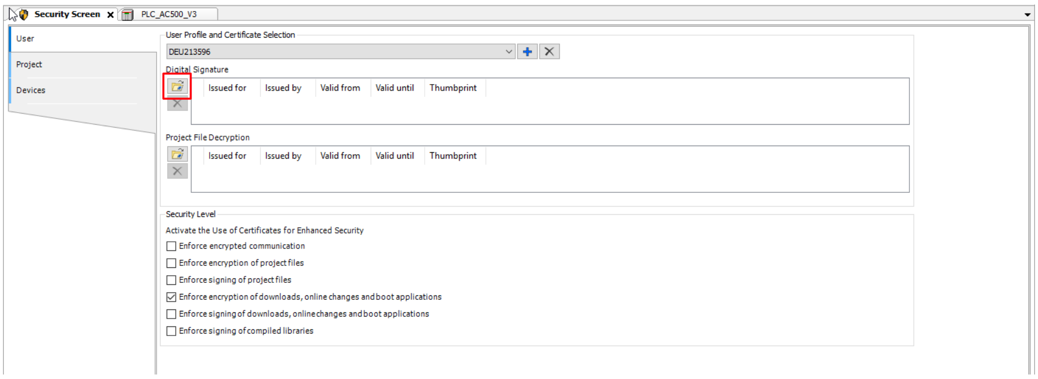
Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

- ☐ Enforce encrypted communication
- ☐ Enforce encryption of project files
- ☐ Enforce signing of project files
- ☐ Enforce encryption of downloads, online changes and boot applications
- ☐ Enforce signing of downloads, online changes and boot applications
- ☐ Enforce signing of compiled libraries

2. In the “User” tab, select the user profile for which the communication will be encrypted. By default, the specified user profile is the one you have used on your computer to sign into Windows.



User Profile and Certificate Selection

DEU213596

Digital Signature

Issued for	Issued by	Valid from	Valid until	Thumbprint

Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

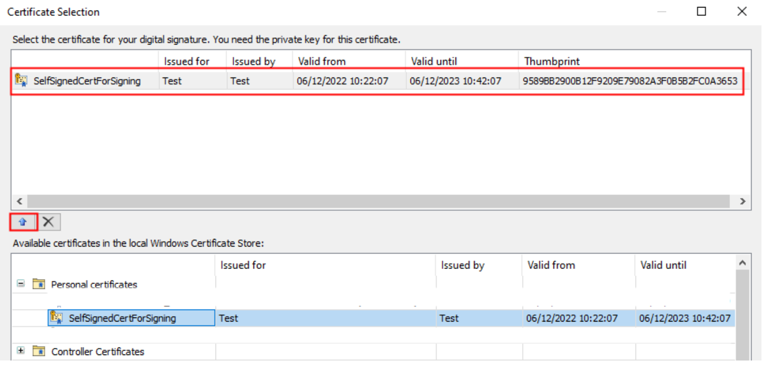
Security Level

Activate the Use of Certificates for Enhanced Security

- ☐ Enforce encrypted communication
- ☐ Enforce encryption of project files
- ☐ Enforce signing of project files
- ☑ Enforce encryption of downloads, online changes and boot applications
- ☐ Enforce signing of downloads, online changes and boot applications
- ☐ Enforce signing of compiled libraries

3. Click the 📂 button in the “Digital signature” area. The “Certificate Selection” dialog opens.

4. Select the certificate with a private key from the list “Personal certificates” which was created in chapter 4.
   Certificates with a private key are identified by the 🔑 symbol.



Certificate Selection

Select the certificate for your digital signature. You need the private key for this certificate.

	Issued for	Issued by	Valid from	Valid until	Thumbprint
SelfSignedCertForSigning	Test	Test	06/12/2022 10:22:07	06/12/2023 10:42:07	9589BB2900B12F9209E79082A3F0B5B2FC0A3653

