Anpassen der OpenLDAP CA

03.07.2024 15:39:01

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Verzeichnisdienste	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	12:32:34 - 13.04.2023

Schlüsselwörter

OpenLDAP Zertifikat

Lösung (öffentlich)

Die Kommunikation zum zentralen OpenLDAP Dienst (ldap-lzr.zih.tu-dresden.de) erfolgt ausschließlich in verschlüsselter Form über Port TCP 389 (via StartTLS) oder Port 636 (LDAPS). Während des Aufbaus der verschlüsselten Verbindung wird das Serverzertifikat auf Gültigkeit geprüft. Im Normalfall finden Prüfungen auf den Namen und das Ablaufdatum des Serverzertifkats sowie die Herkunft statt. Die Herkunft wird meist gegen eine Liste vertrauenswürdiger Stammzertifikatsaussteller geprüft.

Das bisherige OpenLDAP Serverzertifikat wurde von der DFN PKI [1] ausgestellt, das neue Zertifikat kommt von Sectigo [2] und hat somit ein anderes Stammzertifkat. Für LDAP-Clients ergeben sich somit zwei Szenarien bei der Umstellung des Zertifikats des OpenLDAP Dienstes:
1) Der Client ist so konfiguriert, dass die im System installierte Liste vertrauenswürdiger Stammzertifikatsaussteller zur Prüfung des LDAP-Server-Zertifikats verwendet wird.
2) Für den Client ist explizit die Zertifikatskette hinterlegt.

Für Szenario 1) muss im Normalfall nichts auf Client-Seite getan werden, da die Root-Zertifikate von Sectigo bereits im System hinterlegt sind. Eine Prüfung der Root Zertifikate wird unter [5] beschrieben.

Für Szenario 2) muss der LDAP-Client angepasst werden.
2a) Am einfachsten ist es, die Prüfung so umzustellen, dass Szenario 1) Anwendung findet. Dann sollte am Tag der Umstellung ein problemloser Weiterbetrieb des LDAP-Clients gewährleistet sein.
2b) Falls dies nicht möglich ist, muss die neue Zertifikatskette ([3]+[4], fertig im PEM-Format im Anhang dieses Artikels) im Client hinterlegt werden. Ob dies zusätzlich zur aktuellen Kette möglich ist oder erst nach Umstellung erfolgen kann, hängt von der jeweiligen Anwendung ab. Dies muss durch den/die jeweiligen Administator:in geprüft werden.

Für Anwendungen basierend auf Linux/Unix LDAP-Abfragen gibt es u.a. folgende Möglichkeiten zur Prüfung von Stammzertifikaten:

- Verwendung des Zertifikatsspeichers des Systems = Szenario 1)
- /etc/ssl/certs/
- dieser wird verwendet, wenn keine Vorgaben gesetzt sind
- die Sectigo Root Zertifikate sollten enthalten sein

- Java Keystore
- /path/to/my/store.keystore
- Liegt meist in dem Verzeichnis, wo auch Java installiert ist

- Skriptsprachen oder Betriebssystem Linux
- /etc/ldap/ldap.conf oder /etc/openldap/ldap.conf
- hier nach TLS_REQCERT oder TLS_CACERT schauen

- Skriptsprache (selbst)
- Im Aufruf der LDAP Verbindung schauen, was hier explizit gesetzt wurde

[1] [1]https://pki.pca.dfn.de/tu-dresden-g2-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=0
[2] [2]https://sectigo.com/resource-library/sectigo-root-intermediate-certificate-files
[3] [3]http://crt.comodoca.com/USERTrustRSACertificationAuthority.crt
[4] [4]http://crt.sectigo.com/SectigoRSAOrganizationValidationSecureServerCA.crt
[5] [5]https://faq.tickets.tu-dresden.de/otrs/public.pl?ItemID=825

[1] https://pki.pca.dfn.de/tu-dresden-g2-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA_ID=0
[2] https://sectigo.com/resource-library/sectigo-root-intermediate-certificate-files
[3] http://crt.comodoca.com/USERTrustRSACertificationAuthority.crt
[4] http://crt.sectigo.com/SectigoRSAOrganizationValidationSecureServerCA.crt
[5] https://faq.tickets.tu-dresden.de/otrs/public.pl?ItemID=825