LDAP over SSL

Gründe:

Die LDAP Kommunikation also die Schreib- und Lesevorgänge im Active Directory zwischen dem Client und/oder einem Server/Anwendung wird standardmäßig nicht verschlüsselt. Diese *Lücke* ermöglicht es einem Versierten, die Kommunikation zwischen einem Client und Server mitzuschneiden und auszuwerten. Daher empfehle ich die Aktivierung von SSL.

Anmerkung:

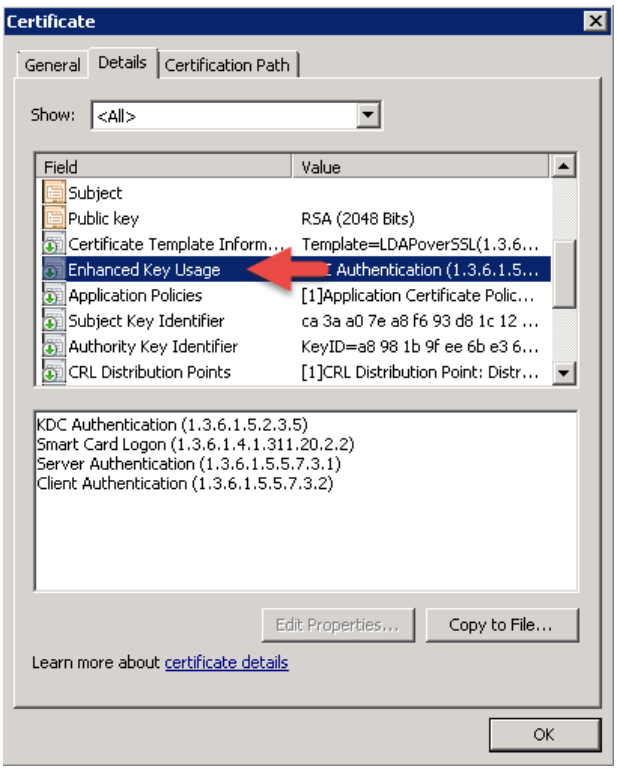
Ich spreche hier nur von der LDAP Datenübertragung! Andere Authentifizierungsmethoden wie z.B. die Autorisierung über Kerberos, SASL und NTLM haben ihre eigene Verschlüsselung und stehen hier nicht zur Debatte.

Voraussetzung:

Das neue *LDAPS*-Server Zertifikat muss die x.509 Zertifikat Erweiterung erfüllen.

Das Zertifikat muss folgende Properties aufweisen:

Enhanced Key Usage > Server Authentication (1.3.6.1.5.5.7.3.1)

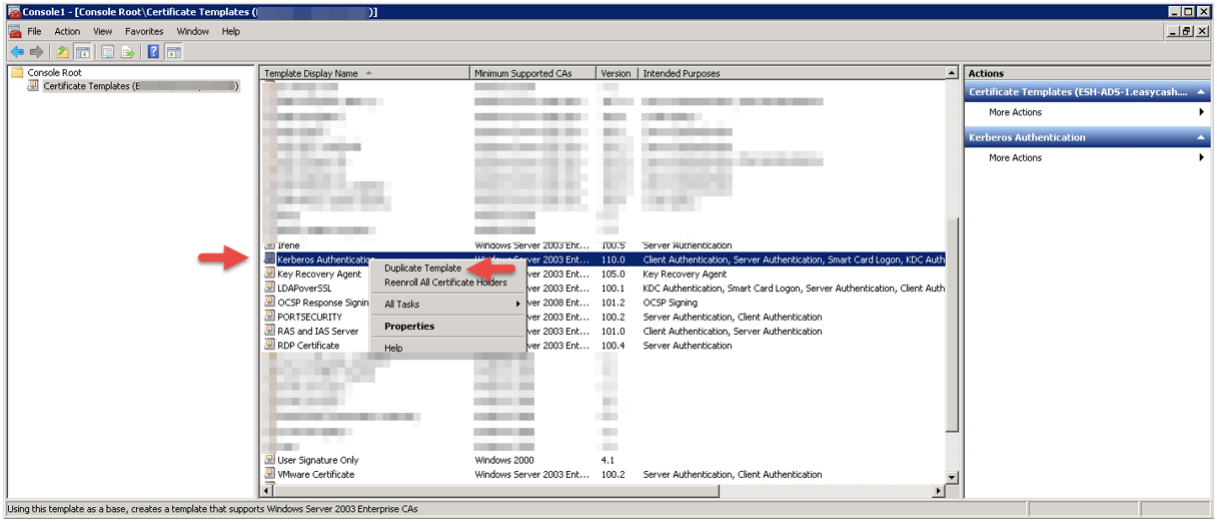


Die Freigabe des **TCP Ports 636** für LDAP und der **Port 3269** für den GC sollten natürlich auch erfolgt sein.

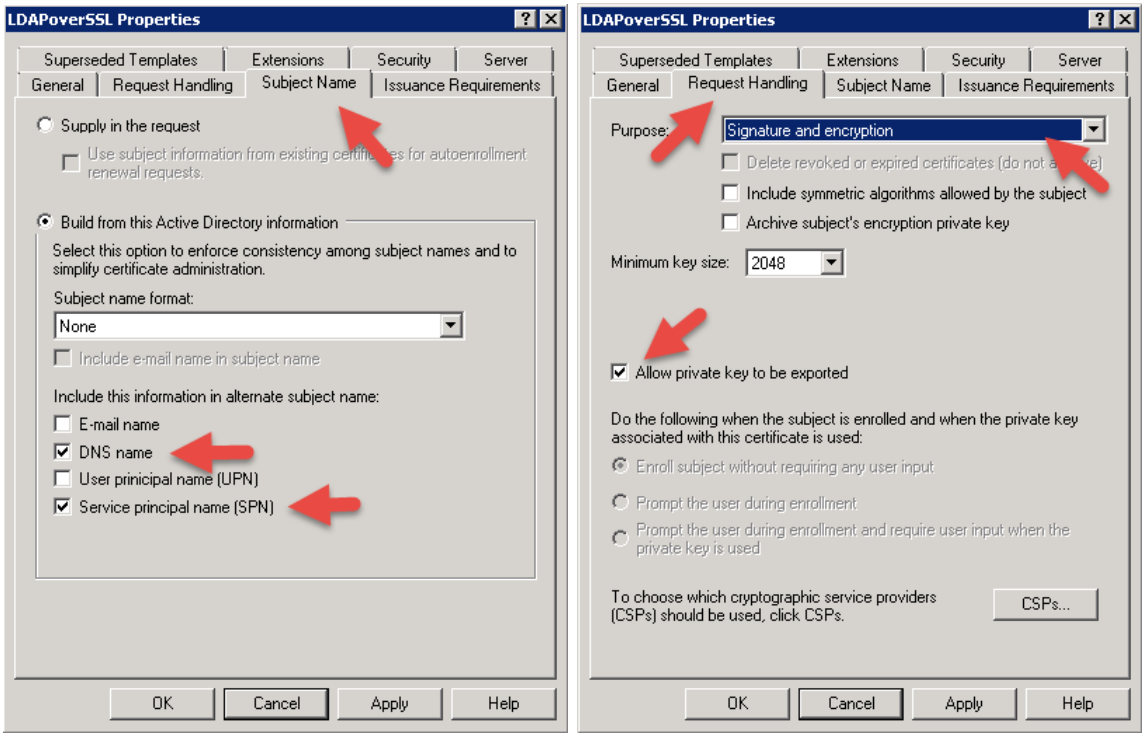
LDAP over SSL

Hinweis und Hilfe:

Wir duplizieren auf unserer CA das vorhandene Template (Kerberos Authentication) und nennen es LDAPoverSSL.