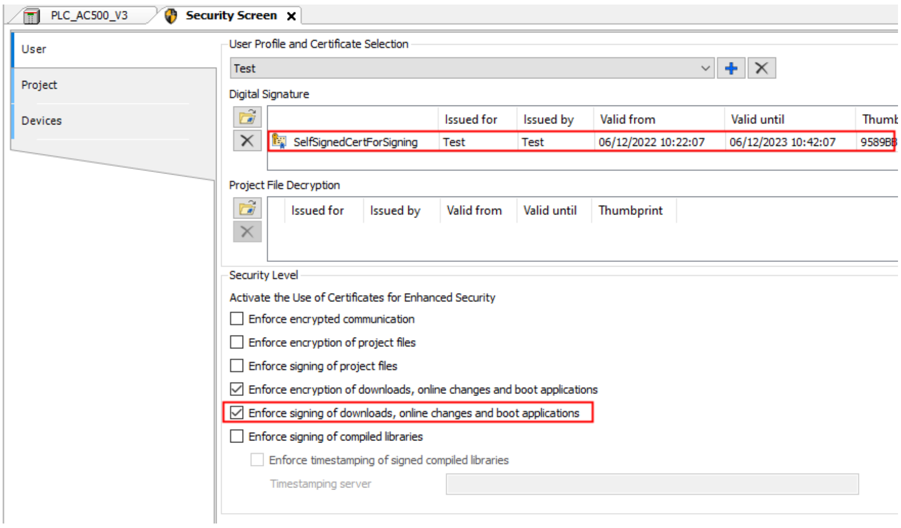
Available certificates in the local Windows Certificate Store:

	Issued for	Issued by	Valid from	Valid until
⊟ Personal certificates				
SelfSignedCertForSigning	Test	Test	06/12/2022 10:22:07	06/12/2023 10:42:07
⊞ Controller Certificates				

5. Click on the arrow up ⇧ button to add the certificate to the upper part of the dialog

6. Click “OK” to confirm your selection. The selected certificate is displayed in the “Security Screen” in the “Digital signature” area.

7. Activate the option “Enforce signing of downloads, online changes and boot applications” in the “Security-Level” area.



User Profile and Certificate Selection

Test

Digital Signature

	Issued for	Issued by	Valid from	Valid until	Thumt
SelfSignedCertForSigning	Test	Test	06/12/2022 10:22:07	06/12/2023 10:42:07	9589BB

Project File Decryption

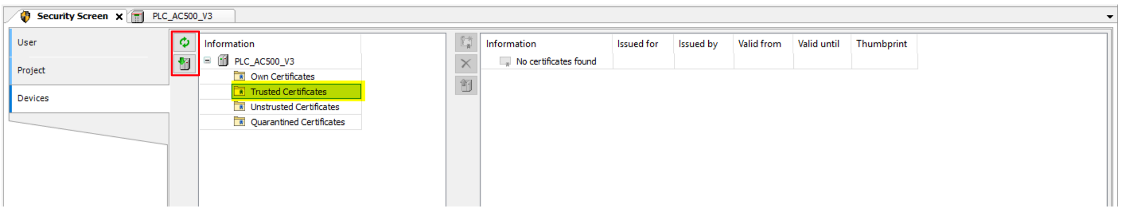
Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

☐ Enforce encrypted communication
☐ Enforce encryption of project files
☐ Enforce signing of project files
☑ Enforce encryption of downloads, online changes and boot applications
☑ Enforce signing of downloads, online changes and boot applications
☐ Enforce signing of compiled libraries
☐ Enforce timestamping of signed compiled libraries
Timestamping server

8. Go to “Devices” tab and click the ⟳ button to refresh the list of available devices and their certificate store.
   Select “Trusted Certificates”

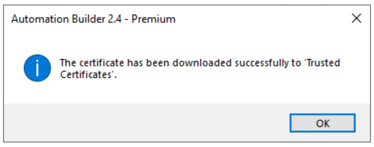


Information
⊟ PLC_AC500_V3
Own Certificates
Trusted Certificates
Unstrusted Certificates
Quarantined Certificates

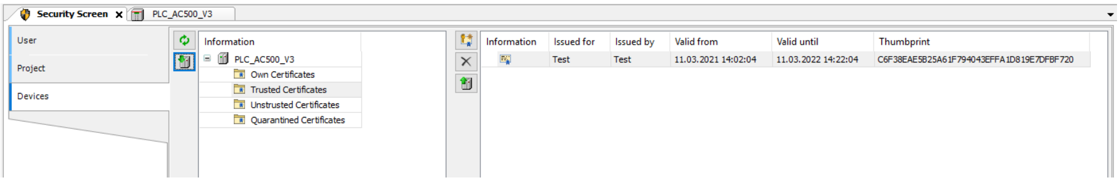
Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
No certificates found					

9. Import the certificate (**MyCertForSinging.cer**), created in chapter: 4, to the “Trusted Certificates” in your PLC, using the 📥 symbol.

10. Once imported the confirmation screen appears


The certificate has been downloaded successfully to 'Trusted Certificates'.

