*XXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2005,** Beograd, 13. i 14. decembar 2005.*

KREIRANJE TESTNOG SERTIFIKACIONOG TELA ZA IZDAVANJE DIGITALNIH SERTIFIKATA

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"

Sadržaj: *U radu je objašnjeno kreiranje testnog sertifikacionog tela za izdavanje digitalnih sertifikata korišćenjem aplikacije OpenSSL, tj. kako korišćenjem navedene aplikacije može da se na jednostavan način kreira tajni ključ i sertifikat CA servera, a posle toga, tajni ključevi i sertifikati korisnika. Sertifikati kreirani na taj način mogu da se koriste isključivo za potrebe testiranja, a **ne** za komercijalnu upotrebu.*

Ključne reči: *Sertifikaciono telo - CA, digitalni sertifikati, aplikacija OpenSSL.*

1. Uvod

Digitalni (elektronski) sertifikat (digital certificate) je elektronski dokument koji izdaje sertifikaciono telo (Certification Authority - CA) [1]. Digitalni sertifikat može da se shvati kao digitalna lična karta, jer sadrži podatke o korisniku sertifikata i podatke o izdavaocu sertifikata. Konkretno, digitalni sertifikat sadrži:

1. podatke o identitetu korisnika kome je izdat sertifikat, kao što su ime i prezime, E-mail adresa,…
2. javni kriptografski ključ korisnika sertifikata,
3. podatke o entitetu koji je izdao sertifikat tj. o sertifikacionom telu.

U okviru digitalnog sertifikata koji se izda korisniku nalazi se pored ostalog i korisnikov javni kriptografski ključ (Public Key), koji je par njegovom tajnom kriptografskom ključu (Private Key). Sertifikaciono telo garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom istom sertifikatu. Zbog toga, ostali korisnici na Internetu ukoliko imaju poverenje u sertifikaciono telo, mogu da budu sigurni da određeni javni ključ zaista pripada korisniku koji je vlasnik pripadajućeg tajnog ključa.

Digitalni sertifikat je elektronski dokumenat koji je javno dostupan na Internetu. Zbog toga što se u okviru sertifikata nalaze javni ključevi korisnika sertifikata, distribucijom sertifikata se distribuiraju i javni ključevi. Iz tog razloga, omogućena je pouzdana razmena javnih ključeva posredstvom Interneta između korisnika koji se nikada nisu sreli, uz mogućnost verifikovanja identiteta korisnika.

Digitalni sertifikat je nemoguće falsifikovati jer je potpisan tajnim kriptografskim ključem (Private Key) sertifikacionog tela. Za verifikovanje valjanosti digitalnog sertifikata koristi se javni ključ tj. sertifikat sertifikacionog tela. Komunikacioni programi (na primer: Microsoft Internet Explorer) raspolažu sa digitalnim sertifikatima sertifikacionih tela kojima se veruje, pa samim tim i sa njihovim javnim ključevima. U okviru komunikacionih programa omogućeno je da korisnici naknadno instališu sertifikate sertifikacionih tela u koje imaju poverenje.

2. Preduslovi za kreiranje testnog sertifikacionog tela

Postoje dva (2) preduslova za kreiranje testnog sertifikacionog tela:

1. Instalisati aplikaciju OpenSSL, koju je moguće preuzeti sa OpenSSL Web strane (http://www.openssl.org) ili dobiti od autora rada (dspasic@ptt.yu). Aplikacija OpenSSL je alat koji omogućava da se unosom različitih komandi iz komandne linije izvršavaju različite kriptografske operacije [2, 3, 4]:

- kreiranje RSA, DH i DSA ključeva,
- kreiranje X.509 digitalnih sertifikata, zahteva za izdavanje sertifikata (Certificate Signing Request - CSR) i registara opozvanih sertifikata (Certificate Revocation List - CRL),
- izračunavanje *hash* vrednosti datoteka i sertifikata,
- šifrovanje/dešifrovanje i potpisivanje/verifikovanje potpisanih datoteka i elektronskih pisama,
- testiranje SSL/TLS klijent-server komunikacije, i drugo.

