Table of contents

- Encrypting the application

Encrypting the application

Encrypting the application

Know-how protection and copy protection of a boot application can be achieved by means of a control-specific license management and a corresponding setting in the object properties of the application. In this case, the download code and the boot application are encrypted.

Encrypting with certificate

Prerequisites: A project with a application that is to be loaded to the control as encrypted boot application. In the Windows Certificate Store of your computer, there is a certificate for encrypting the application. Note: If you want to load the application on different controls, you need the appropriate certificate for each control.

1. Select the application in the device tree.
2. Select the *"Properties"* command from the context menu.
   ⇒ The *"Properties - <Application name>"* dialog is displayed
3. Select the Security tab
4. For the Encryption technique, select Encryption with certificates.
   ⇒ The *"Certificates"* dialog box becomes active.
5. If no certificate is entered in the table yet, click on the button.
   ⇒ The Certificate selection dialog opens to select a certificate from the local Windows Certificate Store.
6. Select a certificate in the lower area and drag it into the upper field using the button. Confirm with OK.
   ⇒ The certificate is displayed in the Encryption dialog in the Certificates field.

If you want to sign the boot application as well, proceed as follows:

Enable the Digitally sign application code option in the Properties dialog and follow steps 1-13 of the "Sign boot application with certificate only, do not encrypt" guide below.

For further information, see:

↘ Security for the Runtime System / PLC

↘ Encrypting the project with a certificate

Encrypting with the dongle

Prerequisites: A project with a application that is to be loaded to the control as encrypted boot application. A dongle for license management is plugged into your computer.

1. Select the application in the device tree.
2. Select the *"Properties"* command from the context menu.
   ⇒ The *"Properties - <Application name>"* dialog is displayed.
3. Select the *"Encryption"* tab.
4. For *"Encryption technique"*, select *"Simple encryption"* and enter the *"product code"* you received from the hardware manufacturer for the control. Depending on the control, this is protected by means of a dongle (the firm code is displayed automatically) or, for example, via a permanently installed Wibu SD card.
5. Select the command *Online ➔ Login* and perform a download of the application.
   ⇒ If the matching dongle and/or the valid license is available, the application can be loaded to the control. By default, a boot application is automatically created in the control directory. This default setting is defined in the *"properties"* of the application in the *"boot application"* category.
6. Log out again, change the application and log in again.
   ⇒ A prompt is displayed asking the user if an online change is to be performed. In the query dialog you also have the option to update the boot application on the control. If the dongle and license match, you can log in, otherwise you will receive a corresponding message.

Sign boot application with certificate only, do not encrypt it

1. Open the *"Security screen"* view via the button in the status bar of PLC Engineering and select a private key certificate for a *"digital signature "* user profile. The procedure is described in the instructions "Configuring a certificate for the digital signature in a user profile".
2. In the *"Users"* tab, double-click on the *"Digital signature"* certificate.
   ⇒ The *"Certificate"* dialog is displayed.
3. On the *"Details"* tab, select the *"Copy to file"* button.
   ⇒ The *"Certificate export wizard"* starts.
4. In the *"Export private key"* prompt, select the *"No, do not export private key"* option.

5. For *“Format of the file to be exported”*, select the *“DER-encoded-binary X.509 (.CER)”* format.
6. In the next step, select a file name and location for the certificate.
7. After the last step *“Complete”*, a message is displayed whether the export process was completed successfully.
8. After the successful export in PLC Engineering, open the device editor by double-clicking on the control in the device tree and select the *“Files”* tab for file transfer.
9. In the right part of the dialog *“Runtime ”*, select the *“path”* cert/import.
10. In the left part of the dialog *“Host”*, select the path in the file system where you stored the exported certificate and select the certificate.
11. Click on >>.
    ⇒ The certificate is copied to the cert/import folder.
12. Select the *“PLC Shell”* tab.
13. In the input line of the tab, type the command cert-import trusted <filename.cer> and press the *[Enter key]* . Make sure that the file name is specified with the .cer file extension, otherwise the certificate is not imported successfully.
    ⇒ The certificate is created on the control under trusted. This certificate allows the control to verify the integrity of the boot application.
14. Open the *“security screen”* by double-clicking on in the status bar.
15. If you want to always encrypt downloads, online changes and boot applications of your project, enable the option *“Force signing of downloads, online changes and boot applications”* in the *“User”* tab in the *“Security level”* area. The option *“Force encryption of downloads, online changes and boot applications”* also has to be enabled.

Also refer to

- ↘ “Encrypting the project with a certificate”
- ↘ “Encryption, Signature”
- ↘ “Command 'Security Screen'”
- ↘ “Dialog 'Properties' - 'Encryption'”

Encrypting the download, the online change and the boot application

Prerequisite: The add-on product CODESYS Security Agent is installed.

