DOCUMENTS

LDAPS-KOPPLUNG (LDAP OVER TLS)

DOCUMENTS 5.0e

Inhaltsverzeichnis

1. Voraussetzungen

DOCUMENTS unterstützt ab der Version 5.0d HF1 (#2065) LDAP OVER SSL.

Vorausgesetzt wird zunächst, dass auf dem AD LDS Server LDAP OVER SLL aktiviert wurde und dass eine LDAP-Connection über TLS/SSL hergestellt werden kann. Dies kann auf dem AD über die Kommandozeile mit dem Programm „ldp“ überprüft werden:

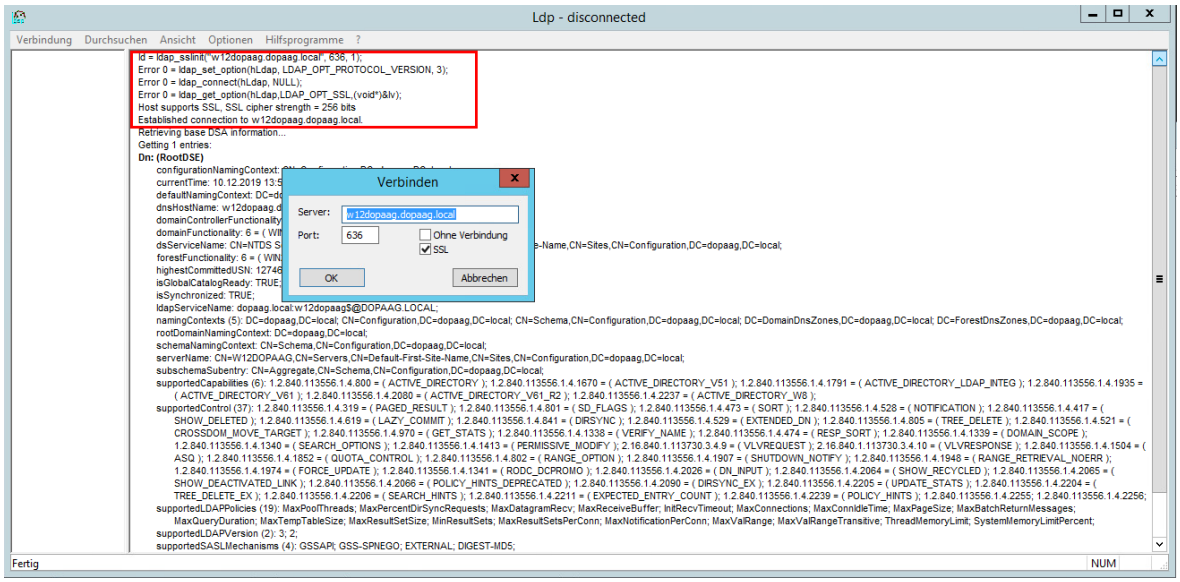

Abb. 1: Über ldp -> Verbinden -> SSL

Ein erfolgreicher SSL-Verbindungsaufbau wird entsprechend protokolliert.

Weiter wird vorausgesetzt, dass man mit dem Einrichten und Konfigurieren des LDAP-Jobs auf dem Standardport 389 (unverschlüsselt) vertraut ist (z.B. über den LDAP Konfigurations-Wizard im DOCUMENTS Manager oder über den Konfigurationsmappentypen).

Im Folgenden werden nur die Punkte aufgeführt bei denen es zu Abweichungen zur LDAP-Standardkonfiguration kommt:

- Erzeugung der notwendigen PEM-Zertifikatsdatei für die TLS/SSL Verbindung zwischen dem DOCUMENTS Server und dem AD LDS

- Testen der Verbindungsparameter und Konfiguration des DOCUMENTS Server zur Verwendung von TLS/SSL

2. Zertifikatskette des AD LDS

Im Folgenden wird ausgehend vom SSL-Zertifikat des AD LDS Servers eine „Zertifikats“-Datei im PEM-Format für den DOCUMENTS-Server erzeugt.

