

Java Keystore import

Sajnos egy meglevő privát kulcsot és tanúsítványt nem lehet olyan könnyen (keytool segítségével) Java Keystore-ba importálni. A művelet folyamata a [Shibboleth Wikiben található leírás alapján](#):

- PKCS8 struktúra készítése, amely tartalmazza a privát kulcsot

```
openssl pkcs8 -topk8 -in be.aai.niif.hu.key -nocrypt -outform DER -out
be.aai.niif.hu.pkcs8
```

- El kell készíteni a tanúsítványhoz tartozó tanúsítvány láncot

```
cat ca-cert.pem be.aai.niif.hu.crt >cert-bundle.pem
```

- Létre kell hozni egy keystore-t. Ezt egy fake kulcs és tanúsítvány létrehozásával csináljuk.

```
/usr/java/latest/bin/keytool -genkey -keyalg RSA -alias "selfsigned" -keystore
myKeystore.jks -validity 360 -storepass "secret"
```

- Töröljük a fake kulcsot, marad az üres keystore

```
/usr/java/latest/bin/keytool -delete -alias "selfsigned" -keystore myKeystore.jks -
storepass "secret"
```

- A Shibboleth IdP **extkeytool** nevű eszközével betöltjük a pkcs8-ban levő kulcsot és a tanúsítványokat az üres keystore-ba. Ehhez persze be kell állítani az `IDP_HOME` változót.

```
export IDP_HOME=/usr/local/shibboleth-idp
/usr/local/shibboleth-idp/bin/extkeytool -importkey -keystore myKeystore.jks -alias
be -storepass secret \
-keyfile be.aai.niif.hu.pkcs8 -certfile cert-bundle.pem -provider
org.bouncycastle.jce.provider.BouncyCastleProvider
```

- Ha minden jól ment, akkor láthatjuk, hogy ott virít a kulcsunk a keystore-ban:

```
[~](bajnokk@dev)$ /usr/java/latest/bin/keytool -list -keystore myKeystore.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry
```

be, Aug 31, 2007, PrivateKeyEntry,

Certificate fingerprint (MD5): 2B:D6:14:00:44:D7:9C:B8:F9:DC:52:CD:3D:E1:3F:FB

Változat #1

document-uploader hozta létre 2025-08-07 12:11:04 CEST

document-uploader frissítette 2025-08-07 12:11:04 CEST