

LUDUS Web – Bestilling og installation af SSL-servercertifikat

Indhold

LUDUS Web – Bestilling og installation af SSL-servercertifikat	1
1. Introduktion	2
1.1 Bestilling af certifikat fra andre udbydere	2
2. Bestilling af certifikat fra UNI-C.....	3
2.1 Klargøring til bestilling.....	3
2.2 Bestilling af certifikat, herunder oprettelse af ny keystore og CSR-fil.....	3
3. Installation af certifikat fra UNI-C	4
3.1 Klargøring til installation.....	4
3.2 Installation af selve certifikatet vha. Comodos vejledning	5
3.2.1 Typiske fejlbeskeder og andre problemer ved installation.....	6
3.3 Installation af det nye certifikat i LUDUS Web.....	7
4. Eksempel på brug af keytool	8

1. Introduktion

For at kunne benytte LUDUS Web med SSL-kryptering kræves det, at der er installeret et server-certifikat i LUDUS Web.

Det er muligt at bestille et certifikat via UNI-C, der benytter Comodo som underleverandør af selve certifikatet. På denne måde får man et "officielt" certifikat, der er kendt af web-browseren, dvs. browseren kan umiddelbart danne en sikker forbindelse mellem brugeren og LUDUS Web.

1.1 Bestilling af certifikat fra andre udbydere

Bestiller man et certifikat fra andre udbydere end UNI-C, er det vigtigt at sikre sig at der bestilles et SSL-servercertifikat, og at det leveres i enten JKS- (Java Keystore) eller PKCS12-format.

Ved bestilling fra andre udbydere end UNI-C, så skal denne vejledning først følges fra punkt 3.3.

2. Bestilling af certifikat fra UNI-C

Bemærk: Ved bestilling af et certifikat hos Comodo (UNI-Cs nye certifikat-leverandør), er det vigtigt at der bestilles et certifikat af typen ”Java-based web servers (using keytool)”.

2.1 Klargøring til bestilling

Følgende 4 trin skal følges, *inden* Comodos vejledning til bestilling af certifikat tages i brug:

1. Opret et midlertidigt arbejdsbibliotek (herfra kaldet <TMP>). Det midlertidige arbejdsbibliotek må **ikke** være `keys`-biblioteket i LUDUS Web-installationen, men kan i stedet f.eks. være `C:\skole-certifikat`.
2. Åbn en kommandolinie og naviger til <TMP>.
3. Programmet `keytool.exe` skal findes i Path-miljøvariablen. Programmet er installeret sammen med Java (i underbiblioteket `bin`).

Path-variablen kan redigeres på følgende måde:

1. Åbn kontrolpanelet fra Start-menuen.
2. Vælg System.
3. Vælg avancerede indstillinger (Advanced).
4. Vælg miljøvariabler (Environment Variables).
5. Herefter redigeres systemvariablen Path ved at indsætte stien til `keytool.exe`.
Stien kan f.eks. være `C:\Programmer\Java\jdk_1.6.0_18\bin`.
4. Programmet `keytool.exe` skal findes i Path-miljøvariablen. Programmet er installeret sammen med Java (i underbiblioteket `bin`).

2.2 Bestilling af certifikat, herunder oprettelse af ny keystore og CSR-fil

Der skal nu dannes en ny keystore og CSR-fil ved at følge Comodos vejledning på URLen:

https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=244.

Vigtige bemærkninger til Comodos vejledning:

1. Udfør `keytool`-kommandoerne i vejledningen inde fra <TMP>-arbejdsbiblioteket.
2. **Vigtigt:** password til den keystore der oprettes, samt password til det alias der angives skal være det samme.

3. Installation af certifikat fra UNI-C

3.1 Klargøring til installation

Efter modtagelse af et nyt certifikat fra Comodo, skal følgende 2 trin følges, *inden* Comodos vejledning tages i brug:

1. Naviger hen til <TMP>-biblioteket, hvor keystore-filen, der blev oprettet i afsnit 2.2 ligger.

Det er vigtigt, at det er samme keystore-fil som CSR-filen blev dannet fra (CSR-filen er den fil, som I har indsendt til UNI-C/Comodo for at få et nyt certifikat).

Keystore-filen kan f.eks. hedde `www.ludus.skole.dk.keystore`, og er herfra kaldet <keystore>.

2. Notér private key-alias (til brug i punkt 4 af Comodos vejledning). Alias findes med følgende kommando:

```
keytool -list -keystore <keystore>
```

Der vil være en linie med teksten PrivateKeyEntry, i flg. format:

```
<alias>, <dato>, PrivateKeyEntry
```

Hvis der f.eks. står:

```
ludus, 05-03-2009, PrivateKeyEntry
```

så er alias = ludus.