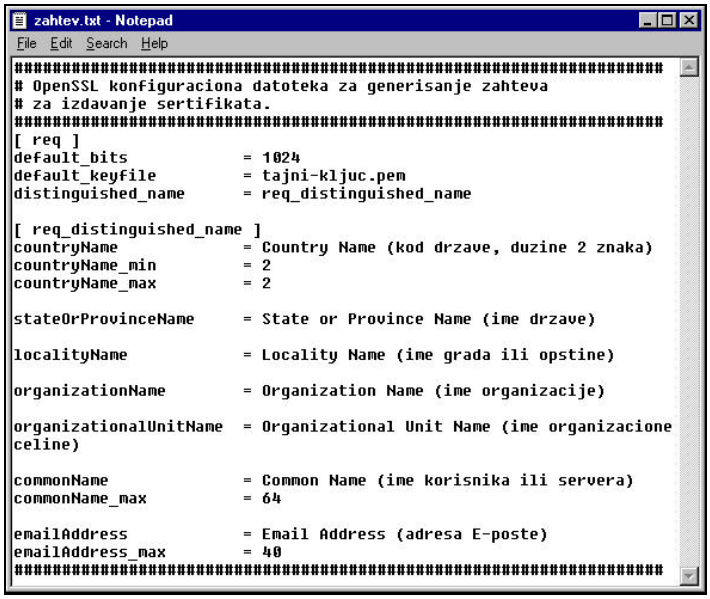
2. Kreirati OpenSSL konfiguracionu datoteku za generisanje PKCS#10 zahteva za izdavanje sertifikata **zahtev.txt** i iskopirati je u direktorijum u kome se nalazi OpenSSL izvršna datoteka **openssl.exe** (na primer: c:\Program Files\OpenSSL\bin). Sadržaj datoteke **zahtev.txt** koja je korišćena u ovom radu, je prikazan na slici 1. Opcije koje su navedene u datoteci **zahtev.txt** imaju sledeće značenje:

- default_bits, označava dužinu kriptografskog ključa u bitima. Dužina ključa može da bude: 512, 1024, 2048,... bita,
- default_keyfile, označava ime datoteke tajnog ključa,
- distinguished_name, označava sekciju u OpenSSL konfiguracionoj datoteci u kojoj se nalaze atributi koji čine jedinstveno ime korisnika ili servera (Distinguished Name - DN). Korišćeni su sledeći atributi (slika 1.): countryName (C), stateOrProvinceName (ST), localityName (L), organizationName (O), organizationalUnitName (OU), commonName (CN) i emailAddress (Email).

Korisne napomene u vezi atributa jedinstvenog imena korisnika ili servera su sledeće:

- U OpenSSL konfiguracionoj datoteci, umesto punih naziva atributa, mogu da se koriste njihovi skraćeni nazivi, koji su u prethodnom paragrafu iza punih naziva navedeni u zagradi.
- Moguće je da se koristi atribut domainComponent (DC), koji je karakterističan za Microsoft Active Directory (AD). U slučaju da se želi simuliranje da je direktorijum (repozitorijum) sertifikata Microsoft AD, tada u OpenSSL konfiguracionoj datoteci trebaju da postoje samo tri (3) atributa: DC, OU i CN.

- Moguće je višestruko korišćenje istog atributa, uz odgovarajuću numeraciju. Na primer, u slučaju višestrukog atributa OU, numeracija je sledeća: 1.organizationalUnitName, 2.organizationalUnitName, 3.organizationalUnitName,... ili 1.OU, 2.OU, 3.OU,...
- Za svaki atribut mogu da se koriste sledeće linije parametara atributa:
  - ImeAtributa=naziv atributa koji se prikazuje korisniku pre unosa vrednosti atributa,
  - ImeAtributa _default=*default*-na vrednost atributa,
  - ImeAtributa _min=X, gde je X minimalan broj znakova vrednosti atributa,
  - ImeAtributa _max=Y, gde je Y maksimalan broj znakova vrednosti atributa.