11. The imported certificate is now visible in the “Trusted Certificates” area.


Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
	Test	Test	11.03.2021 14:02:04	11.03.2022 14:22:04	C6F38EAE5B25A61F794043EFFA1D819E7DFBF720

12. Logout of the PLC

13. Select Build → Clean All

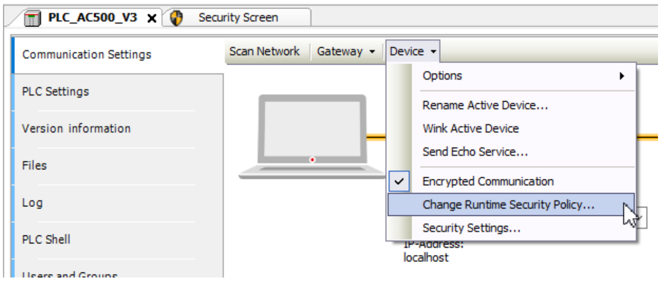
14. Login to the PLC

5.2 Change policy to signed only

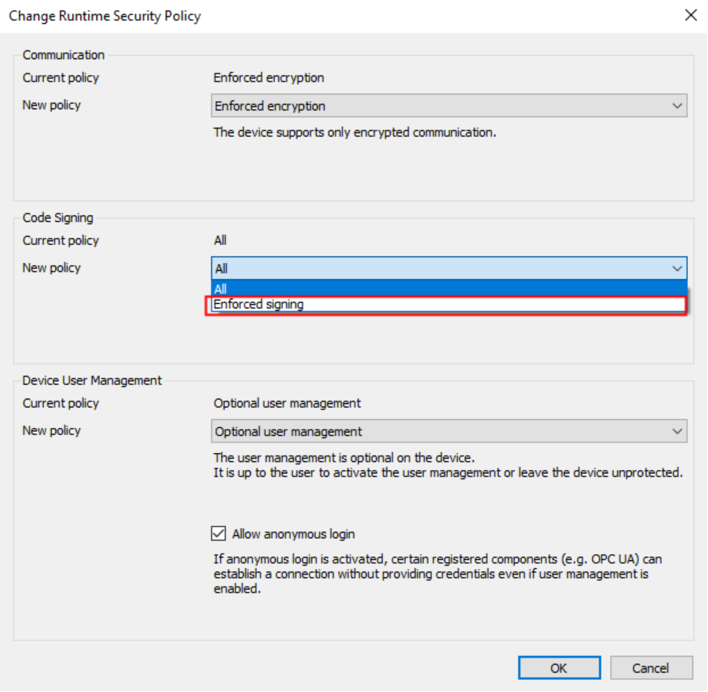
In the last chapter the signing in one project was activated. But another project which is not encrypted & signed can also be loaded from the CPU. In this chapter it is explained how to enforce the signing of projects.

1. Open the Communication Settings

2. Click Device → Change Runtime Security Policy…



3. In the section Code Signing the policy is changed to Enforced signing



Change Runtime Security Policy

Communication

Current policy: Enforced encryption

New policy: Enforced encryption

The device supports only encrypted communication.

Code Signing

Current policy: All

New policy: All

Device User Management

Current policy: Optional user management

New policy: Optional user management

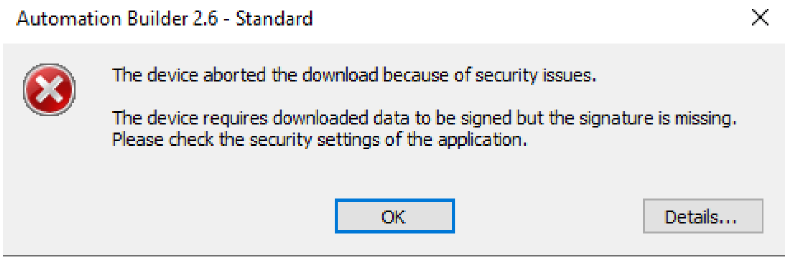
The user management is optional on the device.
It is up to the user to activate the user management or leave the device unprotected.

☑ Allow anonymous login

If anonymous login is activated, certain registered components (e.g. OPC UA) can establish a connection without providing credentials even if user management is enabled.

4. Confirm with OK

In future, only signed boot applications can be loaded. In case an unsigned application is downloaded following error pops up.



Automation Builder 2.6 - Standard

The device aborted the download because of security issues.

The device requires downloaded data to be signed but the signature is missing.
Please check the security settings of the application.

