MICROSOFT LDAP SIGNING / CHANNELBINDING

Überblick

Microsoft wird ab März einen Security Patch ausliefern:

https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows

Saperion ist grundsätzlich in der Lage mit der Änderung umzugehen. In allen Versionen 8.X und Saperion ECM Foundation ist dieser bereits enthalten. In der Version 7.5.6 ist ein Hotfix auf Basis von Patchlevel 19 verfügbar.

Um die Software mit diesem Microsoft Patch einsetzbar zu machen ist eine kleine Konfigurationsanpassung nötig.

Technischer Hintergrund:

Microsoft aktiviert mit dem März Update zwei Sicherheitsfeatures per Default, welche vorher Optional vorhanden waren. Danach ist es nicht mehr möglich, unverschlüsselt mit dem Active Directory Controller zu kommunizieren.

In Saperion sind zwei LDAP SDKs implementiert OpenLDAP und Microsoft. Derzeit wird als Standard „OpenLDAP“ verwendet.

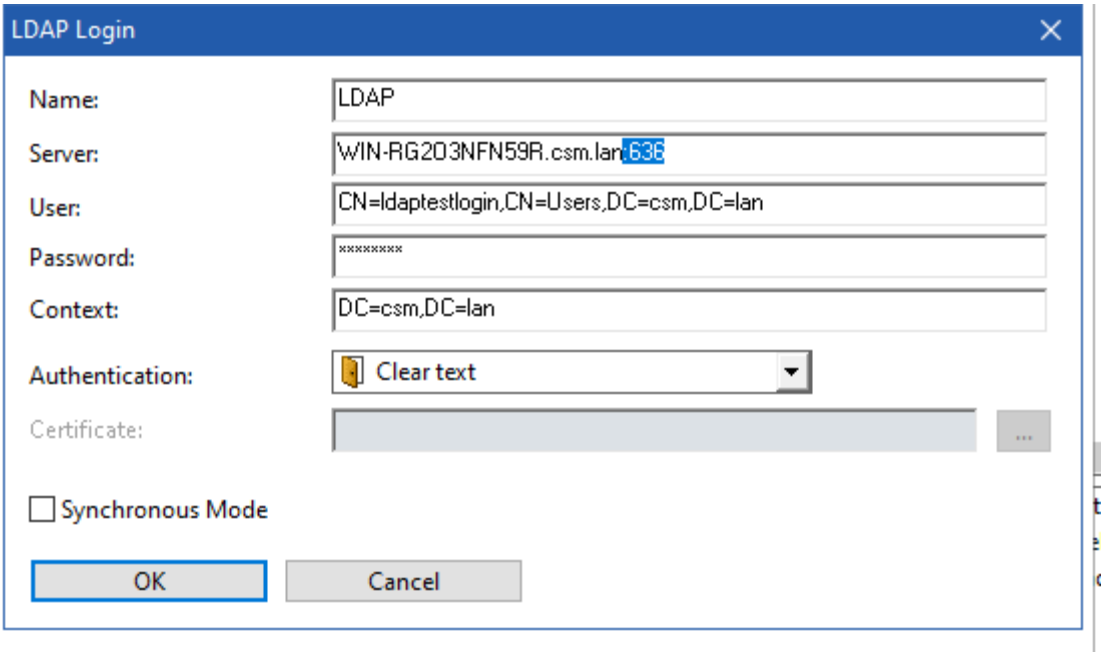
Um das Microsoft SDK zu aktivieren muss der folgende INI Schalter gesetzt werden

Program.ini Server

[LDAP Sync]

StandardSDK=Microsoft

In der LDAP Server Konfiguration im Client muss jetzt nur noch der **Port 636** hinzugefügt werden.



Authentication bleibt auf „Clear text“.

Danach muss der Server neu gestartet werden, da er sonst die geänderten LDAP Server und das neue SDK nicht kennt. Eine Benutzername / Passwort Authentifizierung würde noch fehl schlagen.