Slika 1. *OpenSSL konfiguraciona datoteka*

3. Kreiranje sertifikata za server sertifikacionog tela

Kreiranje sertifikata za CA server se izvršava u dva (2) koraka:

1. **Generisati kriptografske ključeve i zahtev za sertifikatom za CA server (izvršava CA administrator), što se radi sledećom komandom:**

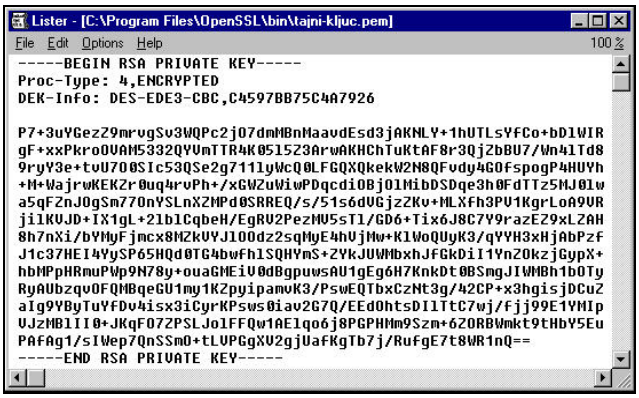
```
c:\Program Files\OpenSSL\bin>openssl req -config zahtev.txt -new -out ca-
root.csr
```

Vrednosti koje CA administrator posle toga treba da unese i primeri unetih vrednosti su:

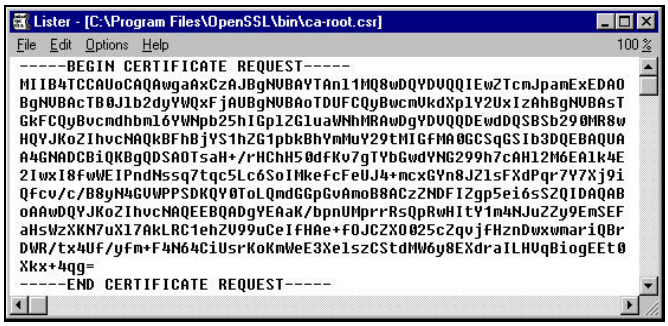
- Lozinka tajnog ključa CA servera (PEM pass phrase):**caca**
- Country Name (kod drzave, duzine 2 znaka) []:**yu**

- State or Province Name (ime drzave) []:**Srbija**
- Locality Name (ime grada ili opstine) []:**Beograd**
- Organization Name (ime organizacije) []:**ABC preduzece**
- Organizational Unit Name (ime organizacione celine) []:**ABC organizaciona jedinica**
- Common Name (ime korisnika ili servera) []:**CA Root**
- Email Address (adresa E-poste) []:**ca-admin@abc.com**

Kao izlaz se dobijaju dve (2) datoteke: **tajni-kljuc.pem** (slika 2.) i **ca-root.csr** (slika 3.). Posle toga, potrebno je reimenovati datoteku **tajni-kljuc.pem** u **ca-tajni-kljuc.pem**.