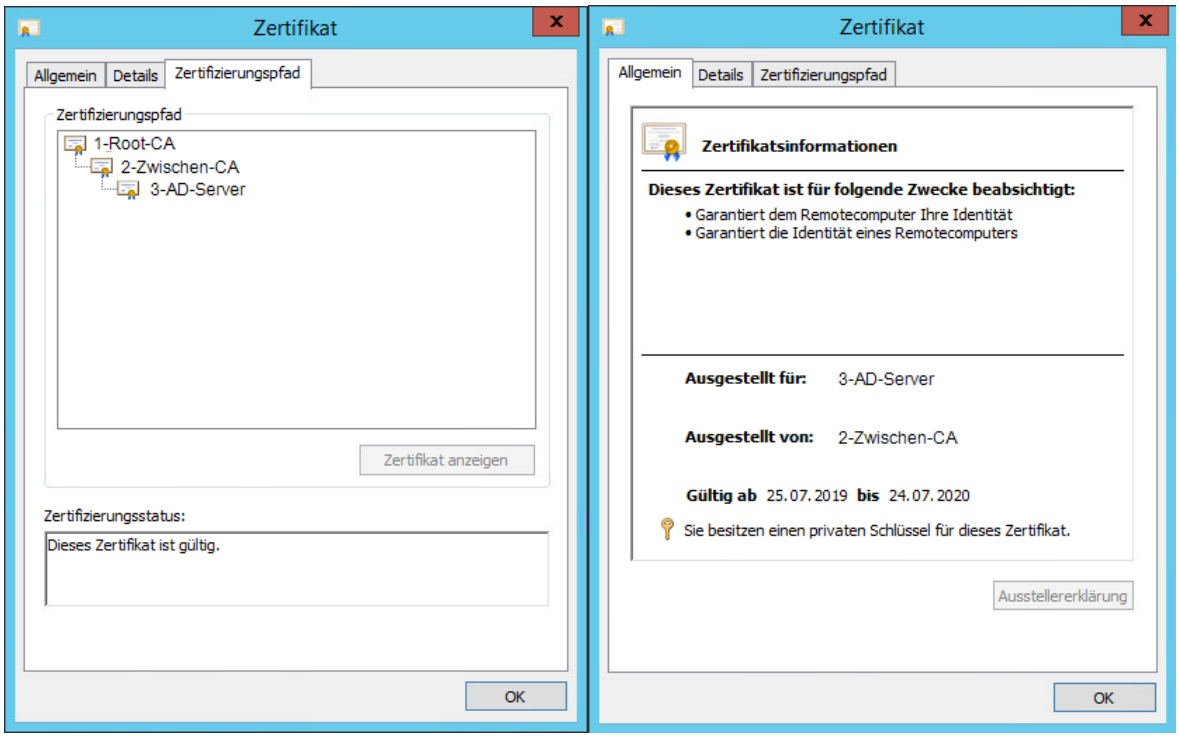

Abb. 2: SSL - Zertifikat des LDAP-Servers

In der Abbildung oben wird das SSL-Zertifikat des AD-Rechners mit dem Namen „3-AD-Server“ gezeigt. Ausgestellt wurde das Zertifikat von der CA „2-Zwischen-CA“, die ihrerseits durch „1-Root-CA“ zertifiziert wurde. Der DOCUMENTS Server benötigt zur Verifikation der Verbindung nur das Root-CA, welches im Folgenden exportiert wird.

Wichtiger Hinweis
Es muss ausschließlich das oberste Zertifikat (1-Root-CA) exportiert werden.

Anhand des Zertifikates wird in wenigen Schritten eine „PEM-Zertifikats“-Datei erstellt, die dann auf dem DOCUMENTS-Server hinterlegt werden muss.