Bei der Duplizierung ist darauf zu achten, dass unter dem **> Reiter Subject Name** DNS und SPN Name ausgewählt werden. Wenn das Zertifikat über den AD DS importiert werden soll, dann muss der Private Schlüssel unter dem **> Reiter Request Handling** als exportierbar aktiviert werden.

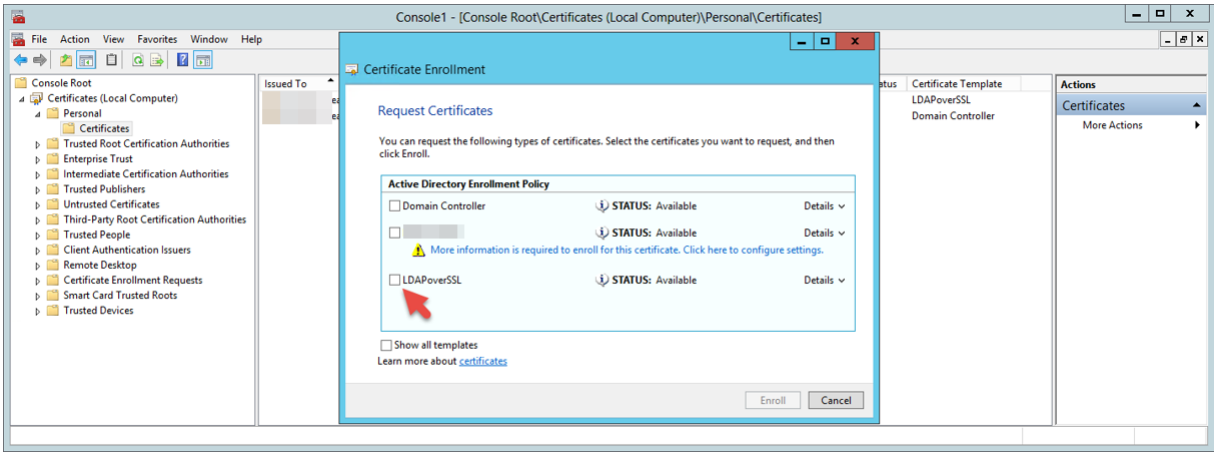


In unserer Umgebung habe ich den fehlenden Haken bei **Service Principal Name** nachgesetzt, siehe linkes Bild.

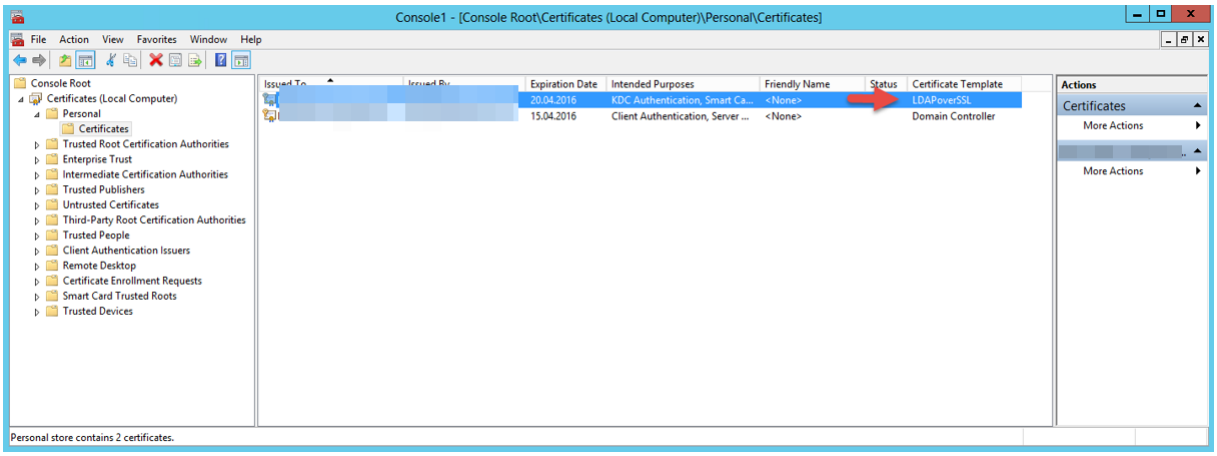
LDAP over SSL

Die Umsetzung von LDAPS Server-Authentifizierung in kurzen Schritten erklärt:

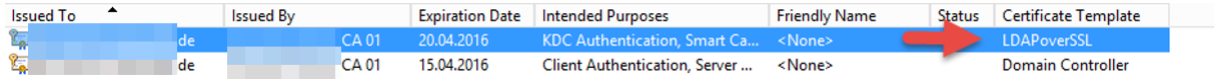
Auf jedem DC der eine Server-Authentifizierung über LDAPS anbieten soll muss das Zertifikat LDAPoverSSL angefragt werden.



Nach der Zertifikatsanfrage wird das Zertifikat im Personal Speicher abgelegt.



Vergrößerung



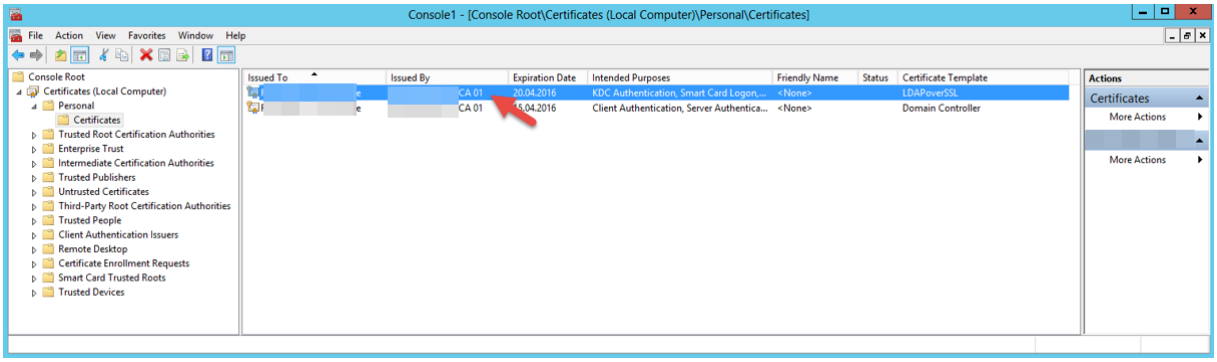
Fertig.

