

Uputstvo za dobijanje MREN sertifikata

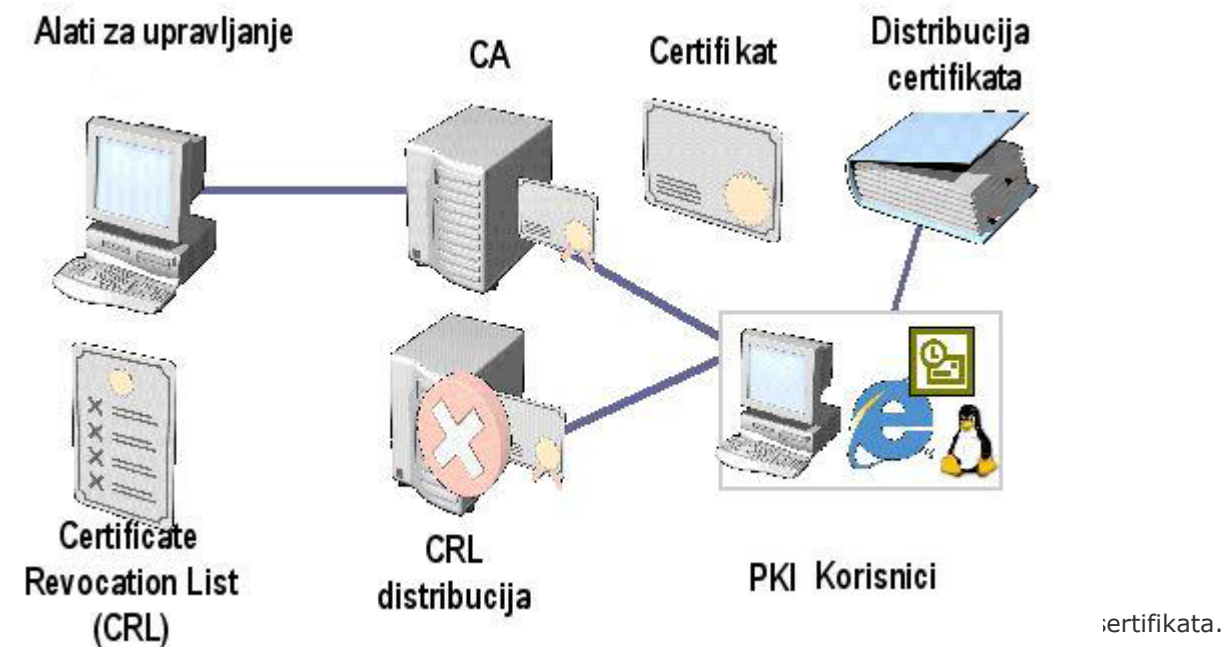
Šta je digitalni sertifikat?

Šta je PKI?

PKI (*Public Key Infrastructure*), poznat i kao X.509, je sistem koji se temelji na strogoj hijerarhijskoj organizaciji izdavanja korisničkih sertifikata. PKI sistem čini kombinacija tehnologije enkripcije i servisa koji omogućavaju sigurnu međusobnu komunikaciju i elektronske transakcije.

PKI se sastoji od više međusobno povezanih objekata, aplikacija, servisa, alata za upravljanje i nadgledanje:

- CA (*Certification Authority*) koji se brine za izdavanje i valjanost sertifikata
- distribucije izdanih sertifikata
- distribucije CRL liste (*Certification Revocation List*)
- korisničkog sertifikata
- korisničkih aplikacija, servera itd., koji koriste PKI autorizaciju.



Kriptografija kao sastavni dio PKI-a

Digitalni sertifikati omogućavaju sigurnost elektronskih komunikacija, analogno slanju pisma u kojem se potpisom ovjerava sadržaj i autorstvo pisma, a zatvorenom kovertom garantuje i sigurnost i privatnost sadržaja pisma. Pravno gledano, digitalni potpis ima istu važnost kao i svojeručni potpis.