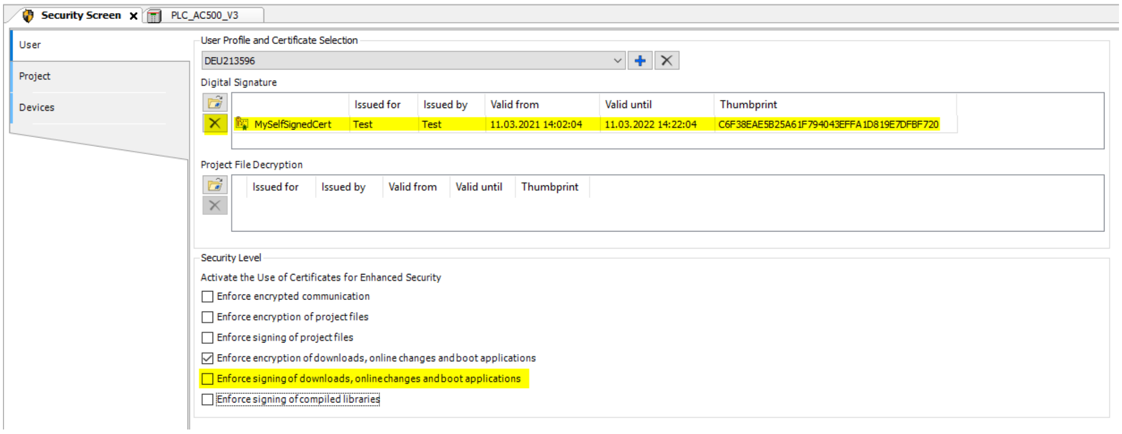
⚠	CAUTION! **A not signed boot application can be downloaded to the PLC which is replacing the existing boot application. When trying to load this not signed boot application the error occurs. Nevertheless, the old boot application is already replaced so not boot application is available anymore.**

6 Delete certificates and user management

Certificates can be deleted in the “Security Screen” view, either directly on the “User” tab or in the “Certificate Selection” dialog.

6.1 Delete certificate for signing the application

- Dialog “Security Screen”, tab “User”, “Digital signature”.
  Select a certificate and click ☒



User Profile and Certificate Selection

DEU213596

Digital Signature

	Issued for	Issued by	Valid from	Valid until	Thumbprint
MySelfSignedCert	Test	Test	11.03.2021 14:02:04	11.03.2022 14:22:04	C6F38EAE5B25A61F794043EFFA1D819E7DFBF720

Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

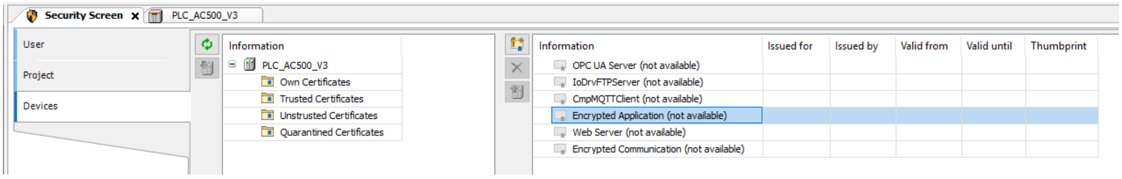
Activate the Use of Certificates for Enhanced Security

☐ Enforce encrypted communication
☐ Enforce encryption of project files
☐ Enforce signing of project files
☑ Enforce encryption of downloads, online changes and boot applications
☐ Enforce signing of downloads, online changes and boot applications
☐ Enforce signing of compiled libraries

Remove the checkboxes in the “Security Level”.

6.2 Deleting a certificate for the encryption of boot application, download and, online change

1. In the “Security Screen” view, on the “User” tab, remove the checkbox for “Enforce encryption of downloads, online changes, and boot applications“
2. In the “Security Screen” view, on the “Project” tab, in the bottom view, double click the entry for the “Application”.
3. The “Properties dialog for the application opens with the “Encryption” tab.
4. In the “Certificates” group, click 📂.
   In the “Certificate Selection” dialog, delete the certificate by selecting the certificate and click ☒
5. Click “OK” to close the “Certificate Selection” dialog.
6. The certificate is no longer displayed in the “Properties” dialog.
7. Remove the checkbox in the “Certificates” section for “Digitally sign application code”
8. Set the “Encryption technology” to “No encryption”
9. Click “Apply” and “OK”
10. In the “Security Screen” view, on the “Device” tab, select the PLC and remove the certificate for “Encrypted Application”



