Zertifikat für TLS Zugriff hochladen

Diese Dokumentation beschreibt wie ein Zertifikat auf der STARFACE installiert werden kann, dass für den LDAP Zugriff mit TLS Verschlüsslung auf ein Adressbuch oder ein Active Directory benötigt wird (siehe auch Adressbuch der STARFACE nutzen und Active Directory auf der STARFACE konfigurieren) . Diese Dokumentation gilt nur für die Version 6.7.3.11 der STARFACE und ab der Version 7.0.0.X der STARFACE kann der Upload des Zertifikats via Standardmodul durchgeführt werden (siehe Modul "CA Certificate for LDAPS" konfigurieren).

> ⚠ **Hinweis:** Es ist auf Cloud Anlagen nicht möglich eigene Root-Zertifikate hochzuladen.

Die Zertifikatsdateien müssen via SFTP in das Verzeichnis "/root" übertragen werden. Für den Zugriff via SFTP kann der root Benutzer der STARFACE verwendet werden (siehe auch Passwort für den root-User).

Es muss das Root-CA-Zertifikat eingespielt werden und das Zertifikat des AD/LDAP-Servers das nicht von einer gängigen Zertifizierungsstelle (CA) ausgestellt wurde (Option in der Checkbox = TLS ohne Zertifikatsprüfung). Auch bei der Option "TLS ohne Zertifikatsprüfung" wird das Ablaufdatum des verwendeten Zertifikats geprüft. Das bedeutet wenn ein selbst erstelltes Zertifikat genutzt wird und das Ablaufdatum überschritten ist, kann keine Verbindung aufgebaut werden.

Im letzten Schritt muss eine Verbindung via ssh zur STARFACE aufgebaut werden und das folgende Kommando ausgeführt werden:

keytool -importcert -alias **Aliasname** -keystore /usr/lib/jvm/java-1.8.0-oracle-1.8.0.202.x86_64/jre/lib/security/cacerts -storepass changeit -file **Name der Zertifikatsdatei** -storetype JKS

> ⚠ **Hinweis:** Die im oben aufgeführten Kommando fett dargestellten Textstellen müssen vollständig durch die korrekten Bezeichnungen ersetzt werden.

Die bereits bestehenden trusted CAs können über das folgenden Kommando ausgegeben werden:

keytool -list -keystore /usr/lib/jvm/java-1.8.0-oracle-1.8.0.202.x86_64/jre/lib/security/cacerts