1) Das Zertifikat „3–AD-Server“ am Ende der Zertifikatskette und mögliche Zwischenzertifikate (hier „2-Zwischen-CA“) müssen nicht weiter beachtet werden.

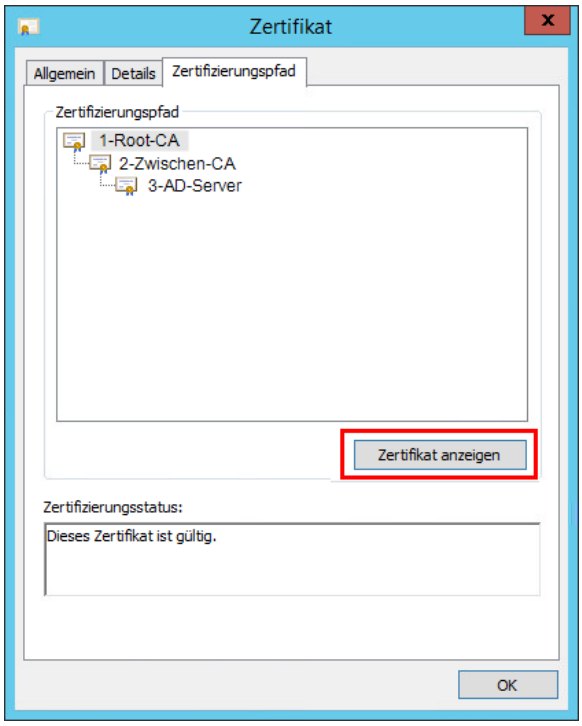

Abb. 3: Das Root-Zertifikat auswählen und anzeigen.

2) Auf dem Detaildialog für das Zertifikat „1-Root-CA“ kann nun über den Button „In Datei kopieren“ ein Zertifikatsexport angestoßen werden.

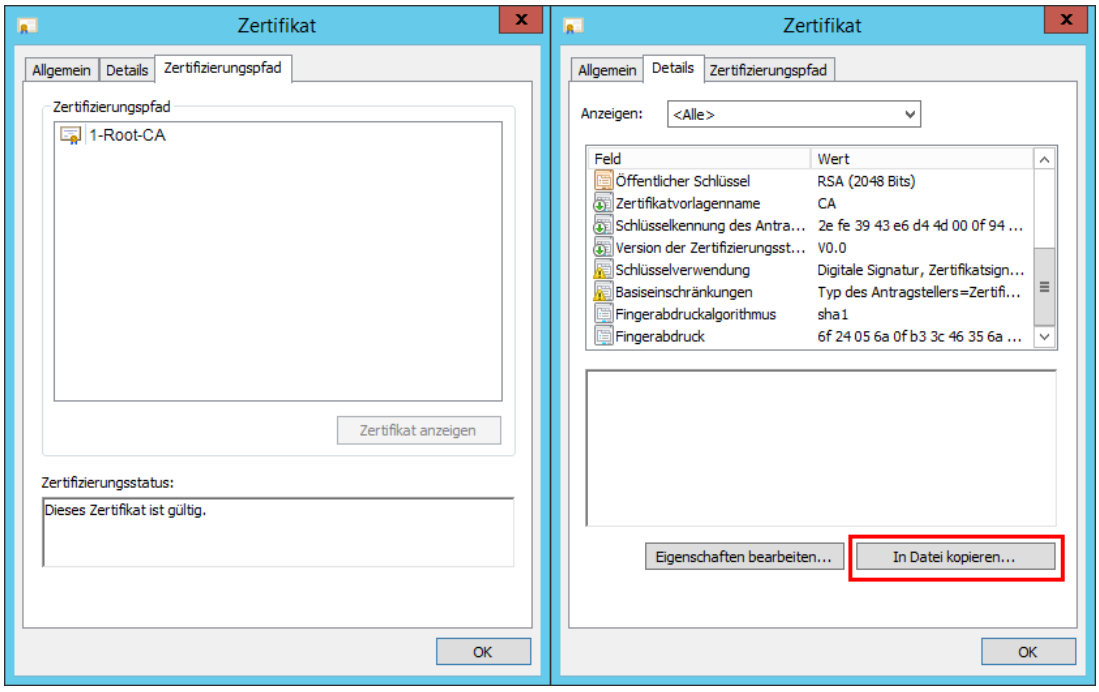

Abb. 4: Auf dem geöffneten Root-Zertifikat einen Zertifikatsexport starten.