U PKI sistemu povjerljivost podataka se osigurava enkripcijom poruka odnosno korišćenjem tajnog (*private key*) i javnog (*public key*) ključa u asocijaciji s kompleksnim matematičkim algoritmom (tzv. asimetrična enkripcija).

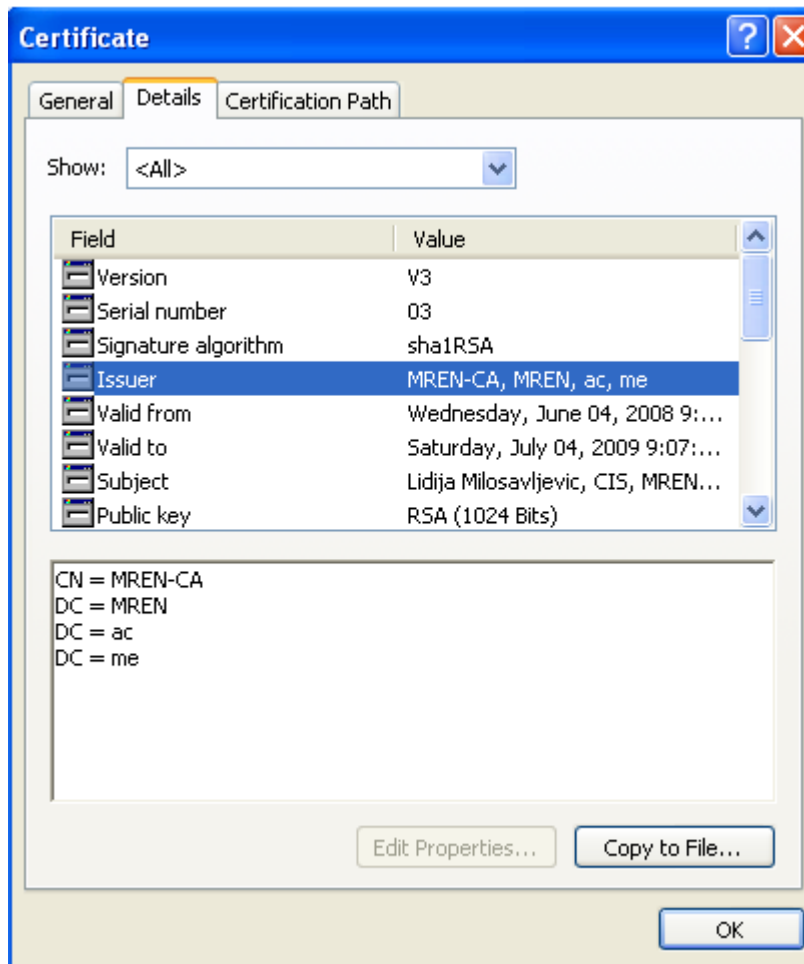
Svaka osoba u PKI sistemu ima vlastiti javni i tajni ključ, nadopunjen sertifikatom. Osnovni princip je sigurno čuvanje tajnog ključa koji mora biti dostupan i poznat samo korisniku. Korisnički certifikat, u kojem se nalazi javni ključ, je dostupan svima. Korištenjem kombinacije tajnog i javnog ključa prilikom slanja poruke, sadržaj poruke se kriptuje čime poruka postaje nečitljiva. Primjenom pripadajućeg tajnog ključa, koji svaka osoba u PKI sistemu čuva za sebe, poruka se dekriptuje i nanovo postaje čitljiva.

Tajni ključ se koristi i kod digitalnog potpisivanja poruka pa primalac pomoću pošiljaočevog javnog ključa može provjeriti je li sadržaj poruke prilikom dostave mijenjan, odnosno je li dobio originalni HASH zapis.