Information
- PLC_AC500_V3
  - Own Certificates
  - Trusted Certificates
  - Unstrusted Certificates
  - Quarantined Certificates

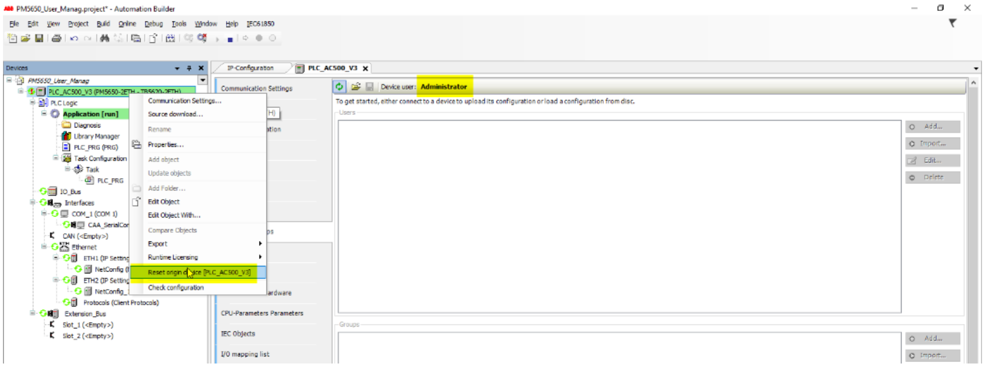
Information	Issued for	Issued by	Valid from	Valid until	Thumbprint
OPC UA Server (not available)					
IoDrvFTPServer (not available)					
CmpMQTTClient (not available)					
Encrypted Application (not available)					
Web Server (not available)					
Encrypted Communication (not available)					

6.3 Deleting a certificate for the encrypted communication

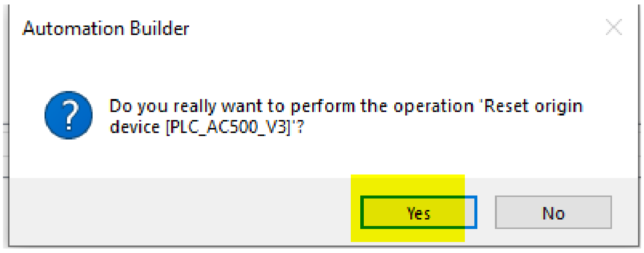
1. In the “Security Screen” view, on the “User” tab, remove the checkbox for “Enforce encrypted communication“
2. In the “Security Screen” view, on the “Device” tab, select the PLC and remove the certificate for “Encrypted Communication”

6.4 Delete the user management

1. Login as Administrator
2. Right click to the PLC_AC500 in the device tree
3. Select reset origin Device

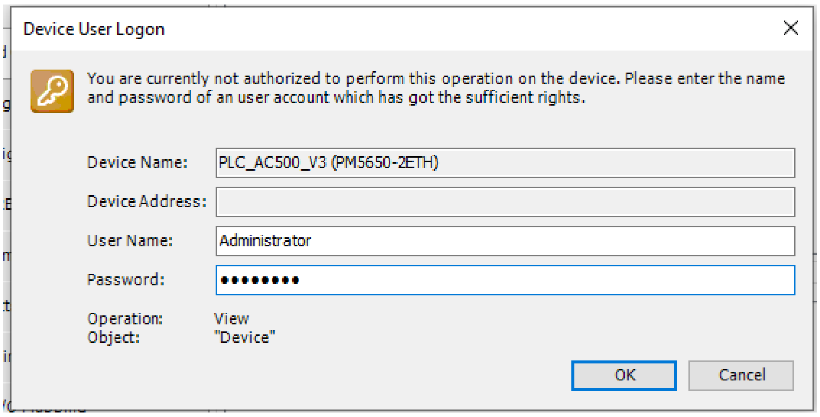


4. Confirm with yes


Automation Builder

Do you really want to perform the operation 'Reset origin device [PLC_AC500_V3]'?

5. Wait about 30s, you’ll be logged out
6. Login Again, you’ll be asked for Username and Password


Device User Logon

You are currently not authorized to perform this operation on the device. Please enter the name and password of an user account which has got the sufficient rights.