3) Das Zertifikat „Base 64 codiert X.509 (.CER)“ z.B. in die Datei „adroot.cer“ exportieren.

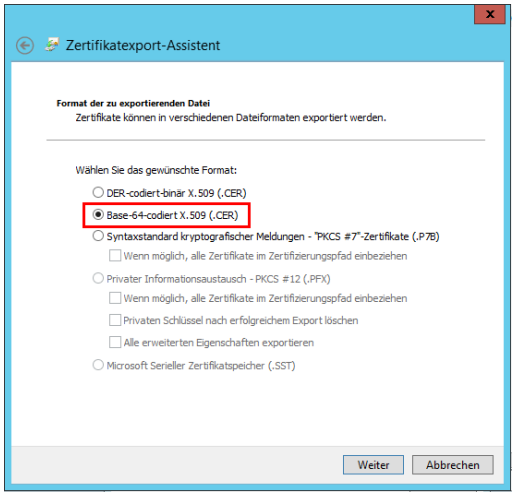

Abb. 5: Zertifikatsexport Base-64-codiert veranlassen.

4) Die Datei adroot.cer in adroot.pem umbenennen (das Base-64-codiert X.509 (.CER) Format entspricht dem PEM-Format).

Die adroot.pem muss dann dem DOCUMENTS -Server so zur Verfügung gestellt werden, dass dieser darauf zugreifen kann, indem man sie beispielsweise im Serververzeichnis ablegt.

Hinweis
Ein korrekt konfigurierter LDAPS – Server liefert mögliche Zwischenzertifikate beim TLS/SSL-Handshake implizit aus. Falls durch fehlerhafte Konfiguration dies nicht erfolgt, können in der pem-Datei weitere Zwischenzertifikate miteingefügt werden.

3. DOCUMENTS-LDAPS-Konfiguration

Zur Prüfung Zunächst muss das Testskript „otrTestLdapConnection.xml“ importiert werden. Die Datei wird mit ausgeliefert und befindet sich im Verzeichnis „\server\scriptlibs\Ldap\“.