Sertifikat ili digitalni potpis (*digital ID*) je dodatak koji se dodaje digitalnom dokumentu i služi kao autentifikacija osobe ili računara (servera ili servisa) koje koriste neku uslugu, aplikaciju ili komunicira s drugim korisnicima putem Interneta ili drugačije. Sam certifikat u sebi sadrži korisnički javni ključ koji, korištenjem HASH algoritma, mora biti potpisan, odnosno odobren od organizacije koja garantuje da je certifikat izdat po pravilima.

Ispravnost certifikata se garantuje certifikatom višeg nivoa hijerarhije, tzv. *root certifikatom* odnosno certifikatom potpisanim od nekog podređenog *CA (Certification Authority)* operatera koji je potpisan od *root CA (Certification Authority)*. MREN CA ne dodjeljuje podređene CA.

Na slici je prikazan certifikacijski put korisničkog digitalnog potpisa potpisanog od MREN-CA. U digitalnom potpisu se nalazi certifikat organizacije koja je izradila i potpisala, odnosno potvrdila korisnički certifikat.



Korisničkim certifikatom se definiše nekoliko elemenata:

- vrijeme trajanja («vjerovanja») certifikata
- ekstenzije korisničkog certifikata kojima se definišu usluge za koje korisnik može koristiti svoj certifikat
- link na listu na kojoj se provjerava je li certifikat izgubio na valjanosti
- polje u kojem je zapisan korisnikov javni ključ

Udruživanje certifikata sa standardnim aplikacijama

Nakon izdavanja certifikata, uz standardne kriptografske funkcije, postoje i različite upotrebe u aplikacijama za autorizacijske i autentifikacijske potrebe kao što su na primjer: S/MIME (*Secure Multi-purpose Internet Mail Extensions*), web autentifikacija, prijava na računar, login na Win domenu, login za ostvarivanje VPN konekcije.

Digitalni certifikat možete koristiti uglavnom iz istih razloga iz kojih biste potpisali dokument na papiru. Digitalni potpis se koristi za **provjeru identiteta** digitalnih informacija pomoću računarskog šifrovanja. Digitalni certifikati utvrđuju slijedeće garancije:

- **Autentičnost** Digitalni sertifikat garantuje da je potpisnik vjerodostojan.
- **Integritet** Digitalni sertifikat garantuje da sadržaj nije promijenjen ili neovlašćeno izmijenjen nakon što je digitalno potpisan.
- **Nemogućnost poricanja (non repudation)** Digitalni sertifikat pomaže u dokazivanju porijekla potpisanog sadržaja svim stranama. „Poricanje“ se odnosi na čin odbacivanja bilo kakve veze sa potpisanim sadržajem od strane potpisnika.

Kako digitalni potpis funkcioniše?

Kod digitalnog potpisivanja e-mail-a, digitalni sertifikat (sadrži javni ključ i informacije o pošiljaocu) se dodaje poruci. Primalac može koristiti vaš digitalni potpis za verifikovanje identiteta, i vaš javni ključ za slanje kriptovanog maila koji samo vi možete dekriptovati. Da bi se mogla poslati kriptovana poruka , Address Book pošiljaoca mora sadržati digitalni sertifikat primaoca. Na taj način se koriste javni ključevi za kriptovanje poruka. Kada primalac dobije kriptovanu poruku, dekriptovanje se vrši pomoći njegovog privatnog ključa.

Riječnik pojmova:

Certification Authority (CA). CA je punomoćje dodijeljeno od jedne ili više organizacija za izdavanje, korišćenje i administriranje sertifikata (MREN-CA je opunomoćen od strane [EUGridPMA](#) koja je član [IGTF-a](#)). CA je rješenje za nadziranje bezbjednosti rada na internetu. CA omogućava da se pri upravljanju elektronskim transakcijama omogući povjerljivost, integritet podataka, autentifikacija korisnika, i zaštita od poricanja (non-repudiation)

Non-repudiation. Ne-poricanje je garancija da pošiljalac ima dokaz o prijemu, i da primalac ima dokaz o pošiljaočevom identitetu, tako da niko kasnije ne može poricati svoje učešće u procesiranju posdataka).

