šifrování / certifikáty

generovani zadosti o serverovy certifkat

Viz take OpenSSL Command-Line HOWTO

Navod funguje pro generovani serveroveho certificate requestu pro Prvni certifikacni autoritu (ICA)

1) vygenerovat privatni klic (openssl vyzaduje heslo, takze prozatim s heslem)

```
openssl genrsa -des3 -out server.skey 1024
```

2) odstranit heslo z privatniho klice (apache by jinak po restartu cekal na heslo)

```
openssl rsa -in server.skey -out server.key
```

3) vygenerovat verejny klic

```
openssl genrsa -out server.key 1024
```

4) vygenerovat zadost

```
openssl req -new -key server.key -out server.csr
```

5) zkontrolovat parametry zadosti (vcetne kodovani znaku)

```
openssl req -noout -subject -nameopt show_type,sep_multiline -in serve
r.csr
```

! POZOR !
v defaultnim nastaveni vytvari openssl nektere polozky v kodovani, ktere ICA neprijima (TeletexString)
je treba PREDEM upravit konfiguracni soubor openssl, aby ukladal v kodovani UTF8String: /etc/ssl/openssl.cnf

```
#string_mask = nombstr
string_mask = utf8only
```

Unique solution ID: #1199
Author: Daniel
Last update: 2009-03-16 12:03