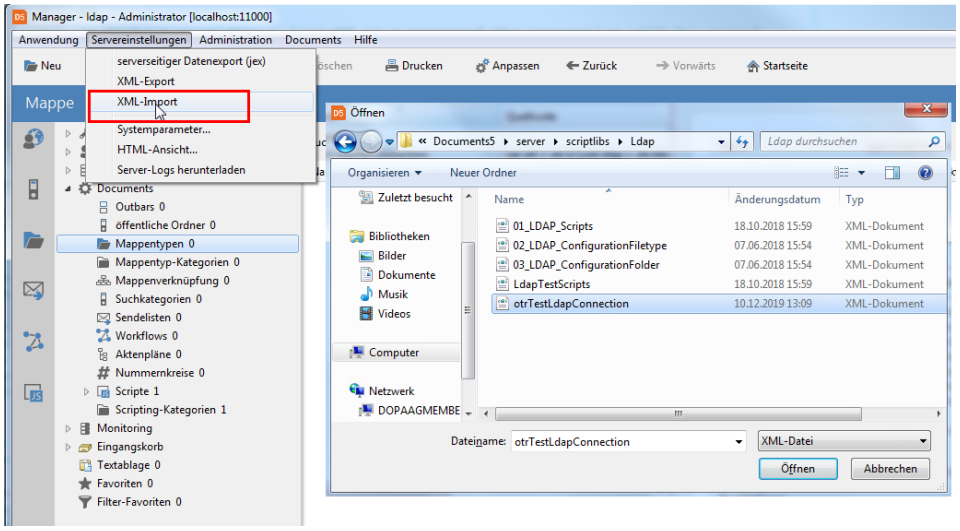

Abb. 6: XML-Import der openLdapSSLConnection.xml

Anschließend müssen die Verbindungsdaten als Script-Parameter konfiguriert und das Skript ausgeführt werden. (Bitte keine Änderungen am Script-Quelltext durchführen, da es signiert ist und damit auch ohne Scripting-Lizenz ausführbar ist.)

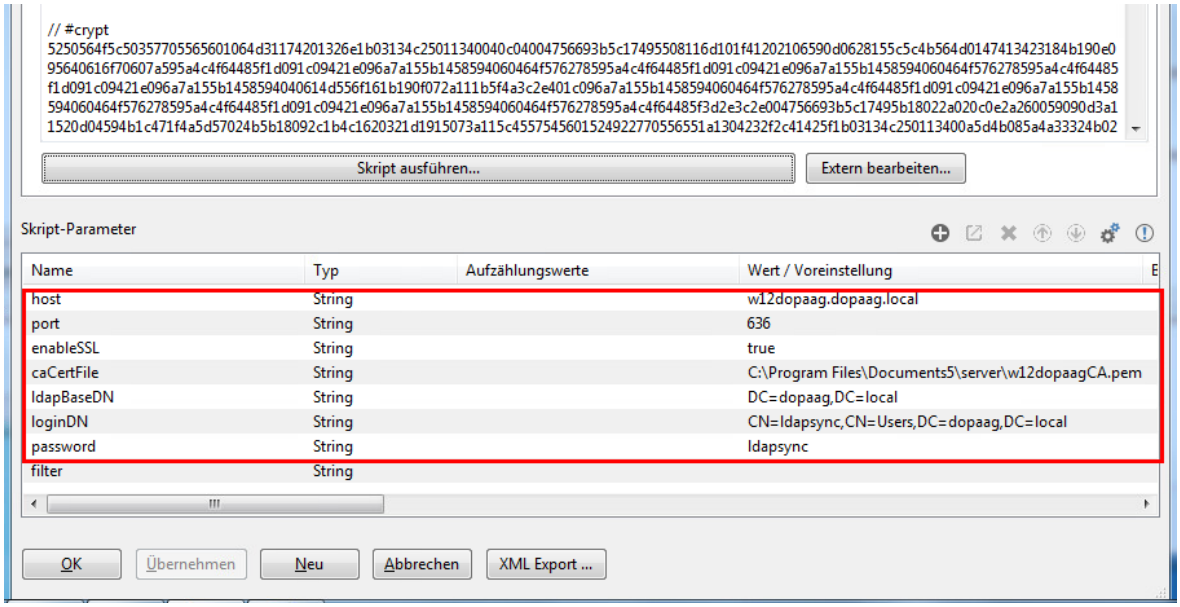

Abb. 7: Verbindungsdaten für den SSL-Zugriff

Wenn die Verbindung geöffnet werden konnte, so wird im Serverfenster und auf dem Client die folgende Meldung ausgegeben:

```
Verbindung hergestellt mit [Domain-Name]
```

Kann die Verbindung nicht hergestellt werden, so wird die Fehlermeldung angezeigt, die aus der openLdap-Schnittstelle an den Server weitergereicht wurde.

Hinweis
Wenn Änderungen am caCertFile vorgenommen wurden, kann es notwendig sein den DOCUMENTS-Server neu zu starten, da die openLdap-Schnittstelle die Zertifikate cached.

Wenn der Verbindungstest erfolgreich war, so müssen für den LDAP-Job und das LDAP-Logon im Weiteren die SSL-spezifischen Parameter als Eigenschaften am Mandanten oder optional in dem Skript „LdapParamDomain“ angepasst werden.