[Certificate Policy/ Certificate Practices Statement \(CP/ CPS\).](#) CP je pravilnik o radu sa sertifikatima. CP određuje sve aspekte vezane za generisanje, obradu, distribuiranje, oporavak, i administriranje digitalnih sertifikata. Indirektno, CP takođe može kontrolisati transakcije vođene komunikacionim sistemima koji imaju sistem zaštite baziran na sertifikatima. Kontrolisanjem ekstenzija sertifikata, CP i odgovarajuća tehnologija mogu podržati zahtjeve sigurnosti servera i servisa potrebnih za određene aplikacije.

CPS je interna izjava o praksi koju CA služba primjenjuje. CPS je detaljan i sveobuhvatan tehnički i proceduralni document kojim su objašnjene procedure koje se trebaju ispoštovati pri izdavanju sertifikata.

[Certificate Revocation List \(CRL\).](#) CRL je spisak nevažećih sertifikata i objavljuje se najkasnije nakon svaka 23 dana. Sertifikat može biti opozvan ako se posumnja da su informacije koje on sadrži nevažeće, ako je neovlašćeno korišten, ili ovlašćeni korisniku više nije potreban. Ovo uključuje sljedeće situacije :

- CA je informisan da ovlašćeni korisnik nije dao tačne informacije o svom učešću u aktivnostima MRENa.
- Private key (privatni ključ) je izgubljen, ili se sumnja da je dostupan nekom drugom.
- Informacije u sertifikatu su pogrešne ili netačne, ili se sumnja da su pogrešne ili netačne.
- Ovlašćeni korisnik je prekršio svoje obaveze.
- Ovlašćeni korisnik nje koristi sertifikat u skladu sa zakonom Crne Gore.
- Ovlašćeni korisniku više ne treba sertifikat .

[Digital Certificate.](#) Digitalni sertifikat je digitalni prikaz informacija koji:

- Identifikuje CA koji je izdao sertifikat.

- Identifikuje ime, tj identitet ovlašćenog korisnika.
- Sadrži ovlašćeni korisnikov public key (javni ključ).
- Identifikuje operativni period (period važenja sertifikata).
- Digitalno je potpisan od strane CA-a koji je izdao sertifikat..

Digitalni sertifikat je struktura podataka koja se koristi u public key (javni ključ) sistemu da omogućí individualnu autorizaciju za određeni public key (javni ključ). Može biti validan, expired (istekao), ili revoked (opozvan). U [pravnom smislu](#) digitalni sertifikat potpisan od strane opunomoćenog CA ima istu važnost kao svojeručni potpis.

[Ovdje](#) se mogu provjeriti svi sertifikati koje je izdao MREN-CA.

E-mail Certificate. E-mail sertifikat je sertifikat koji se koristi za kreiranje enkriptovanog e-maila.

Encryption Kriptovanje je matematički proces transformacije teksta u manje čitljivu formu. Manje čitljiva forma je informacija enkriptovana u naizgled besmislen kod, koji može biti pročitan samo od strane onog ko ima ključ za njegovo dekriptovanje.

Passphrase. To je fraza koju je ovlašćeni korisnik odredio, koristi se prilikom konektovanja na URL. Passfrazе se koristi umjesto passworda. Sastoji se od jedne riječi, ili više riječi bez praznih prostora između njih. Ne preporučuju se standardne riječi dostupne u riječnicima, niti riječi bazirane na imenima. Mora biti alfanumerička i sadržati i mala i velika slova.

Private Key. Privatni ključ je:

- jedan od para ključeva, koristi se za kreiranje digitalnog potpisa, ili
- jedan od para ključeva, koristi se za dešifrovanje (dekriptovanje) povjerljivih podataka.

U oba sličaja ovaj ključ **mora** biti čuvan u tajnosti.

Public key. Javni ključ je:

- jedan od para ključeva, koristi se pri provjeri validnost digitalnog potpisa, ili
- jedan od para ključeva, koristi se pri šifrovanju (enkriptovanju) povjerljivih informacija.