Verifikation

Ob die Änderung aktiv ist und die Saperion Softwareversion nutzbar ist, erkennt man im Coreserver-Log beim Start. Dort taucht folgende Meldung auf. Im Standard sieht die Meldung so aus:

2988 2020-01-30 08:14:54:79 NOTICE LDAP value_free: **Using LDAP-SDK autodetect**

Ob die Änderung aktiv ist, erkennt man an dieser Meldung beim Start des Servers:

2224 2020-01-29 14:54:06:59 NOTICE LDAP value_free: **Using Microsoft LDAP-SDK**

Weitere Anmerkungen:

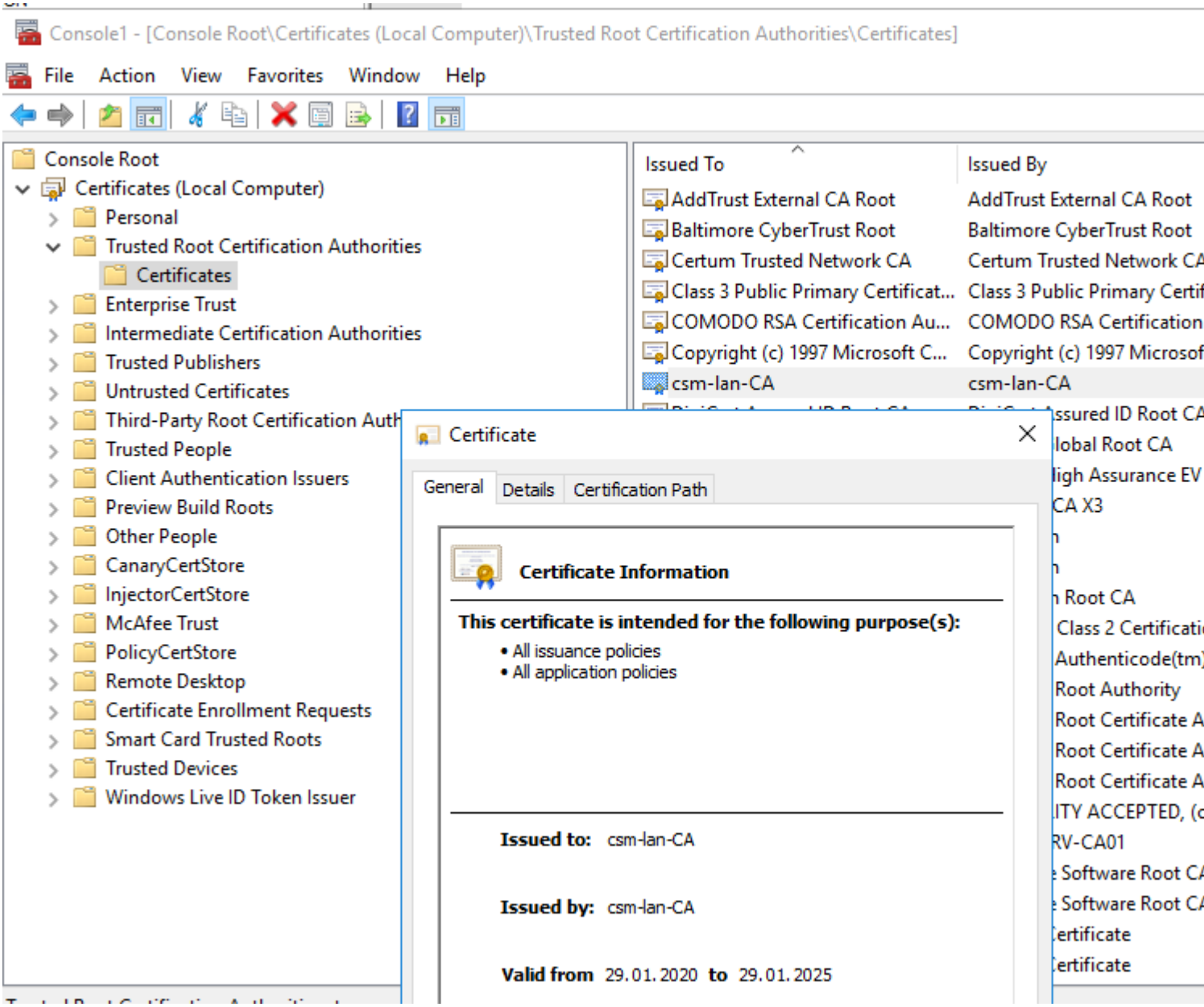
Das Microsoft SDK führt nun alle Operationen über das Betriebssystem durch, so dass das Signing und Channelbinding transparent durchgeführt wird. Auch die Validierung des Serverzertifikates. Da die Zertifikate auf Computernamen ausgestellt werden, kann der Kunde **keine IP** mehr verwenden z.B. „10.184.244.211:636“. Dies funktioniert nicht.