Device Name: PLC_AC500_V3 (PM5650-2ETH)

Device Address:

User Name: Administrator

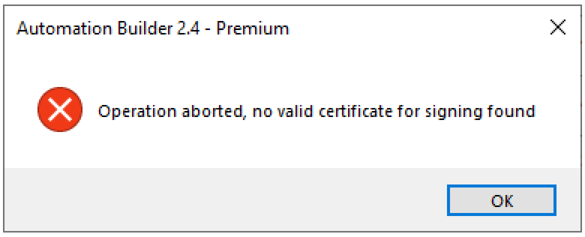
Password: ••••••••

Operation: View
Object: "Device"

7. Type in and confirm. The error message “Too many Tries” is shown
8. Now the user management is deleted and no more password is needed

7 FAQs

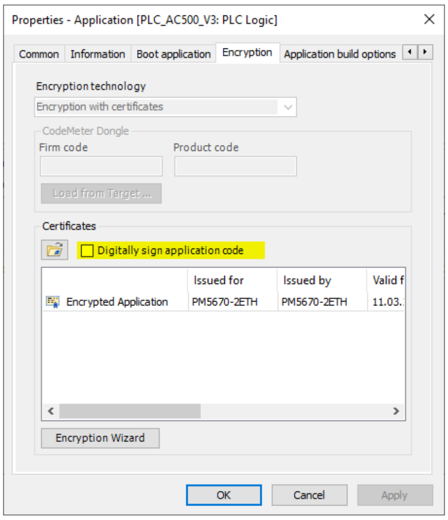
Q1: What’s wrong when I got the Error: Operation aborted, no valid certificate for signing found



Automation Builder 2.4 - Premium

Operation aborted, no valid certificate for signing found

A1: If you do not want to use Code Signing, it could happen, that you have selected the “Digitally sign application code” is selected



Properties - Application [PLC_AC500_V3: PLC Logic]

Encryption technology: Encryption with certificates

CodeMeter Dongle

Firm code:

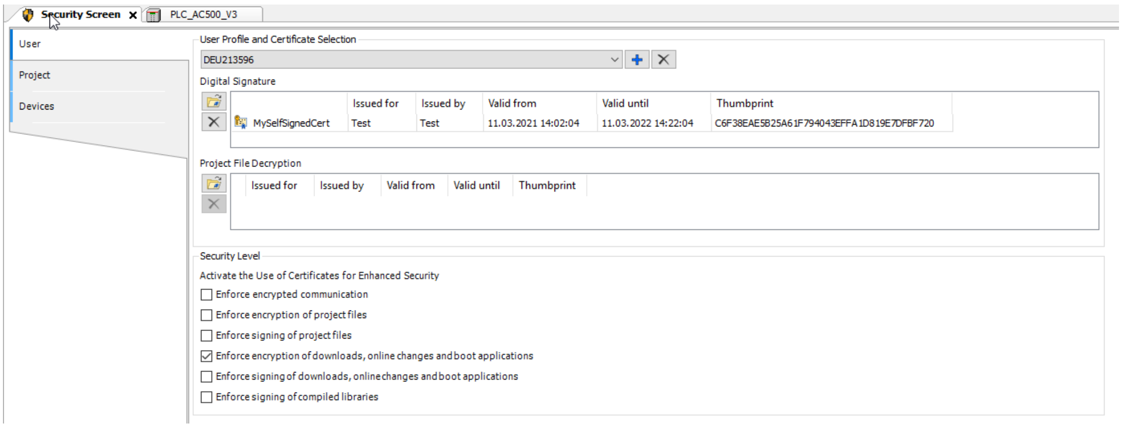
Product code:

Certificates

□ Digitally sign application code

	Issued for	Issued by	Valid f
Encrypted Application	PM5670-2ETH	PM5670-2ETH	11.03.

If you want to use Code Signing than, please be sure you have imported your certificate.



User Profile and Certificate Selection: DEU213596

Digital Signature

	Issued for	Issued by	Valid from	Valid until	Thumbprint
MySelfSignedCert	Test	Test	11.03.2021 14:02:04	11.03.2022 14:22:04	C6F38EAE5B25A61F794043EFFA1D819E7DFBF720

Project File Decryption

Issued for	Issued by	Valid from	Valid until	Thumbprint

Security Level

Activate the Use of Certificates for Enhanced Security

- □ Enforce encrypted communication
- □ Enforce encryption of project files
- □ Enforce signing of project files
- ☑ Enforce encryption of downloads, online changes and boot applications
- □ Enforce signing of downloads, online changes and boot applications
- □ Enforce signing of compiled libraries

—

ABB Automation Products GmbH
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444
Fax: +49 62 21 701 1382
E-Mail: plc.support@de.abb.com
www.abb.com/plc

—

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.