## LDAPS für EASY Archive

Zur Verschlüsselung der Kommunikation mit dem externen Verzeichnisdienst (SSL-/TLS-Verschlüsselung) wird ein gültiges Zertifikat benötigt. Dieses muss zuerst erstellt werden. Alternativ kann ein vorhandenes Zertifikat verwendet werden.

Das Zertifikat muss für die "Server-Authentifizierung" ausgestellt werden und den Servernamen und den vollqualifizierten Servernamen (fully qualified server name) als "DNS-Name"-Eintrag enthalten.

Console1 - [Console Root\Certificates (Local Com	nputer)\Trusted Root Certification A	ithorities\Certificates]				
奋 File Action View Favorites Window He	lp	R Zertifikat	×			
Console Root	Issued To	Issued By adc	Expiration Date 14.06.	Intended Purposes Server Authentication	Allgemein Details Zertifizierungspfad	_
<ul> <li>Preside Root Certification Authorities</li> <li>Certificate:</li> <li>Entermediate Certification Authorities</li> <li>Trusted Publishers</li> <li>Untrusted Certification Authorities</li> <li>Trusted Party Root Certification Authorities</li> <li>Trusted Party Root Certification Authorities</li> <li>Client Authoritication Issuers</li> <li>Preview Build Roots</li> <li>Test Roots</li> <li>Renote Desktop</li> <li>Certificate Roots</li> <li>Strusted Cardificate Roots</li> <li>Trusted Paviper</li> <li>Windows Live ID Token Issuer</li> </ul>		Certificate Certification Pair Certification Pair Show: <ai> Field Public key Public key parameters Certification Pair Constraints Enhanced Key Usage Basic Constraints DNS Name-adc DNS Name-adc Usage Usage DNS Name-adc Usage U</ai>	h Value ESA (2048 Bits) 05 00 OKS Home-add; DKS Server Authenticator Digital Signature, Ke Subject Type=End B Desilae479e3606600	×	Zertifikatsinformationen         Dieses Zertifikat ist für folgende Zwecke beabsichtigt:         • Garantiert die Identität eines Remotecomputers         Ausgestellt für:         Ausgestellt für:         Ausgestellt von:       galdep.local	_
			Edit Properties !	Copy to File OK	Sie besitzen einen privaten Schlüssel für dieses Zertifikat.	ärung OK

Das Zertifikat muss im DER-Format exportiert werden.

Der EASY-Archivserver macht keinen Gebrauch vom Zertifikatsspeicher des Windows-Betriebssystems. Daher muss das Zertifikat in den Truststore der Java-Laufzeitumgebung des EASY-Archivservers importiert werden.

Dies geschieht mit dem Tool keytool.exe, das Sie im Unterverzeichnis Java Runtime Ihrer EASY-Archiv-Installation finden, d.h.

c:\<EASY Archive installation directory>\<jre-version>\bin\keytool.exe -import -alias <Aliasname> -file <path/file name of the certificate> -keystore c:\<EASY Archive installation directory>\<jre-version>\lib\security\cacerts

Der Parameter AliasName kann frei gewählt werden.

Dann werden Sie aufgefordert, ein Passwort einzugeben. Das Standard-Passwort des JAVA- Schlüsselspeichers ist "changeit" (ohne Anführungszeichen).

Danach muss die Option "SSL" im LDAP-Assistenten (zu finden im Configuration Manager  $\rightarrow$  Benutzerverwaltung  $\rightarrow$  Verzeichnisdienste  $\rightarrow$  Rechtsklick "Verzeichnisdienst bearbeiten") aktiviert werden.

Der Port 389 DARF NICHT geändert werden. Die Änderung auf Port 636 (LDAPS-Standard) wird intern vorgenommen.

EN	Create new connection	
Credentials Please enter the credentials for the directory service.		5
		EASY ENTERPRISE.x
Server IP address ADSERVERS	Port 389	SSL

Abschließend muss der EASY-Archivdienst neu gestartet werden.