LDAP over SSL

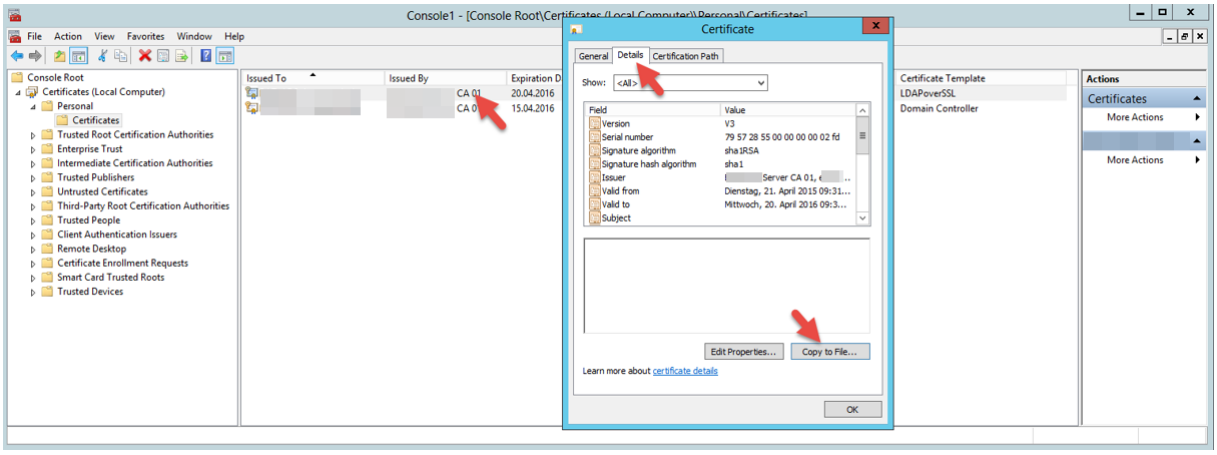
Die Umsetzung von LDAPS AD DS in kurzen Schritten erklärt:

Bevor wir anfangen die AD DS (Active Directory Domain Services) zu konfigurieren müssen wir noch das **LDAPoverSSL** Zertifikat exportieren.

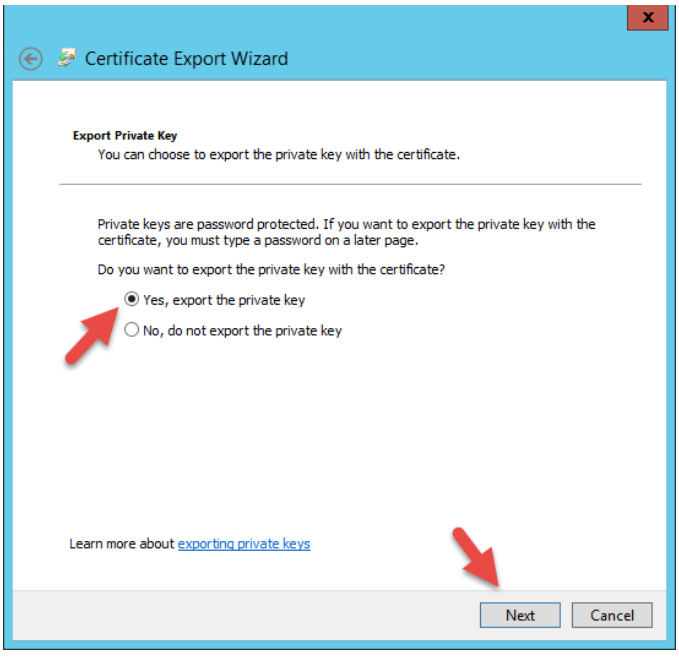
Dazu öffnen wir die mmc auf einem DC der das Zertifikat bereist angefragt und im Speicher hat.



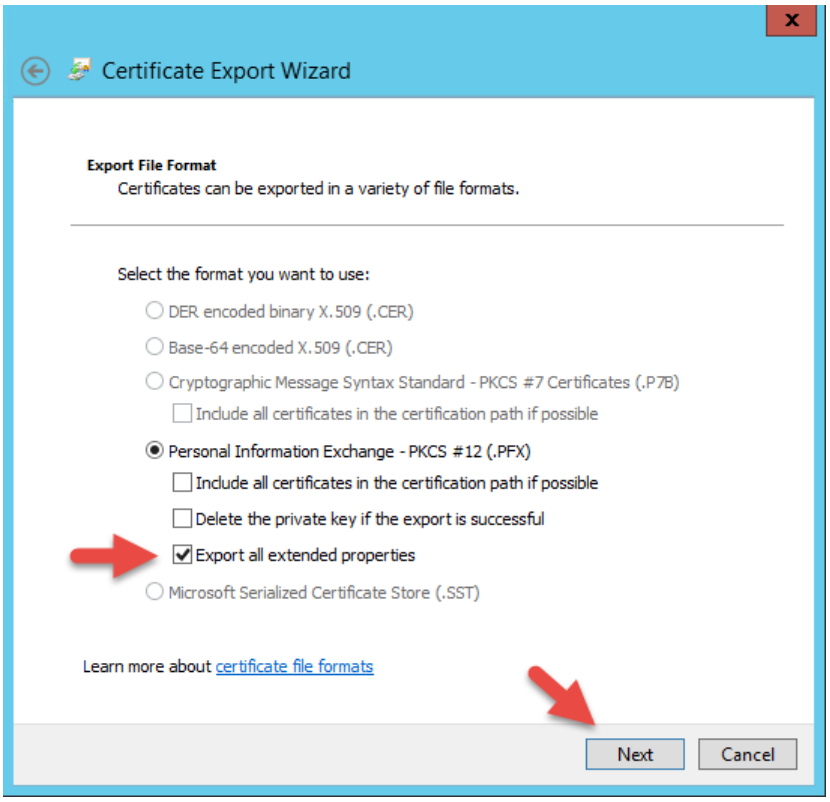
Doppelklick auf das Zertifikat **> Reiter Details > Copy to File...**



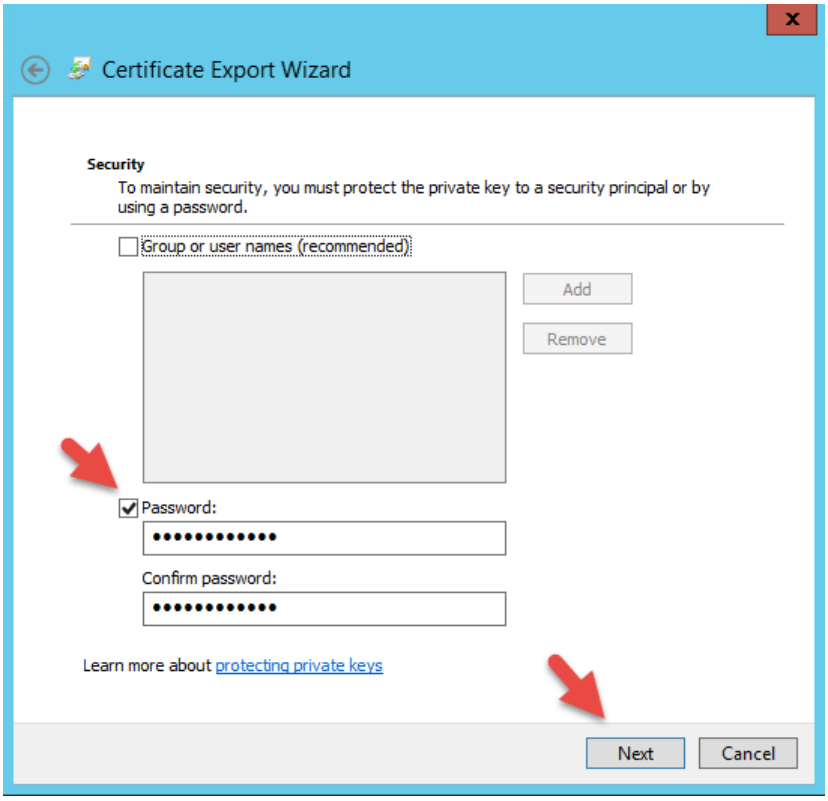
Klicken im nächsten Fenster auf **> Next** und aktivieren den **Export** des **privaten** Schlüssels.