Slika 2. *Tajni (privatni) ključ CA servera*

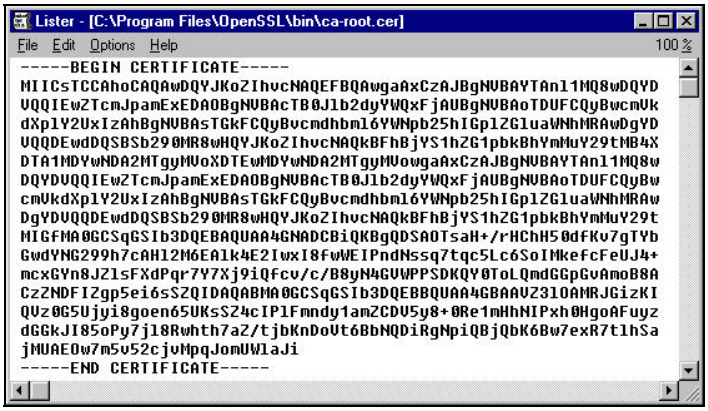


Slika 3. *Zahtev za sertifikatom za CA server*

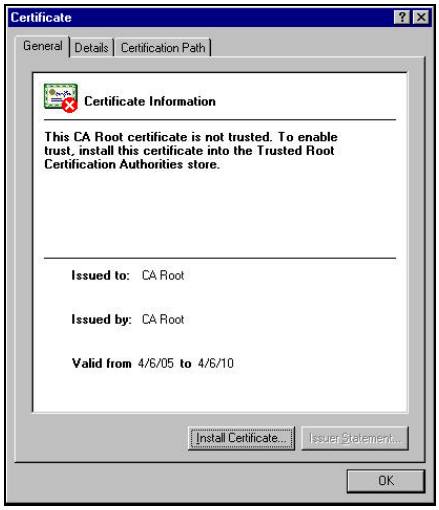
2. Kreirati samopotpisani sertifikat za CA server (izvršava CA administrator), što se radi sledećom komandom:

```
c:\Program Files\OpenSSL\bin>openssl x509 -in ca-root.csr -out ca-root.cer
-req -signkey ca-tajni-kljuc.pem -days 1826 -sha1
```

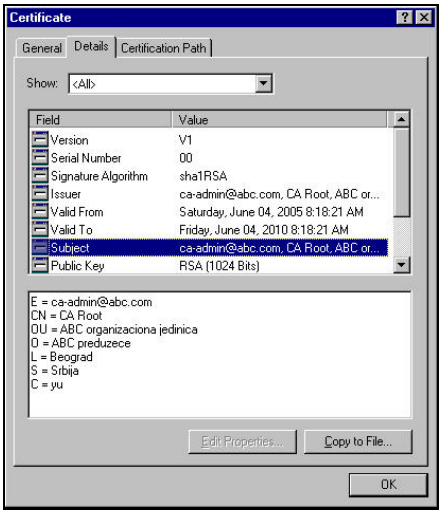
Posle navedene komande, CA administrator mora da unese lozinku tajnog ključa CA servera (PEM pass phrase), koja je u navedenom primeru **caca**. Kao izlaz se dobija datoteka sertifikata CA servera **ca-root.cer** (slika 4., 5. i 6.).



Slika 4. *Sertifikat CA servera, PEM (Base 64) format*



Slika 5. *Sertifikat CA servera, kartica General, MS Internet Explorer prikaz*



Slika 6. *Sertifikat CA servera, kartica Details, MS Internet Explorer prikaz*

S obzirom na to da korisnici autentičnost sertifikata CA servera mogu da utvrde samo na osnovu *hash* vrednosti sertifikata CA servera, sertifikaciono telo je dužno da javno objavi SHA1 (Secure Hash Algorithm 1) i MD5 (Message Digest 5) *hash* vrednost CA sertifikata. Pre izračunavanja *hash* vrednosti, potrebno je sertifikat CA servera **ca-**

root.cer iz PEM (Base 64) formata konvertovati u DER binarni format **ca-root.der**, što se radi sledećom komandom:

```
C:\Program Files\OpenSSL\bin>openssl x509 -in ca-root.cer -outform der -out
ca-root.der
```

Za izračunavanje SHA1 i MD5 *hash* vrednosti koriste se sledeće komande:

```
C:\Program Files\OpenSSL\bin>openssl sha1 -c ca-root.der
SHA1(ca-root.der)=
c7:cb:29:bd:98:af:fc:2a:3b:58:28:b0:3d:19:e7:5a:19:39:f7:5d

C:\Program Files\OpenSSL\bin>openssl md5 -c ca-root.der
MD5(ca-root.der)= 8c:78:e5:bd:62:9e:35:95:37:9b:4a:94:7a:a9:41:83
```

SHA1 algoritam daje 160-bitnu *hash* vrednost, koja se zapisuje sa 40 heksadecimalna znaka, dok MD5 algoritam daje 128-bitnu *hash* vrednost, koja se zapisuje sa 32 heksadecimalna znaka.

