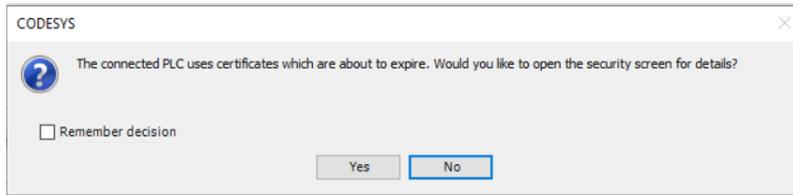# Expired certificates message for encrypted communication

Problem and error description

The following error message is displayed in the Codesys IDE:

Under the 'Security Screen', existing certificates are displayed which will expire in the near future:

This warning of an expiring certificate is intended to alert the user in a timely manner so that the user still has enough time to react.

Solution

The following solutions are available if you want to resolve this message and the reason behind it:

1. create a certificate with longer duration (e.g. 365 days) with the security agent. Then the message comes at least more rarely.
2. if it is ensured that no encrypted online communication is used (of course not recommended from a security point of view), the communication policy can be set to "no encryption".
   This means that the Runtime no longer allows encrypted online communication and does not have to maintain a valid certificate.
   Accordingly, the LZS no longer generates the corresponding certificate.

After setting the communication policy to "no encryption", any existing certificates may have to be deleted so that they can no longer expire.

In the event of a transitional period

For the assurance of a further possible communication, the Runtime automatically generates a new self-signed certificate as soon as the certificate has expired.
Otherwise, one would indeed lock oneself out if only encrypted communication is allowed.

When logging in, a message appears that the controller uses an unknown certificate and the question whether the user wants to trust it.

> ⓘ   All other certificates are not renewed automatically and must be created and renewed according to the user's specifications.

Configurations settings

! Not recommended from a security point of view !

If the following setting is written into the CODESYSControl.cfg before the first start, then the Runtime does not even initially generate a certificate for the encrypted communication and the user does not have to delete any:

[CmpSecureChannel]
SECURITY.CommunicationMode=ONLY_PLAIN

ⓘ Setting the communication policy to "no encryption" uses the same setting:

Change Communication Policy

Communication
Current policy   No encryption
New policy   No encryption
                        The device does not support encrypted communication.