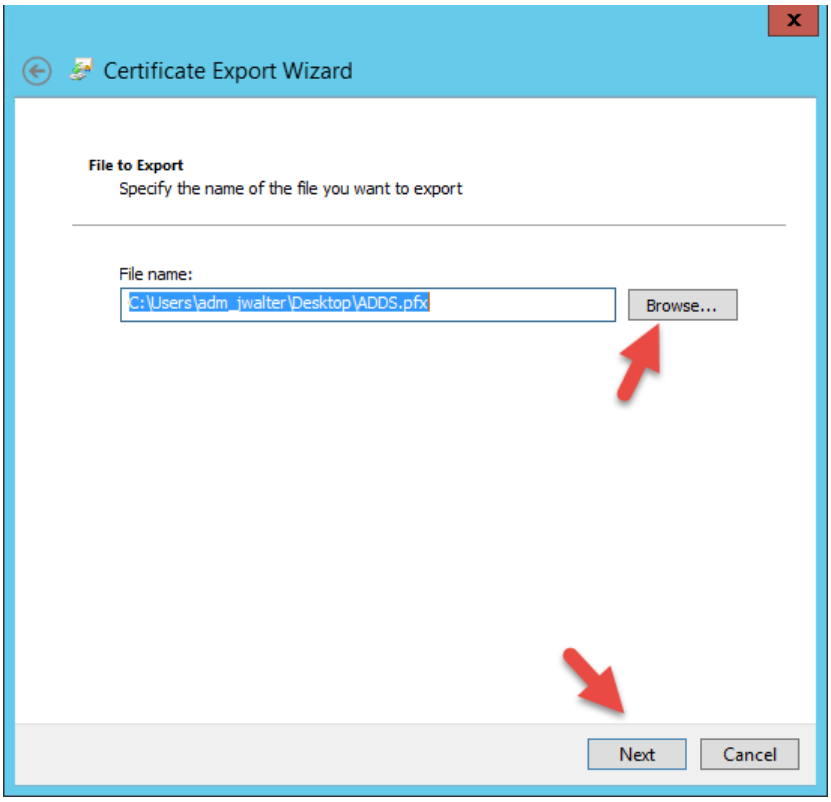
Exportieren alle erweiterten Einstellungen und klicken auf **> Next**