Hvis man ikke har angivet et alias eksplicit da keystoren blev oprettet (i afsnit 2.2), så er alias = mykey.

3.2 Installation af selve certifikatet vha. Comodos vejledning

Nu kan Comodos vejledning følges. Anvend vejledningen med titlen "Certificate Installation: Java Based (Tomcat) Web Servers (using keytool)". Denne findes på flg. URL:

https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1204&nav=0,96,1,95.

Bemærkninger til Comodos vejledning:

- Vejledningen henviser til et alias *mykey* – her skal der indtastes det alias, der blev fundet under punkt 2 i sektion 3.1 Klargøring til installation.
- Rækkefølgen for installation af certifikatet-filer i guiden er:

1. AddTrustExternatCARoot.crt
2. UTNAddTrustServer_CA.crt
3. TERENASSLCA.crt
4. <nummer>.crt

- Efter installation af certifikaterne i rækkefølgen 1-3 bør keytool svare

```
Certificate was added to keystore.
```

Efter installation af det sidste certifikat (det med nummeret, som er jeres private certifikat), bør keytool svare

```
Certificate reply was installed in keystore.
```

I modsat fald er jeres certifikat *ikke* blevet installeret korrekt. I afsnit 3.2.1 er vist nogle typiske fejlbeskeder og andre problemer. Hvis dette ikke afhjælper problemet, kontakt da LUDUS Service på tlf. 36 14 70 70.

- I afsnit 4 er vist et eksempel på de kommandoer der skal udføres, samt de svar, keytool giver.
- Hvis keytool svarer "Certificate already exists in system-wide CA keystore under alias <alias>", så er det ikke en fejl. Der skal blot svares "yes" til spørgsmålet om hvorvidt man alligevel vil tilføje det til keystoren.

3.2.1 Typiske fejlbeskeder og andre problemer ved installation

Oftest forekommende fejlbeskeder fra keytool:

- Fejlbesked: "Keystore was tampered with or password was incorrect"

Betydning: Keystore password er forkert. Prøv igen med det korrekte password.

- Fejlbesked: "Public keys in reply and keystore don't match"

Betydning: Denne fejl kan opstå ved installation af det sidste certifikat (<nummer>.crt). Hvis fejlen opstår, så er der brugt en forkert keystore ved installationen. Der skal bruges samme keystore, som der blev brugt ved bestilling – dvs. den keystore der blev oprettet ved at følge Comodos vejledning i oprettelse af keystore og CSR-fil i afsnit 2.2 af denne vejledning.

Andre problemer:

Hvis keytool svarer "Certificate was added to keystore" til filen <nummer>.crt, så er det en fejl. Keytool **skal** svare "Certificate reply was installed in keystore". I modsat fald er certifikatet ikke parret korrekt med den private nøgle i keystore.

Denne fejl opstår typisk hvis der bruges en forkert keystore eller et forkert alias under installationen.

3.3 Installation af det nye certifikat i LUDUS Web

LUDUS Web skal nu benytte jeres nye certifikat.

1. Hvis keystore-filen med certifikatet ligger i biblioteket `keys` i LUDUS Web-installationen, så skal den kopieres hen til en anden mappe, evt. `C:\skole-certifikat`.

Advarsel: Hvis keystore-filen ligger i `keys`-biblioteket, så vil den efter kørsel af konfigurator.bat være tom (0 KB i størrelse), og dermed være ubrugelig! Dette vil endvidere medføre at LUDUS Web ikke kan starte korrekt op!

2. Start konfigurator.bat, der ligger i roden af jeres LUDUS Web-installation.
3. Tryk "Næste" to gange for at komme til certifikat-menuen.
4. Vælg at importere jeres nye keystore indeholdende certifikatet. Husk at vælge korrekt keystore-type (JKS eller PKCS12).
5. Indtast det korrekte password til keystoren.
6. Afslut konfiguratoren.
7. Genstart LUDUS Web-servicen.
8. Herefter burde det nye certifikat virke. Dette kan verificeres ved at åbne LUDUS Web i en Explorer-browser via https-protokollen, dvs. f.eks. <https://ludus.skole.dk>.

Kan denne åbnes uden fejlbeskeder, så virker jeres nye certifikat. Oplysninger om hvilket certifikat browseren modtager, kan ses ved at klikke på hængelåsen til højre for adresselinien i browseren.

9. Opstår der problemer, kontakt da LUDUS Service på tlf. 36 14 70 70.

