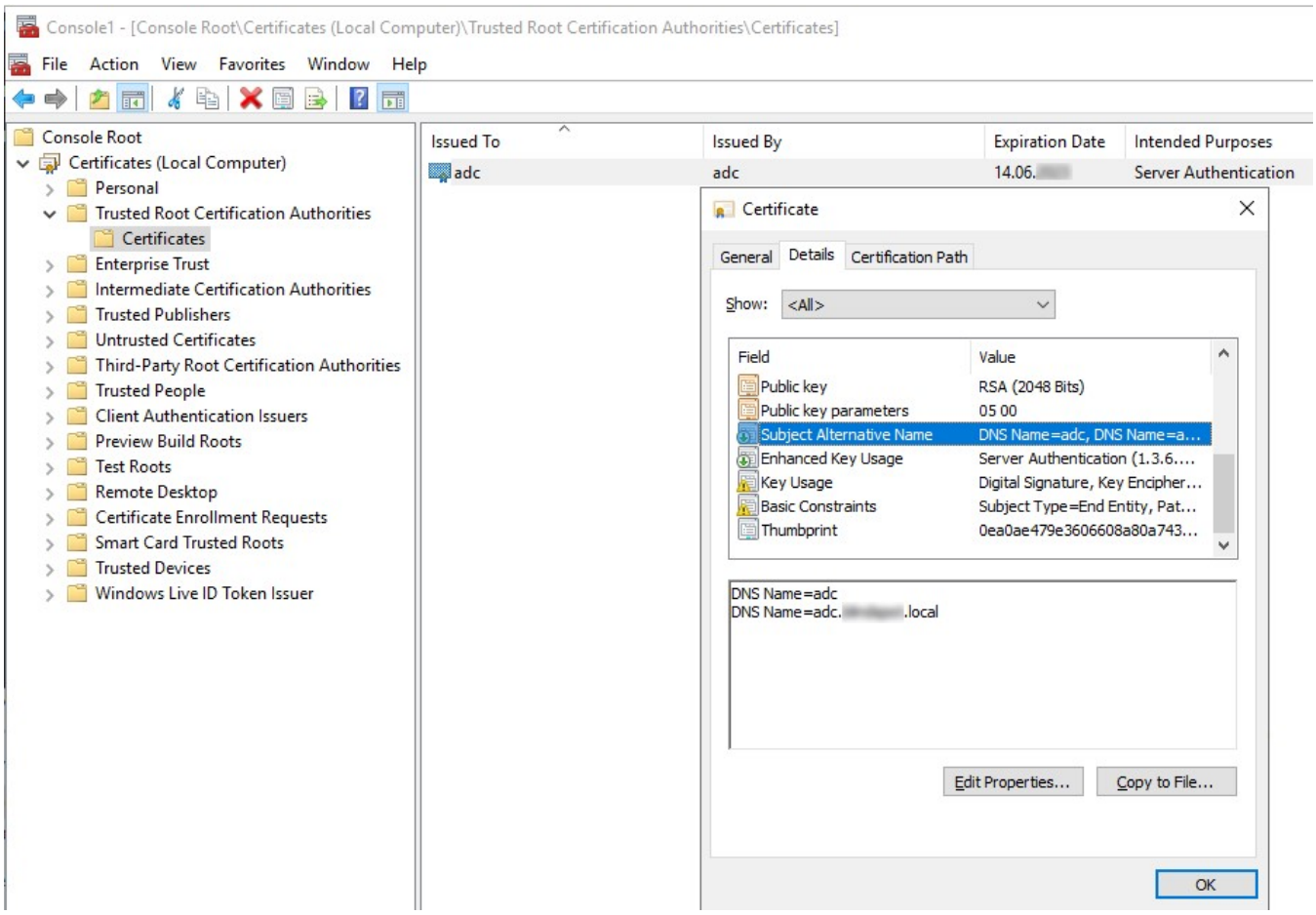
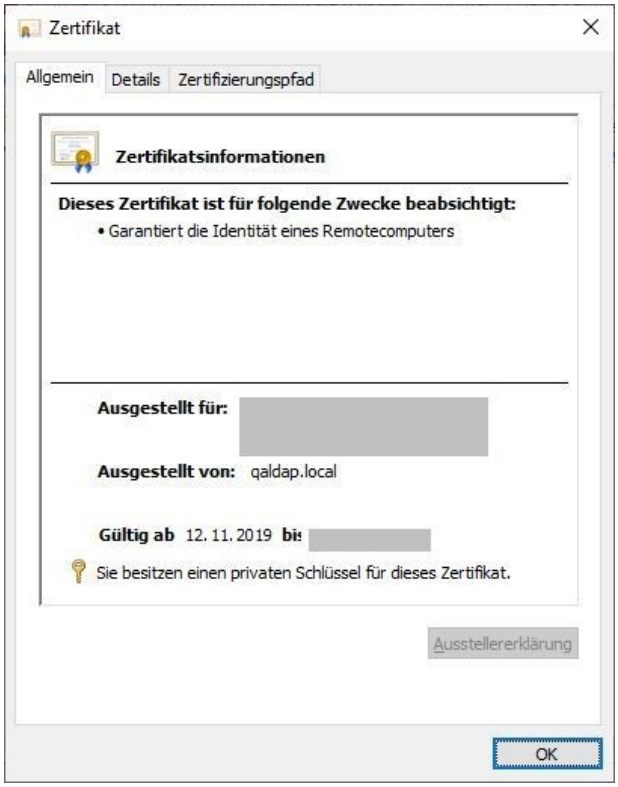
EASY Archive

To encrypt the communication with the external Directory Service (SSL encryption) a valid certificate is needed. This has to be created first. Alternatively, an existing certificate can be used.

The certificate must be issued for "Server Authentication" and contain the server name and the fully qualified server name as a "DNS Name" entry.





The certificate must be exported in DER format.

The EASY Archive server does not make use of the Certificate Store of the Windows operating system. Therefore, the certificate has to be imported into the truststore of the Java Runtime Environment of the EASY Archive server.

This is done by the *keytool.exe* tool to be found in the Java Runtime subdirectory of your EASY Archive installation, i.e.

```
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
```

The parameter *AliasName* can be freely chosen.

Then you will be prompted to enter a password. The default password of the JAVA keystore is "changeit".

Afterwards the "SSL" option in the LDAP wizard (to be found in Configuration Manager → User Management → Directory services → Right mouse click "Edit directory service") must be activated.

> The port 389 MUST NOT be changed. The change to port 636 (LDAPS default) is done internally.

Finally, the EASY Archive service must be restarted.