Vergeben ein sicheres Passwort und klicken auf **> Next**

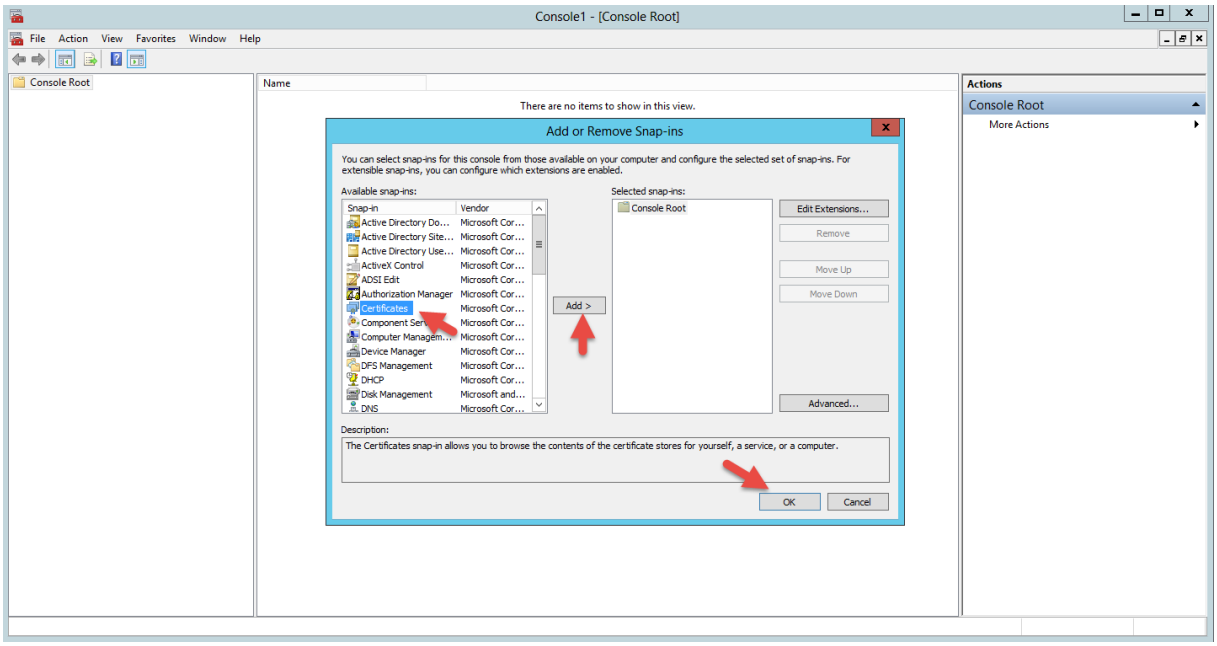


Geben einen Speicherort an und klicken auf **> Next und > Finish**

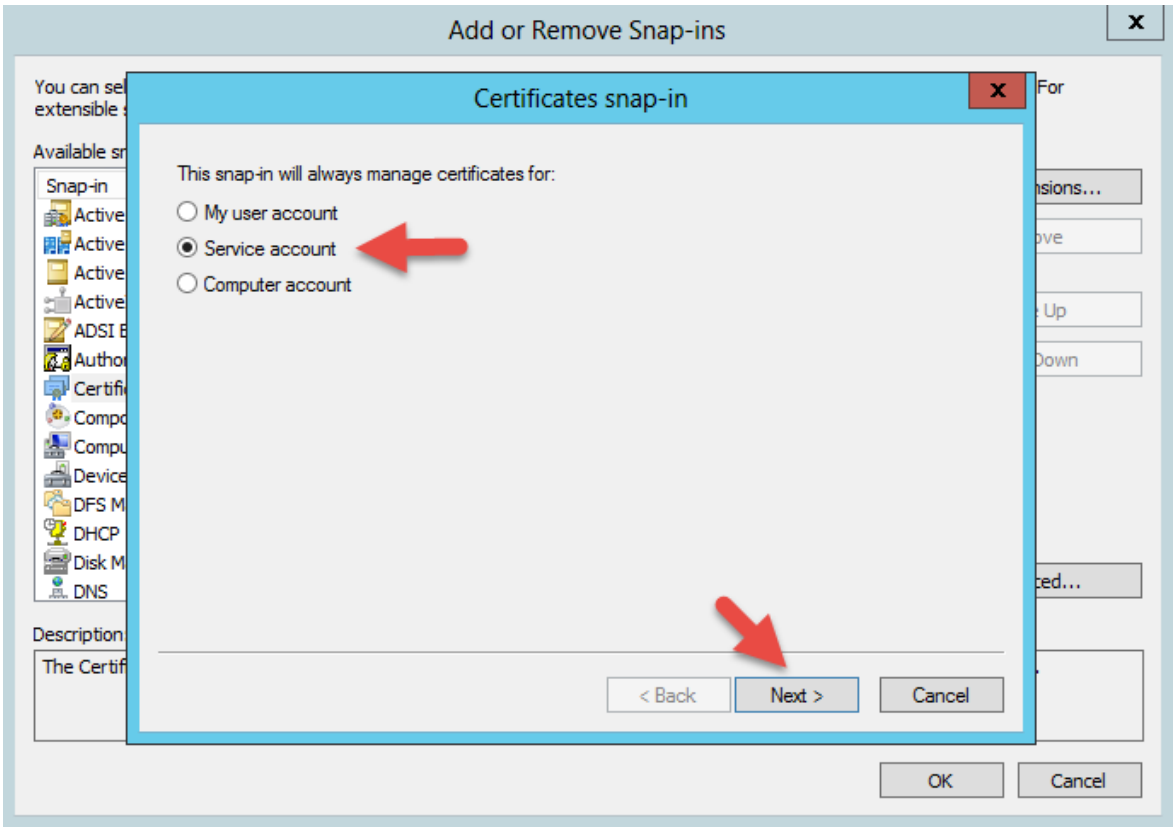


Die Vorarbeiten sind getan, kommen wir jetzt zur Einrichtung des „AD DS" Active Directory Domain Services.

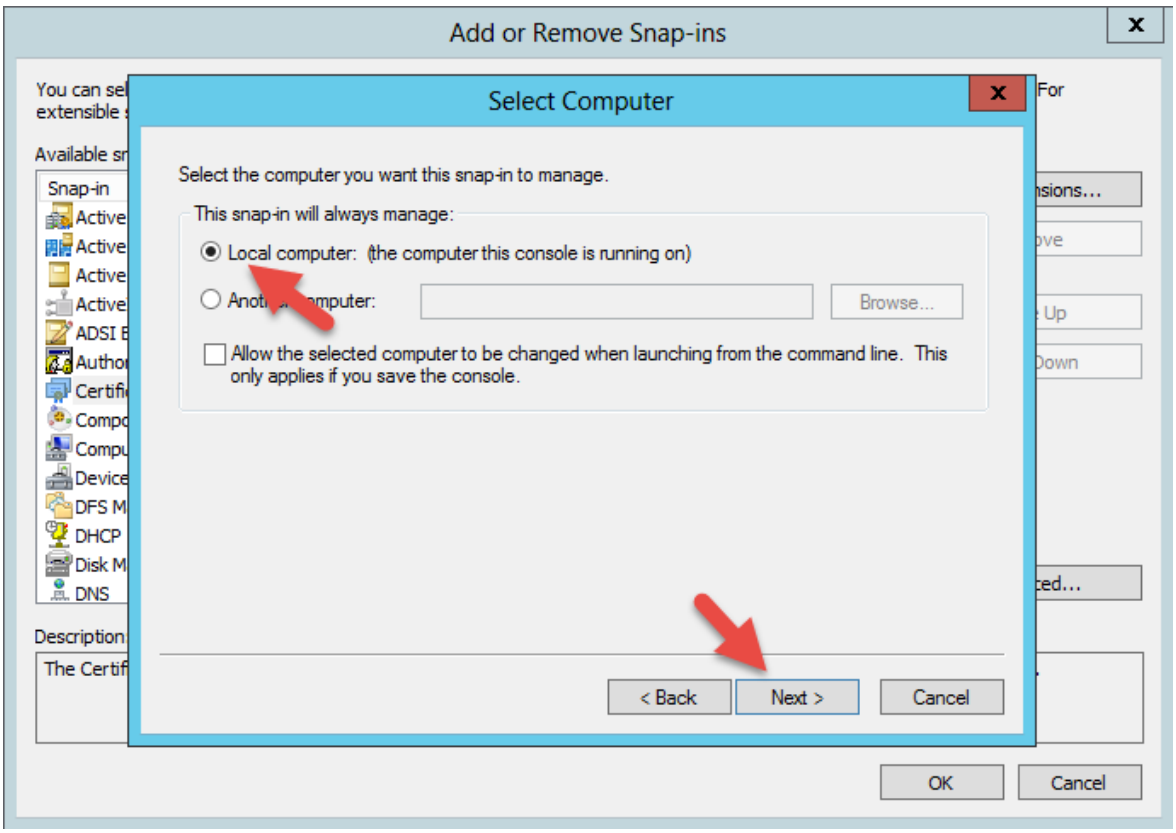
Wir öffnen auf dem DC die **mmc** und fügen aus der Konsole das **Snap-In Certificate** hinzu.



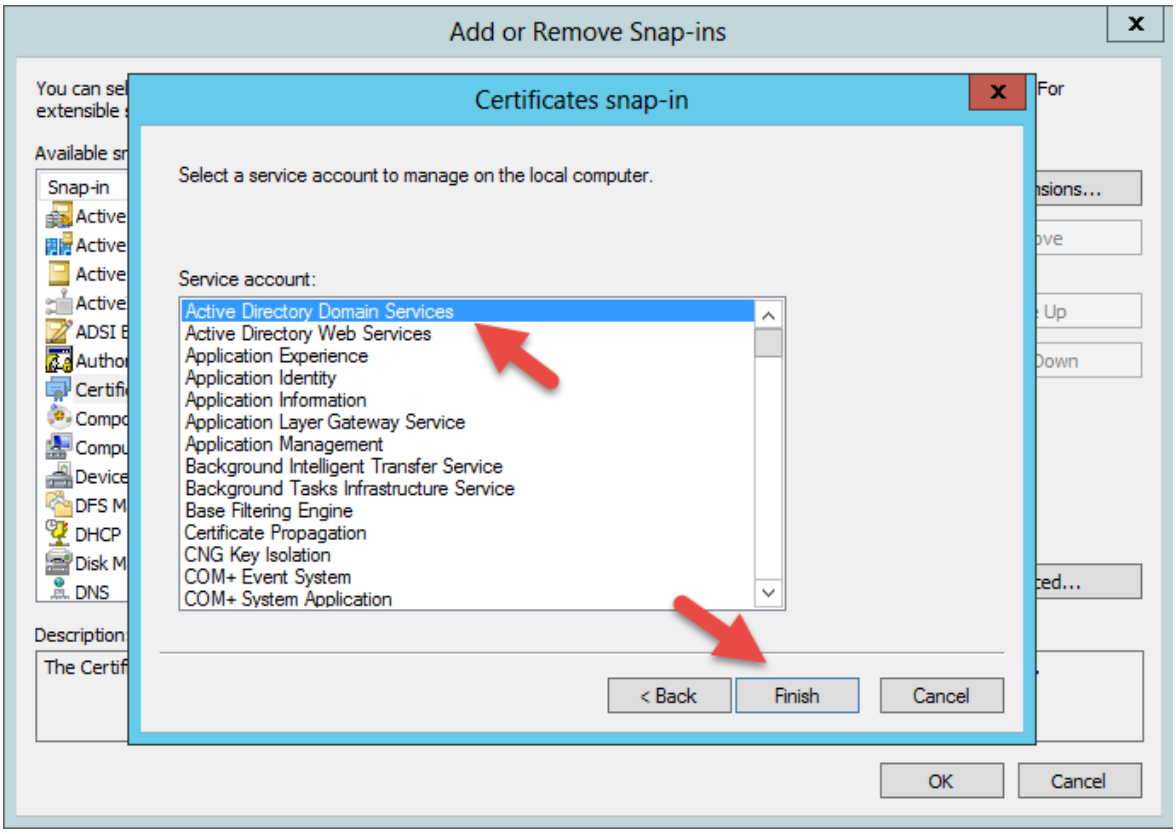
Wählen den **Service Account** aus und klicken auf **> Next**