4. Kreiranje sertifikata za korisnika

Kreiranje sertifikata za korisnika se izvršava u tri (3) koraka:

1. **Generisati kriptografske ključeve i zahtev za sertifikatom za korisnika (izvršava korisnik), što se radi sledećom komandom:**

```
c:\Program Files\OpenSSL\bin>openssl req -config zahtev.txt -new -out pera-
peric.csr
```

Vrednosti koje korisnik posle toga treba da unese i primeri unetih vrednosti su:

- Lozinka tajnog ključa korisnika (PEM pass phrase):**pera**
- Country Name (kod drzave, duzine 2 znaka) []:**yu**
- State or Province Name (ime drzave) []:**Srbija**
- Locality Name (ime grada ili opstine) []:**Beograd**
- Organization Name (ime organizacije) []:**Perino preduzece**
- Organizational Unit Name (ime organizacione celine) []:**Perino podpreduzece**
- Common Name (ime korisnika ili servera) []:**Pera Peric**
- Email Address (adresa E-poste) []:**pperic@yahoo.com**

Kao izlaz se dobijaju dve (2) datoteke: **tajni-kljuc.pem** i **pera-peric.csr**. Posle toga, potrebno je reimenovati datoteku **tajni-kljuc.pem** u **pp-tajni-kljuc.pem**.

2. **Kreirati sertifikat za korisnika koji će da potpiše CA server (izvršava CA administrator), što se radi sledećom komandom:**

```
C:\Program Files\OpenSSL\bin>openssl x509 -in pera-peric.csr -out pera-
peric.cer -req -CA ca-root.cer -CAkey ca-tajni-kljuc.pem -days 365 -sha1 -
CAcreateserial
```

Posle navedene komande, CA administrator mora da unese lozinku tajnog ključa CA servera (PEM pass phrase), koja je u navedenom primeru **caca**. Kao izlaz se dobija

datoteka sertifikata korisnika **pera-peric.cer** i datoteka **ca-root.srl** koja sadrži serijski broj sertifikata koji će da bude upisan u sledeći kreiran sertifikat korisnika.

U navedenom primeru, kreirani sertifikat korisnika je X.509 verzije 1, što znači da **ne** sadrži ekstenzije. Da bi se kreirao sertifikat X.509 verzije 3, koji sadrži željene ekstenzije, neophodno je kreirati konfiguracionu datoteku koja sadrži željene ekstenzije (na primer: keyUsage=Digital Signature, Key Encipherment) i navedenoj komandi **openssl x509**, posle navedenih opcija, dodati opciju **-extfile filename**.

3. Kreirati PKCS#12 datoteku korisnika od sertifikata i tajnog ključa korisnika i sertifikata CA servera (izvršava korisnik), što se radi sledećom komandom:

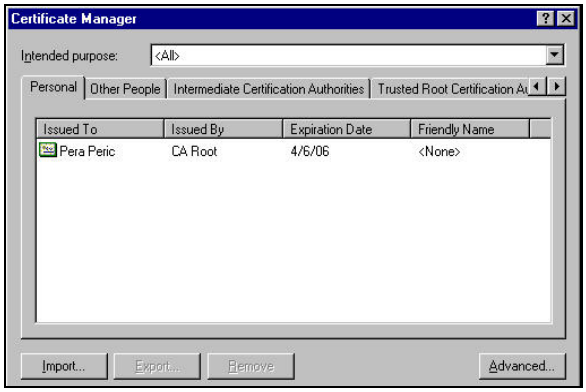
```
C:\Program Files\OpenSSL\bin>openssl pkcs12 -export -in pera-peric.cer -
inkey pp-tajni-kljuc.pem -certfile ca-root.cer -out pera-peric.p12
```

Posle navedene komande, korisnik mora da unese lozinku svog tajnog ključa (PEM pass phrase), koja je u navedenom primeru **pera**, i mora da kreira lozinku PKCS#12 datoteke (Export Password), tako što će dva puta da je unese (na primer: **1234**). Kao izlaz se dobija PKCS#12 datoteka korisnika **pera-peric.p12**.