Wenn die Konfiguration mit Hilfe des LDAP Wizards im DOCUMENTS Manager durchgeführt wurde, empfiehlt es sich am Mandanten die Eigenschaften LdapPort, LdapEnableSSL und LdapCaCertFile zu setzen (in zukünftigen Versionen von DOCUMENTS kann diese Konfiguration im LDAP Wizard durchgeführt werden).

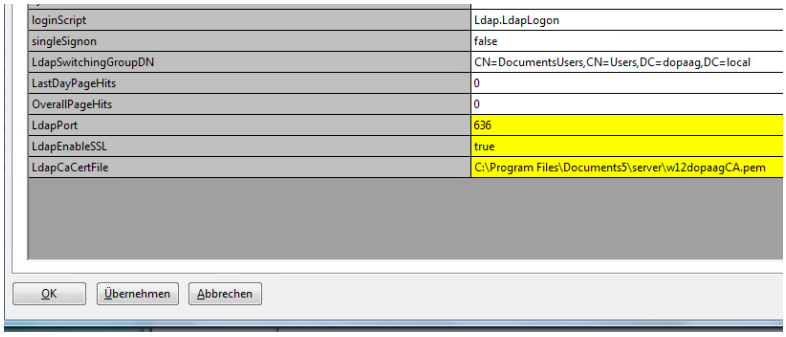

Abb. 8: LDAP-SSL Eigenschaften am Mandanten

Optional kann die Konfiguration im Script „server\scriptlibs\Ldap\LdapParamDomain.js“ vorgenommen werden (z.B., wenn mehrere LDAPS-Server angesprochen werden müssen) oder falls die LDAP-Scripte in den DOCUMENTS-Manager importiert wurden (XML-Import: 01_LDAP_Scripts.xml), dann muss die Konfiguration im DOCUMENTS-Manager im PortalScript „LdapParamDomain“ erfolgen.

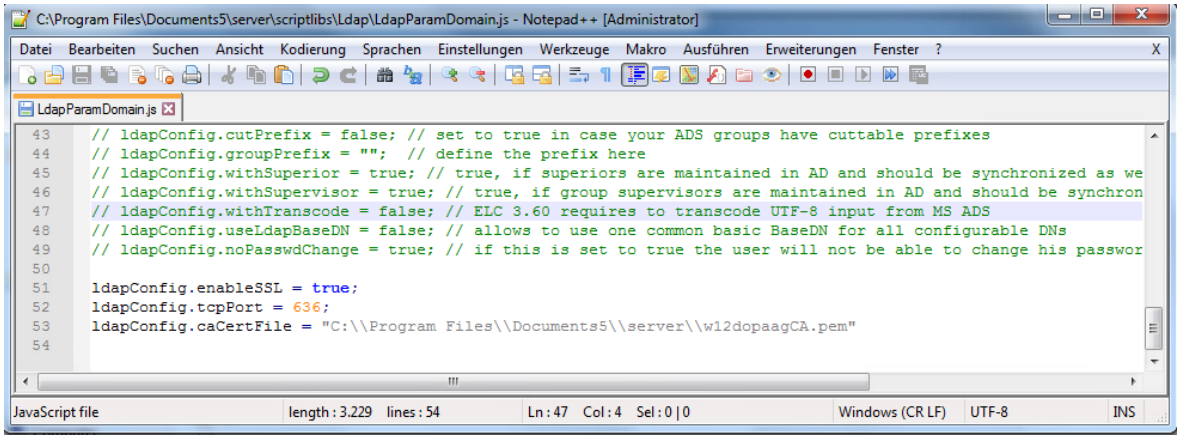

Abb. 9: Skript „LdapParamDomain“ mit den SSL-Parametern „enableSSL, tcpPort, caCertFile“

Abbildungsverzeichnis