Treffen die Auswahl **Local Computer** und Klicken auf **> Next**

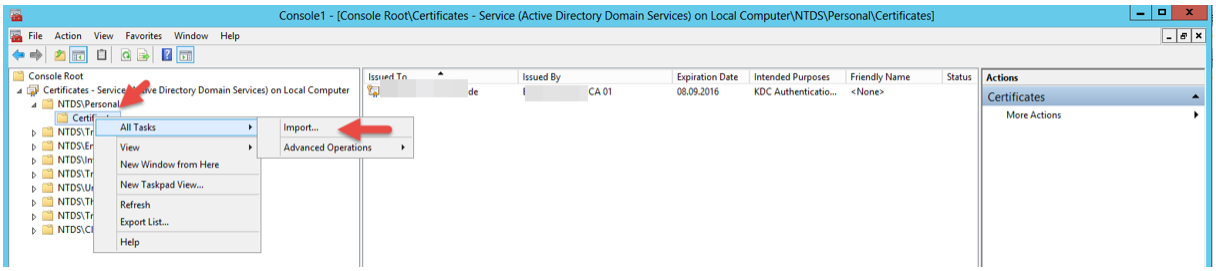


Entscheiden uns für den **Active Directory Domain Services** und Klicken auf **> Finish**

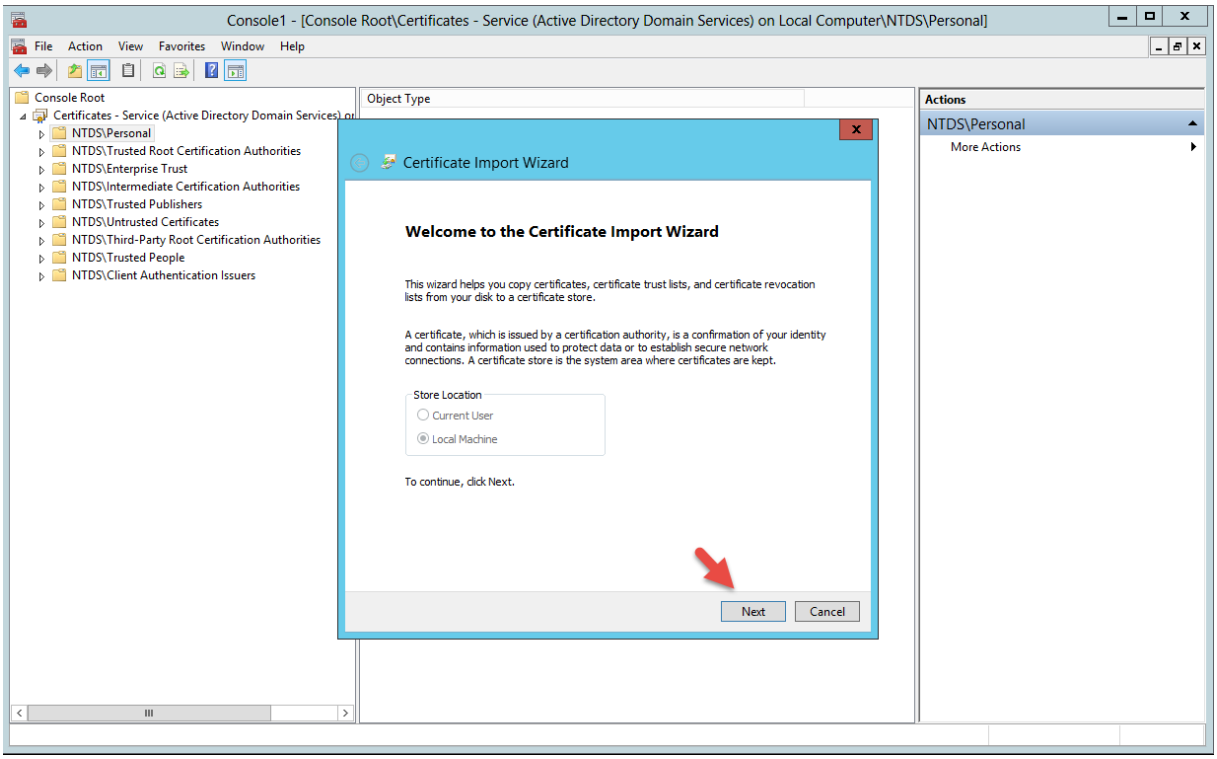


Ganz wichtig! Der Import des Zertifikats muss in den **NTDS Personal Store** geschehen.

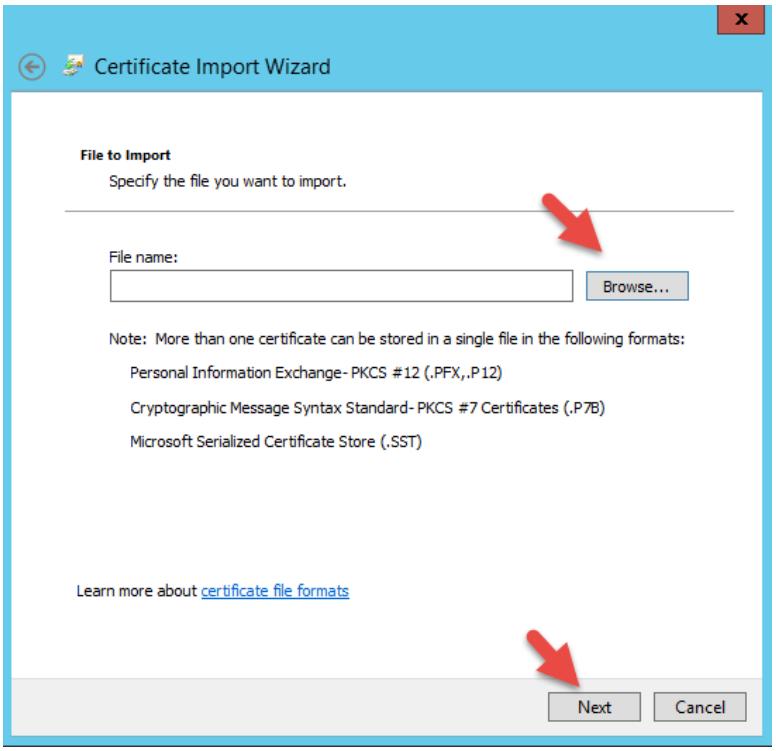
Rechtsklick auf **NTDS Personal Store > Certificates > Import**