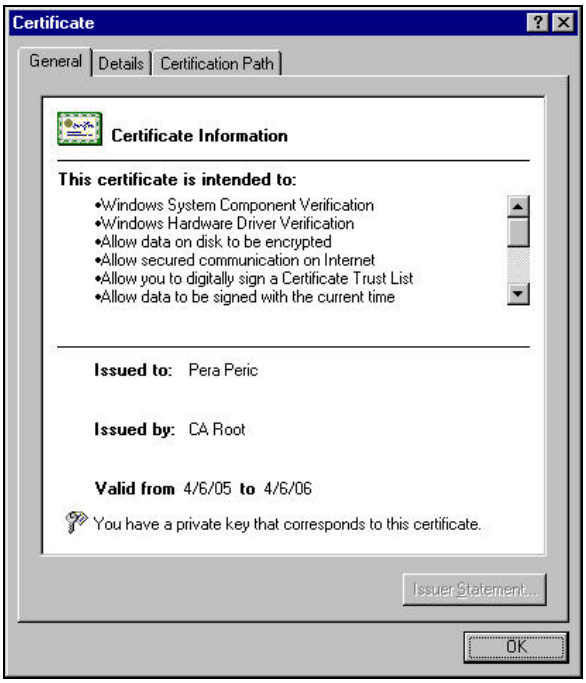
Iz izloženog, najvažnije je primetiti da tajni ključevi moraju da budu u isključivom posedu vlasnika, tj. tajni ključevi ne smeju da se razmenjuje, dok je razmena sertifikata (javnih ključeva) dozvoljena, kako između sertifikacionog tela i korisnika, tako i između korisnika.

5. Prikaz sertifikata korisnika i zahteva za sertifikatom

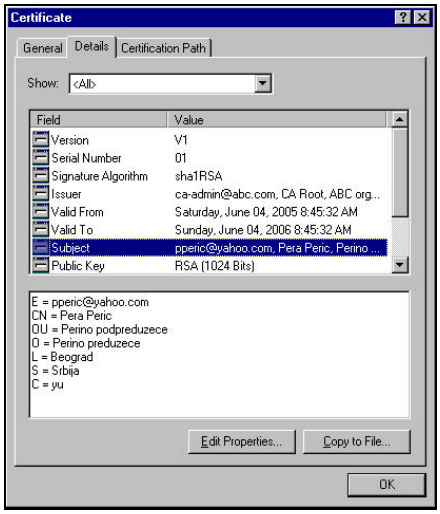
Posle instalisanja (importovanja) PKCS#12 datoteke korisnika u MS Internet Expolerer, moguće je pristupiti sertifikatu, na sledeći način: u Internet Explorer-u sa menija *Tools* izabrati opciju *Internet Options...*, na formi *Internet Options* izabrati karticu *Content*, pritisnuti dugme *Certificates...*, posle čega se pojavljuje forma *Certificates* (*Certificate Manager*) sa izabranom karticom *Personal* (slika 7.), na kojoj su prikazani instalisani sertifikati korisnika sa pridruženim tajnim ključevima. Dvostrukim pritiskom na željeni sertifikat, on će se prikazati (slika 8., 9. i 10.).