Er könnte auch nur „csm.lan:636“ (Domäne:Port) eintragen. Hierdurch wird der zuständig AD Controller per DNS Service Discovery ermittelt (MS Mechanismen).

RichClient SSO (Currentuser) funktioniert auch ohne diese Änderung, da der Server kein Passwort überprüfen muss. Der Benutzer wird auf dem Client ermittelt und für die Anmeldung an den Server übermittelt.

Sonderfall:

Wenn beim Kunden z.B. der Sonderfall vorliegt und der Saperion Server bzw. Client (bei der Konfiguration des LDAP Servers) in einer anderen Domäne ist, als das zu verwendete Active Directory, dann muss man das ROOT-CA Zertifikat als vertrauenswürdiges Zertifikat beim Saperion Server hinzufügen. Andernfalls kann er das Server Zertifikat (LDAPs Zertifikat) nicht validieren und die Verbindung schlägt fehl.



Umstellung LDAP Sync Tool

Das LDAP Sync Tool muss auch auf LDAPS umgestellt werden. Dafür müssen folgende Anpassungen durchgeführt werden.

ROOT-CA Zertifikat zum Java Truststore hinzufügen

Hierzu gibt es zwei Ansätze. Man kann einen eigenen Truststore erstellen oder man fügt das Zertifikat zum ausgelieferten Truststore von Java hinzu.

Hier wird die Variante mit dem eigenen Truststore beschrieben. Zur Administration von Keystores / Trustores wird das Programm „KeyStore Explorer“ verwendet.

- KeyStore Explorer starten und neuen Store erstellen (Ctrl+N)
- Als Typ wird „JKS“ gewählt
- Nun den Menüpunkt „Import Trusted Certificate“ wählen (Ctrl+T)
- das Root Zertifikat importieren
- den Trustsore abspeichern z.B. truststore.jks
- Passwort kann leer gelassen werden, wenn gewünscht

LDAP TOOL Konfiguration

LSC.XML

Passen Sie folgende Einstellungen in der lsc.xml an.

<ldapConnection>
<name>ldap-src-conn</name>
<url>ldaps://WIN-RG2O3NFN59R.csm.lan:636/DC=CSM,DC=LAN</url>
<username>CN=ldaptestlogin,CN=Users,DC=csm,DC=lan</username>
<password>CnPUQ5ijluZrj0IwliCD0Zy58reFfrRqCnPUQ5ijlua7zRyIbZtIIA==</password>
<authentication>SIMPLE</authentication>

…

Verwenden Sie **ldaps** anstatt **ldap** und setzen Sie den **Port „636“.**

Hinweis: Auch hier gilt, dass der Servername und keine IP verwendet werden muss.

ldap-saperion-sync.bat

Fügen Sie folgende Parameter zur ldap-saperion-sync.bat im „**bin**“ Verzeichnis des LDAP Tools hinzu. Vorzugsweise unter dem bereits vorhandenen Eintrag von JAVA_OPTS.

SET JAVA_OPTS=-Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8
SET JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStore=C:/Saperion/truststore.jks
REM SET JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStorePassword=mypass

Hier wird der Pfad zum Truststore hinzugefügt. Verwenden Sie vorzugsweise Slashes als Pfadtrenner, um Probleme vorzubeugen.

Der „trustStorePassword“ Parameter ist mit „REM“ auskommentiert und muss verwendet werden, wenn der Truststore ein Passwort verwendet.