U oba slučaja ovaj ključ je javno dostupan.

Public Key Infrastructure (PKI). PKI je skup pravilnika, procesa, servera, softvera, radnih stanica korištenih u administriranju sertifikata i public-private key parova, uključenih u izdavanje, održavanje, i opozivanje public key (javni ključ) sertifikata.

Registration Authority (RA). RA je odgovoran za provjeru identiteta korisnika, prije izdavanja sertifikata, ali ne potpisuje i ne dodjeljuje sertifikate.

Relying Party. RP je pouzdano pravno ili fizičko lice koje posjeduje informacije koje uključuju sertifikat i digitalni potpis koji može biti verifikovan na osnovu public key-a (javnog ključa) sadržanog u sertifikatu. RP se oslanja na validnost obavezivanja ovlašćenih korisnika. U skladu sa CP/CPS-om RP moraju najmanje jednom dnevno downloadovati CRL i provjeravati validnost sertifikata na osnovu odgovarajućih informacija o statusu sertifikata. RP može koristiti sertifikat da verifikuje integritet digitalno potpisane poruke identifikujući kreatora poruke, ili da omogućí povjerljivu komunikaciju sa ovlašćenim korisnikom sertifikata.

Subscriber. Ovlašćeni korisnik je

- subjekt imenovan i identifikovan u sertifikatu ;
- posjeduje private key (privatni ključ) koji odgovara public key-u (javnom ključu) sadržanom u sertifikatu ;
- ne izdaje sertifikate drugim stranama.

Ime ovlašćenog korisnika pojavljuje se kao "subject" u sertifikatu, u skladu sa CP/CPS-om po kome je izdat sertifikat.

MREN CA izdaje user, host, i servis certificate. Oni koji mogu postati ovlašćeni korisnici MREN sertifikata su:

- Korisnici i administratiri MREN-a ;
- Kompjuteri koji se koriste u aktivnostima MREN-a ;
- Servisi, ili aplikacije koji se izvršavaju na kompjuterima MREN-a.

Postoje dva načinja izdavanja sertifikata

1. Potpisivanjem pkcs#10 zahtjeva koji je subjekt generisao ;
2. Direktno izdavanje bez pkcs#10 zahtjeva.

Prvi način je uobičajeniji, naročito u slučaju server/servis sertifikata.

Distinguished name (DN):

Jedinstveno ime mora biti sljedećeg formata DC=me, DC=ac, DC=MREN, O=XXX, CN=Subject-name. XXX je skraćenica za organizaciju. Spisak skraćenica za O nalazi se u sljedećoj tabeli.

Kod user sertifikata CN je ime i prezime. Kod server sertifikata CN je DNS FQDN, a kod servis sertifikata CN sačinjavaju ime servisa i DNS FQDN odvojeni znakom "/". U cilju izbjegavanja istog CN-a za različite entitete, uglavnom kod personalnih sertifikata, dozvoljeno je dodavanje ekstra karaktera. Ime svakog entiteta mora biti jedinstveno. Karakteri koji su dozvoljeni su: mala i velika slova engleskog alfabeta, cifre od 0-9 isimboli '(,)', '+', ',', '-', '.', ':', '?', ''.

Elektrotehnički fakultet	ETF
Mašinski fakultet	MF
Metalurško-tehnološki fakultet	MTF
Prirodno-matematički fakultet	PMF
Građevinski fakultet	GF
Arhitektonski fakultet	AF
Ekonomski fakultet	EF
Pravni fakultet	PF
Fakultet političkih nauka	FPN
Medicinski fakultet	MDF

Filozofski fakultet	FF
Fakultet za pomorstvo	FZP
Fakultet za turizam i hotelijerstvo	FTH
Muzička akademija	MA
Fakultet dramskih umjetnosti	FDU
Fakultet likovnih umjetnosti	FLU
Fakultet primjenjene fizioterapije	FPF
Institut za strane jezike	ISJ
Biotehnički institut	BTI
Institut za biologiju mora	IBM
Istorijski institut	II
Centar informacionog sistema	CIS
Univerzitetska Biblioteka	UB
Farmacija	F
Geodezija	G
Ministarstvo prosvjete i nauke	MPIN

Kako postati ovlašćeni korisnik digitalnog sertifikata?