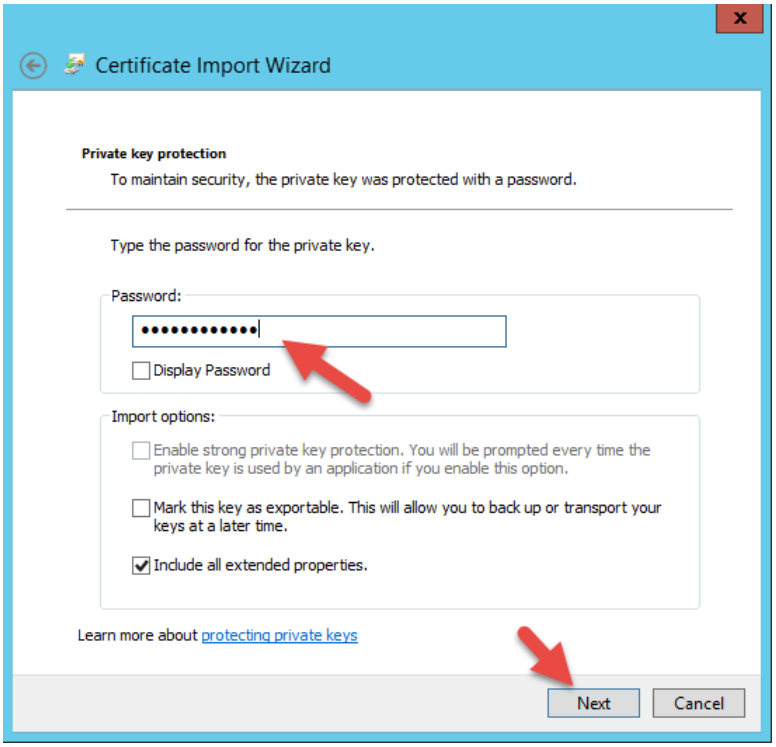
Der Wizard startet und klicken auf **> Next**



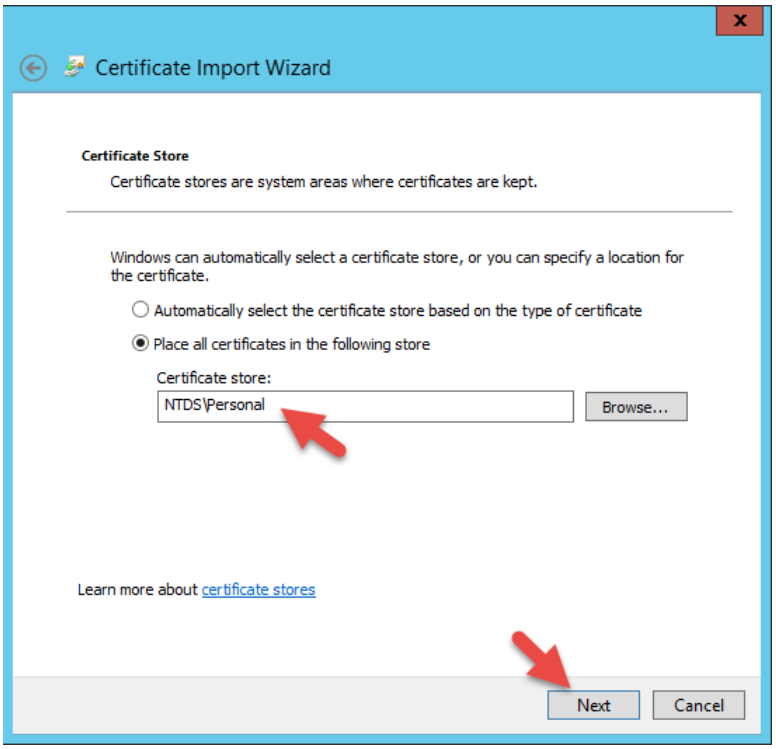
Navigieren über > **Browse**… zum Zertifikat, wählen es aus und klicken auf **> Next**



Wenn der Private Schlüssel exportiert wurde, dann folgt noch die Passwortabfrage während des Importvorgangs.



