

## LYNX- Certificate Error

The standard certificate supplied with LYNX has expired.

Follow the steps below to create a new valid certificate:

Explanation:

The LYNX server only allows encrypted connections (https). A certificate is required for this.

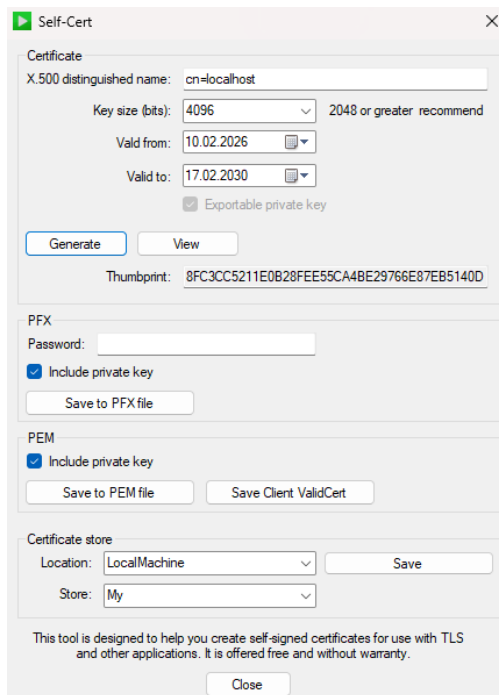
- A certificate in PEM format with a private key is required.
- Hardware keystores, e.g., USB tokens, are not supported.
- Certificates are digital attestations that confirm the security and authenticity of a server.
- They are issued by certificate authorities (CAs) and enable data transmission to be encrypted using SSL/TLS.
- There are external (public) certification bodies and, in many companies, internal (private) certification bodies as well.
- To set up a certificate, you must create a CSR (Certificate Signing Request) and submit it to a CA in order to obtain your certificate and install it on the driver.
- To create a suitable certificate, please contact your IT department.

# Creation of a self-signed certificate for testing purposes and simple applications

## LYNX – Server:

### Attention:

- Self-signed certificates do not allow the browser to fully verify the certificate. They are particularly vulnerable to man-in-the-middle attacks.
- Generate an error message in the browser that must be ignored.



1. To create a self-signed certificate, locate the program “SelfCert.exe” in the LYNX server directory, subdirectory “Tls” -> ‘bin’ -> “SelfCert”.

### Note:

The program should be run as an administrator.

2. After startup, only a few details are required:  
“X.500 distinguished name”: the computer name of the computer running the driver must be entered here.  
**cn=computer name**, e.g., cn=localhost or cn=lynx.server  
Keysize: a key length of > 2048 bits is recommended.  
Validity from – to. (from current date – to select a period)

### Note:

Please note the validity period of your certificate. You must repeat these instructions for creating the certificate before it expires.

3. The “**Generate**” button creates the certificate, which can then be saved to a file in the “**PEM**” section.
4. Make a note of the thumbprint you have created, for example in an editor, or simply leave the “**SelfCert.exe program**” open.

5. Save the certificate under:  
Lynx installation path → LynxServer → Tls → config → LynxTlsServer.pem  
The old certificate contained therein can be deleted or overwritten.
6. Please enter the newly created thumbprint into the ValidCertThumbprint.txt file.  
LYNX installation path → LynxServer → ValidCertThumbprint.txt
7. Either restart the service using the LynxStartupConfigTool or restart the service via Services "LynxServerService".

**LYNX-Client:**

Please enter the newly created thumbprint into the ValidCertThumbprint.txt file or copy the file from the server.

**Driver:**

Please enter the newly created thumbprint into the „ValidCertThumbprint.txt“ file or copy the file from the server.

**Each driver in the directory must be customized! It is best to copy the file to the driver directories.**