

LYNX- Zertifikatsfehler

Das mit ausgelieferte Standard Zertifikat von LYNX ist abgelaufen.

Folgen Sie den unteren Schritten um ein neues gültiges Zertifikat zu erstellen.

Erklärung:

Der LYNX Server lässt nur verschlüsselte Verbindungen (https) zu. Hierfür wird ein Zertifikat benötigt.

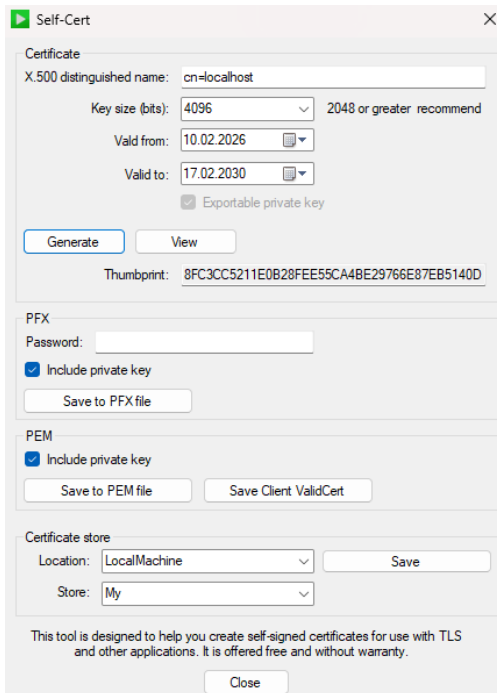
- Es wird ein Zertifikat im PEM-Format mit privatem Schlüssel benötigt.
- Hardware-Keystores, z.B: USB-Tokens werden nicht unterstützt.
- Zertifikate sind digitale Bescheinigungen, die die Sicherheit und Authentizität eines Servers bestätigen.
- Sie werden von Zertifizierungsstellen (Certificate Authorities, CAs) ausgestellt und ermöglichen die Verschlüsselung der Datenübertragung mittels SSL/TLS.
- Es gibt externe (public) und in vielen Unternehmen auch interne (private) Zertifizierungsstellen.
- Zur Einrichtung eines Zertifikats müssen Sie einen CSR (Certificate Signing Request) erstellen und diesen bei einer CA einreichen, um Ihr Zertifikat zu erhalten und auf dem Treiber zu installieren.
- Für die Erstellung eines passenden Zertifikats wenden Sie sich bitte an Ihre IT-Abteilung.

Erstellung eines Self-Signed Zertifikats für Testzwecke und einfache Anwendungen

LYNX – Server:

Achtung:

- Self-Signed Zertifikate bieten dem Browser nicht die Möglichkeit das Zertifikat vollständig zu prüfen. Sie sind besonders anfällig für „Man in middle“ - Angriffe.
- Erzeugen im Browser eine Fehlermeldung die übergangen werden muss.



1. Zum Erstellen eines Self-Signed Zertifikates befindet sich im LYNX Server-Verzeichnis, Unterverzeichnis „Tls“ -> „bin“ -> „SelfCert“, das Programm „SelfCert.exe“.

Hinweis:

Das Programm sollte als Administrator ausgeführt werden.

2. Nach dem Start werden nur sehr wenige Angaben benötigt:
„X.500 distinguished name“: hier muss der Rechnername des Rechners der den Treiber ausführt eingetragen werden
cn=**Rechnername**, z.B. cn=localhost oder cn=lynx.server
Keysize: es wird eine Schlüssellänge von > 2048 Bit empfohlen.
Gültigkeit von – bis. (von aktuelles Datum – bis wählen Sie einen Zeitraum)

Hinweis:

Bitte merken Sie sich die Gültigkeit Ihres Zertifikates. Sie müssen diese Anleitung zur Erstellung des Zertifikates vor Ablauf wiederholen.

3. Über die Taste „**Generate**“ wird das Zertifikat erstellt und kann danach im Bereich „**PEM**“ in eine Datei gespeichert werden.

4. Merken Sie sich den erstellen „Thumbprint“ zum Beispiel in einem Editor oder lassen Sie das „**SelfCert.exe Programm**“ einfach so lange geöffnet
5. Speichern Sie das Zertifikat unter:
Lynx Installationspfad → LynxServer → Tls → config → LynxTlsServer.pem
Das darin enthaltene alte Zertifikat kann gelöscht oder überschrieben werden.
6. Tragen Sie den frisch erstellten „Thumbprint“ bitte in die „ValidCertThumprint.txt“ Datei ein.
LYNX Installationspfad → LynxServer → ValidCertThumprint.txt.
7. Entweder über das LynxStartupConfigTool den Dienst neu starten oder über Dienste „LynxServerService“ den Dienst neu starten.

LYNX – Client:

Tragen Sie den frisch erstellten „Thumbprint“ bitte in die „ValidCertThumprint.txt“ Datei ein oder kopieren Sie die Datei vom Server.

Treiber:

Bitte tragen Sie den frisch erstellten „Thumbprint“ bitte in die „ValidCertThumprint.txt“ Datei ein oder kopieren Sie die Datei vom Server.

Jeder Treiber im Verzeichnis muss angepasst werden! Am besten kopieren Sie die Datei in die Treiberverzeichnisse.