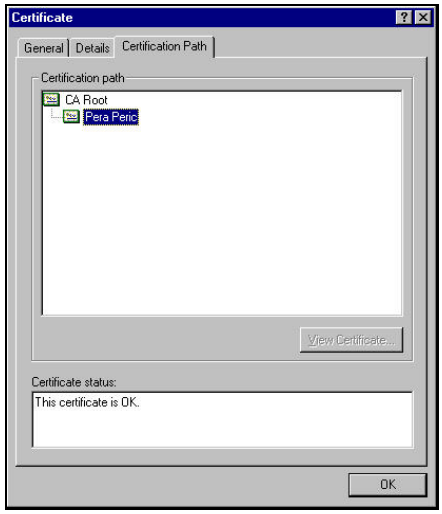
Slika 7. *Skladište sertifikata MS Internet Explorer-a*



Slika 8. *Sertifikat korisnika, kartica General, MS Internet Explorer prikaz*



Slika 9. *Sertifikat korisnika, kartica Details, MS Internet Explorer prikaz*



Slika 10. *Sertifikat korisnika, kartica Cert. Path, MS Internet Explorer prikaz*

Prikaz zahteva za sertifikatom, sertifikata i PKCS#12 datoteke u tekstualnoj formi, korišćenjem aplikacije OpenSSL, izvršava se sledećim komandama:

1. Prikaz zahteva za sertifikatom:

```
C:\Program Files\OpenSSL\bin>openssl req -text -in pera-peric.csr
```

2. Prikaz sertifikata:

```
C:\Program Files\OpenSSL\bin>openssl x509 -text -in pera-peric.cer
```

3. Prikaz PKCS#12 datoteke korisnika:

```
C:\Program Files\OpenSSL\bin>openssl pkcs12 -info -in pera-peric.p12
```

Posle navedene komande, korisnik mora da unese lozinku PKCS#12 datoteke (Import Password), koja je u navedenom primeru **1234**, i mora dva puta da unese lozinku svog tajnog ključa (PEM pass phrase), koja je u navedenom primeru **pera**.

6. Zaključak

Sertifikaciono telo mora da sprovede proceduru (ceremoniju) generisanja tajnog i javnog kriptografskog ključa i X.509 digitalnog sertifikata CA servera, pre nego što počne izdavanje X.509 digitalnih sertifikata korisnicima. Procedura izdavanja sertifikata korisnicima izvršava se na sledeći način:

1. Korisnik na svom računaru generiše tajni i javni kriptografski ključ, a na osnovu javnog ključa generiše PKCS#10 zahtev za sertifikatom (Certificate Signing Request - CSR) koji digitalno potpiše svojim tajnim ključem.
2. Korisnik pošalje PKCS#10 zahtev za sertifikatom prema sertifikacionom telu.
3. Sertifikaciono telo na osnovu korisnikovog PKCS#10 zahteva za sertifikatom kreira X.509 digitalni sertifikat, koji sadrži podatke o korisniku, korisnikov javni ključ i podatke o sertifikacionom telu. Pri tome, sertifikaciono telo digitalno potpiše sertifikat korisnika svojim tajnim ključem.
4. Sertifikaciono telo pošalje X.509 digitalni sertifikat prema korisniku.
5. Korisnik primljeni X.509 digitalni sertifikat pridruži svom tajnom ključu.

Literatura

[1] Web strana Sertifikacionog tela Pošte: http://www.cepp.co.yu/ca.

[2] OpenSSL Web strana: http://www.openssl.org.

[3] The Apache + SSL on Win32 HOWTO: http://tud.at/programm/apache-ssl-win32-howto.php3.

[4] Preuzimanje i instalisanje sertifikata za Web server Apache, Korisničko uputstvo, Sertifikaciono telo Pošte, 2005. (http://www.cepp.co.yu/ca/dokumentacija).

Abstract: *This paper describes creating a test Certification Authority for issuing digital certificates, using OpenSSL command line tool. These digital certificates can be used only for testing,* ***not*** *for commercial purpose.*

Keywords: *Certification Authority - CA, digital certificates, OpenSSL application.*

CREATING A TEST CERTIFICATION AUTHORITY FOR ISSUING DIGITAL CERTIFICATES

Dragan Spasić