The *“Security Screen”* view provides an additional tab: *“Devices”*. It allows the configuration of certificates for encrypted communication with controls. In this case, refer to the CODESYS Security Agent help.

Option:

If CODESYS Security Agent is not available, you can proceed as follows via the PLC shell of the device editor:

To use certificates from the control for download, online change, and boot application encryption, these certificates first have to be generated on the control, loaded from the control, and installed in the Windows Certificate Store.

Prerequisite: You are connected to the control

1. Double-click on the control in the device tree to open the device editor and select the *"PLC shell"* tab.
   ⇒ The tab is displayed with an empty display window. Below you will find an input line for a command
2. Type a ? in the input line and press *[Enter]* .
   ⇒ All commands are listed in the display window.
3. Enter the following command in the input line: cert-getapplist
   ⇒ All used certificates are listed with information about components and availability with certificates.
4. If there is no certificate for the CmpApp component, enter the cert-genselfsigned <Number of the Component in the applist> command.
5. Select the *"Log"* tab and click the refresh button .
   ⇒ It displays whether the certificate was successfully generated.
6. Enter cert-getcertlist and press *[Enter]* .
   ⇒ The individual certificates that can be used for encryption are listed. For the next step, the information Number: and Key usage(s) are important.

   Number: Enter the number specified as a parameter in the next step

   Key usage(s): Data Encipherment means that it is a certificate of control for download, online change and boot application.
7. Export the desired certificate with the command cert-export own 0 and press *[Enter]* . 0 is the Number of the certificate with Key usage(s):Data encryption.
   ⇒ The display shows that the certificate has been exported to a cert folder.
8. Select the *"Files"* tab of the device editor.
9. In the right dialog section *"Runtime"*, click on the refresh button .
   ⇒ The list of the files and directories are updated.
10. In the list, open the *"cert"* folder and subsequently the *"export"* subfolder.

11. In the left half of the *"Host"* dialog, open the directory where the certificate is to be loaded from the control.
12. In the right half of the dialog, select the certificate you have exported and click on <<.
    ⇒ The certificate is copied to the selected folder.
13. Use your file Explorer, go to the folder where the certificate was copied to and double-click on the certificate.
    ⇒ The *"Certificate"* dialog is displayed and provides information about this certificate.
14. In the *"General"* tab, click on the *"Install certificate"* button.
    ⇒ The *"Certificate import wizard"* starts.
15. In the *"Certificate import wizard"*, in the *"Certificate store "* dialog, select *"Save all certificates to the following store "* and select the *"Control certificates"* folder.
    ⇒ The control certificate is imported into the *"controller certificates"* folder in the Windows Certificate Store and is now available to encrypt the download, online change, and boot application.
16. Open the *"Security screen"* by double-clicking on the in the status bar.
17. If you want to always encrypt the downloads, online changes, and boot applications, enable the *"Enforce encryption of downloads, online changes, and boot applications"* option in the *"Security level"* section of the *"Users"* tab.
18. Open the *"Project"* tab and double-click on the application in the *"Encryption of boot application, download and online change"* section.
    ⇒ The properties dialog of the application is displayed.
19. Select the *"Encryption"* tab and select from the drop-down list *"with Encryption technique""Encryption with certificates"* and click on .

    If the *"Force encryption of downloads, online changes, and boot applications"* option is enabled in the *"Security screen"*, *"encryption with certificates"* is already selected.
20. In the *"Certificate selection"* dialog, select the certificate from the *"Controller certificates"* folder and click on .
21. Confirm the dialog with *"OK"*
    ⇒ The certificate is displayed in the properties dialog.
22. Confirm the properties dialog of the application.
    ⇒ The certificate is displayed in the *"Secruity screen"* in the *"Project"* tab in the *"Encryption of boot application, download and online change"* area.

    Boot application, download and online change are encrypted.

Also refer to

- Help for the additional product CODESYS Security Agent
- ↘ ““PLC shell” tab”
- ↘ “Command 'Security Screen'”

Delete the certificate for encrypting the boot application, the download and online change

Prerequisite: The add-on product CODESYS Security Agent is installed. A certificate with the information "Encrypted application" is already installed on your computer.

1. In the *“Security screen”* view, *“Project”* tab, double-click on the entry for the application in the lower part of the window.
   ⇒ The *“Properties”* dialog, *“Encryption”* tab for the application is opened.
2. Select *“encryption technique”* *“encryption with certificates”*. In the *“Certificates”* box, click on  .
3. In the *“Certificate selection”* dialog, delete the certificate as described above.
4. Exit the *“Certificate selection”* dialog with *“OK”*.
   ⇒ The certificate is no longer displayed in the *“Properties ”* dialog.

Also refer to

- Help for the additional product CODESYS Security Agent
- ↘ “Command 'Security Screen'”