

Formati certifikata

Uvod

Certifikati se mogu spremati u više različitih formata. Najčešće korišteni su binarni format PKCS #12 (engl. *Personal Information Exchange Syntax Standard*) i tekstualni format PEM (engl. *Privacy Enhanced Mail*). Binarni format PKCS #12 koriste web i mail klijenti. Tekstualni format PEM koristi gotovo svi grid posrednički sustavi (npr. svi servisi Globus Toolkit).

Pretvorba iz PKCS #12 u PEM format

Korisnički certifikat

```
$ openssl pkcs12 -in user.p12 -out usercert.pem -nokeys -clcerts
Enter Import Password:
MAC verified OK
```

Privatni ključ korisničkog certifikata

```
$ openssl pkcs12 -in user.p12 -out userkey.pem -nocerts
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Poslužiteljski certifikat

```
$ openssl pkcs12 -in host.p12 -out hostcert.pem -nokeys -clcerts
Enter Import Password:
MAC verified OK
```

Privatni ključ poslužiteljskog certifikata

```
$ openssl pkcs12 -in host.p12 -out hostkey.pem -nocerts -nodes
Enter Import Password:
MAC verified OK
```

Pretvorba iz PEM u PKCS #12 format

```
$ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -certfile /etc/grid-security/certificates/ff94d436.
0 -out user.p12
Enter pass phrase for userkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
```