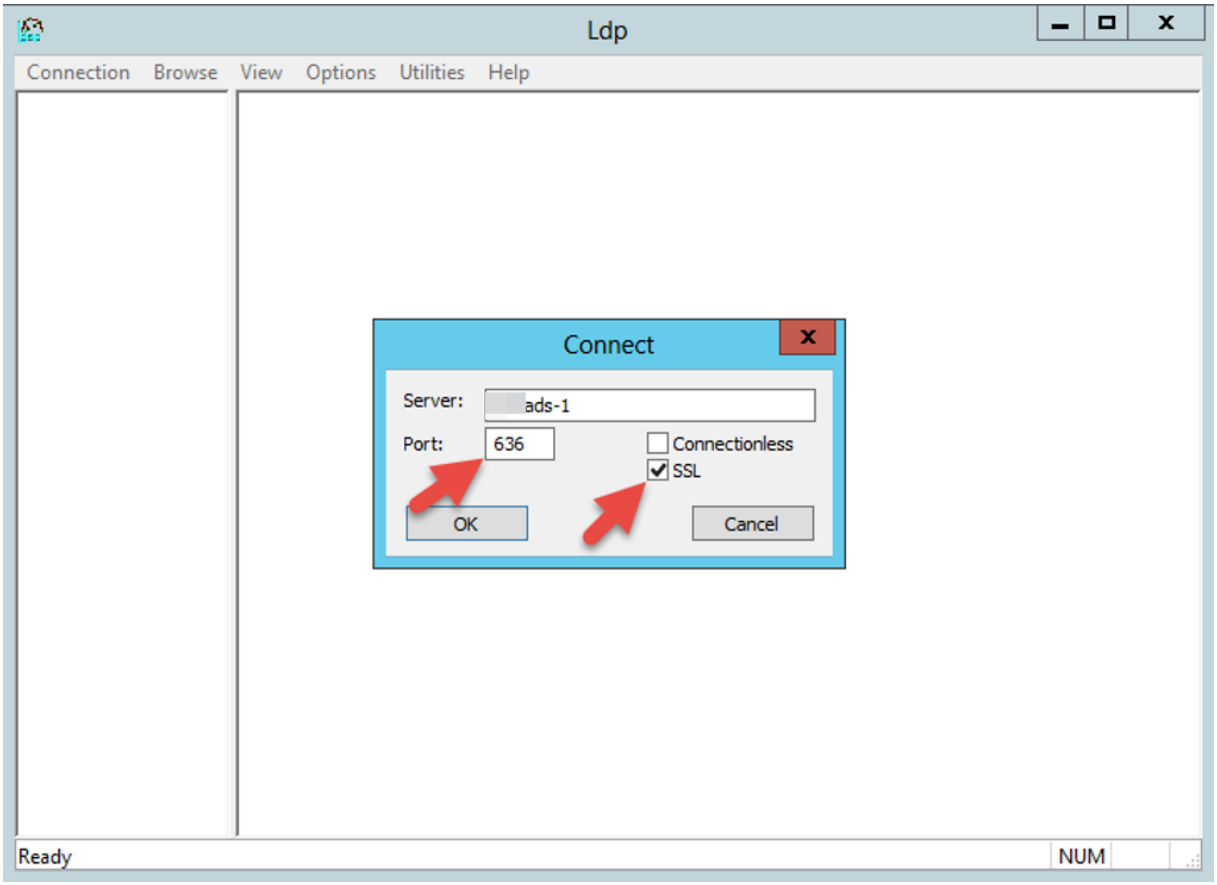
Der Store ist somit ausgewählt



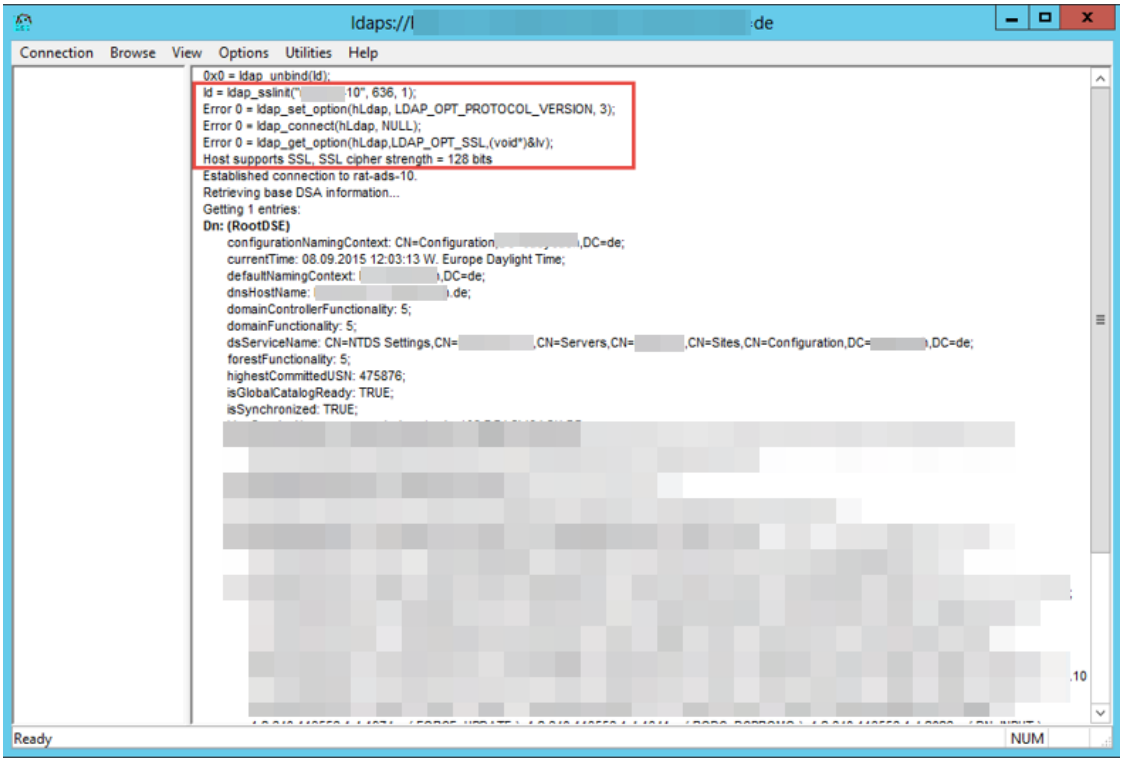
LDAP over SSL

Überprüfung:

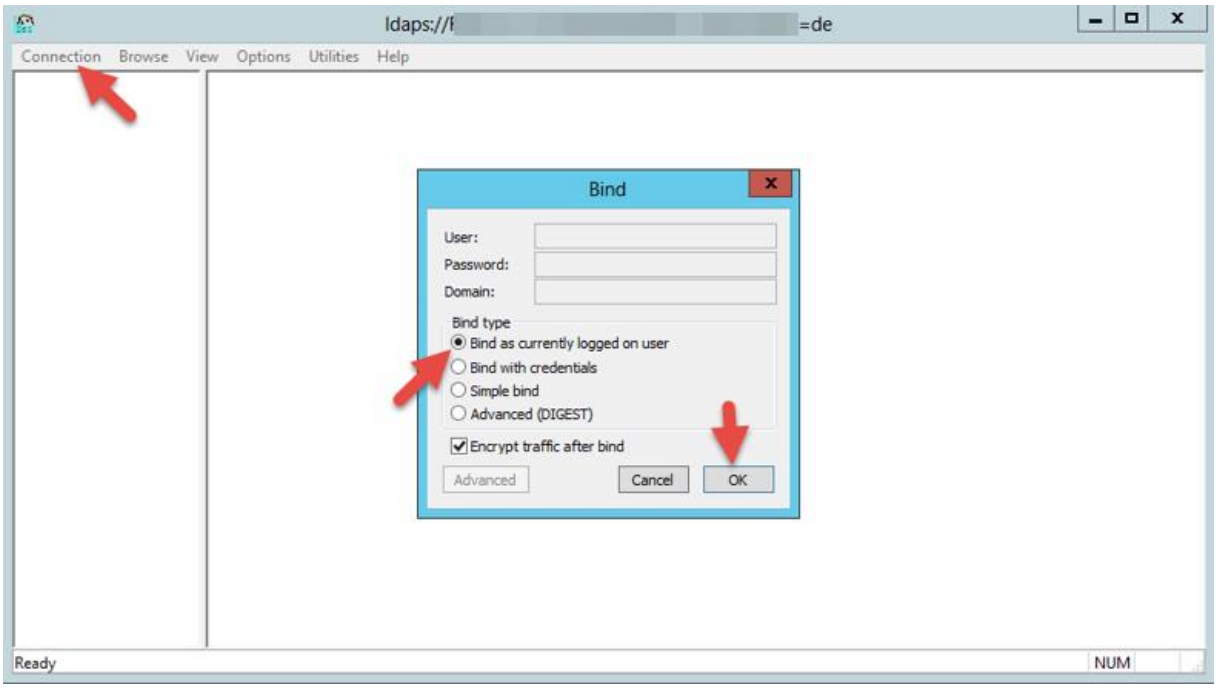
Zur Überprüfung der Einrichtung öffnen wir das Tool **ldp.exe** und verbinden uns mit einem anderen DC über den **Port 636 und SSL**.



Wenn die Verbindung über den **Port 636** zustande kam sollte alles in Ordnung sein.



Sollte der Test nicht erfolgreich sein, dann ist das Binding zu prüfen.



Dieser Vorgang muss auf allen DCs die LDAPS AD DS anbieten sollen umgesetzt werden!

Fertig.

LDAP over SSL

Weitere Infos:

Voraussetzungen für ein LDAPS-Zertifikat im Detail

Um LDAPS aktivieren zu können, müssen wir ein Zertifikat installieren, das folgende Voraussetzungen erfüllt:

- Das LDAPS-Zertifikat befindet sich im persönlichen Zertifikatsspeicher des lokalen Computers (im Programm der Zertifikatsspeicher Meine.
- Ein privater Schlüssel, der dem Zertifikat entspricht, ist im Speicher des lokalen Computers vorhanden und wird korrekt mit dem Zertifikat verknüpft. Für den privaten Schlüssel darf keine verstärkte Sicherheit aktiviert sein!
- Die Erweiterung "Erweiterte Schlüsselverwendung" enthält die Objektkennung (OID) der Serverauthentifizierung (1.3.6.1.5.5.7.3.1).
- Der voll qualifizierte Domänenname des Domänencontrollers im Active Directory (zum Beispiel rat-ads-1) muss an einer der folgenden Stellen erscheinen:
  - Allgemeiner Name (CN = Common Name) im Antragstellerfeld oder
  - DNS-Eintrag in der Erweiterung "Alternativer Antragstellername".
- Das Zertifikat wurde von einer Zertifizierungsstelle ausgestellt, der der Domänencontroller und die LDAPS-Clients vertrauen, in diesem Fall CA-01. Die Vertrauensstellung wird eingerichtet, indem Clients und Server so konfiguriert werden, dass sie der Stammzertifizierungsstelle vertrauen, der die ausstellende Zertifizierungsstelle untergeordnet ist.
- Der Microsoft RSA Schannel Cryptographic Service Provider (CSP) muss zur Erstellung des Schlüssels verwendet werden.