Najprije pročitajte [Certificate Policy/ Certificate Practices Statement \(CP/ CPS\)](#) .
Prije dobijanja sertifikata korisnik mora proći sljedeći postupak :

1) Provjera identiteta :

- User sertifikati : subjekt mora lično kontaktirati RA ili CA u cilju dokazivanja svog identiteta i obezbijediti kopiju svog identifikacionog dokumenta (lična karta, pasoš ili vozačka dozvola).
- Server i servis sertifikati: zahtjev mora uputiti administrator odgovoran za odgovarajući host. Moraju biti zadovoljeni sljedeći uslovi: host mora imati validno DNS ime, administrator mora posjedovati validan user sertifikat izdat od strane MREN CA, administrator mora obezbijediti dokaz o svojoj povezanosti sa hostom, kao i povezanosti sa organizacijom koja je članica MRENa.

2) Generisanje zahtjeva :

Za generisanje zahtjeva za sertifikat potrebno je imati validan nalog na nekom od MREN nodova, a takođe je moguće koristiti OPENSSL za Windows platforme.

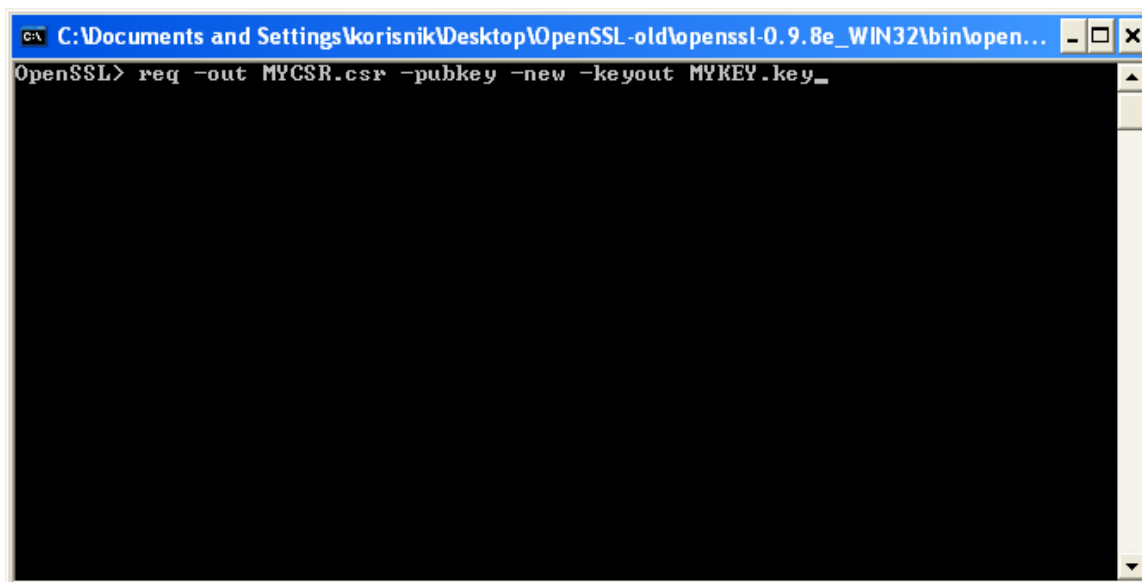
Postoje 2 načina generisanja sertifikata : potpisivanjem unaprijed generisanog pks#10 zahtjeva (što je najbolje, naročito za server sertifikate), ili izdavanje sertifikata direktno bez pks#10 zahtjeva. Prva varijanta je poželjna, I ona se sastoji iz sljedećih koraja:

- Instalirati OpenSSL za Windows (u slučaju da korisnik nema validan nalog na nekom od MREN nodova)
- U folder ... C:\... \OpenSSL\bin presnimiti fajl openssl.cfg (ovaj fajl će korisnik dobiti mailom u vidu attachmenta)
- Iz foldera C:\... \OpenSSL\bin pokrenuti OpenSSL.exe (dvostruki klik lijevim tasterom, ili klik desnim tasterom pa „Open“). Dobićete sljedeći izgled ekrana:



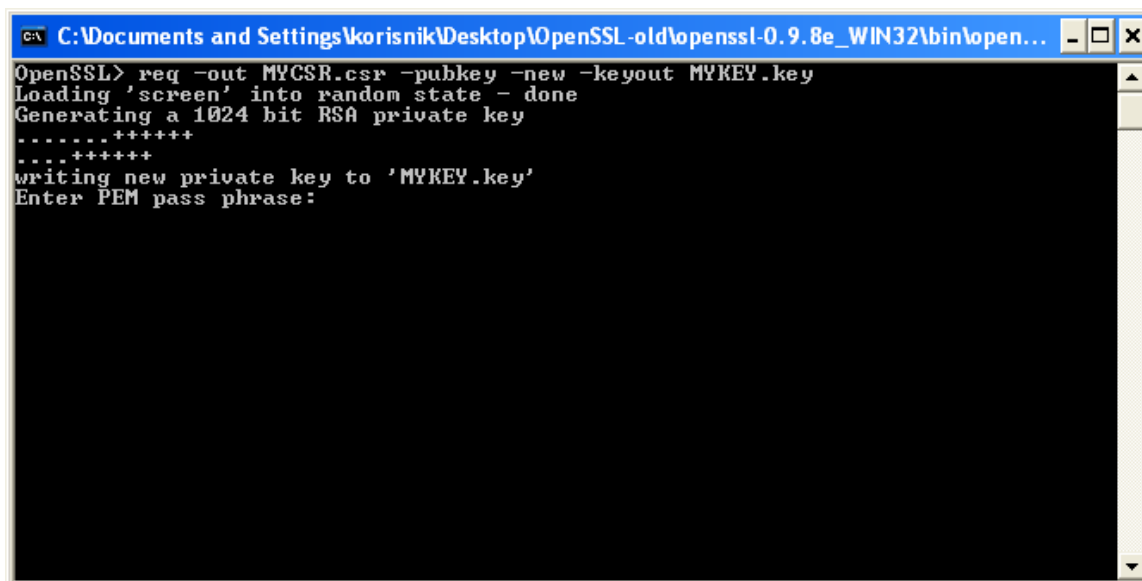
Za generisanje zahtjeva za sertifikat (MYCSR.csr) i odgovarajućeg privatnog ključa (MYKEY.key) unesite sljedeću liniju koda:

```
req -out MYCSR.csr -pubkey -new -keyout MYKEY.key
```

```
C:\Documents and Settings\korisnik\Desktop\OpenSSL-old\openssl-0.9.8e_WIN32\bin\open... - _ □ X
OpenSSL> req -out MYCSR.csr -pubkey -new -keyout MYKEY.key_
```

Biće zatraženo da unesete password za private key:



```
C:\Documents and Settings\korisnik\Desktop\OpenSSL-old\openssl-0.9.8e_WIN32\bin\open... - _ □ X
OpenSSL> req -out MYCSR.csr -pubkey -new -keyout MYKEY.key
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'MYKEY.key'
Enter PEM pass phrase:
```

Zatim trebate unijeti odgovarajuće Jedinствeno Ime za sertifikat (Distinguished Name), Biće vam zatražena jedna po jedna komponenta (podrazumijevane vrijednosti su date u uglastoj zagradi), npr:

domainComponent=me

domainComponent=ac

domainComponent=MREN

O=CIS

CN=Marko Markovic (tj. ime i prezime, a u slučaju servera DNS)

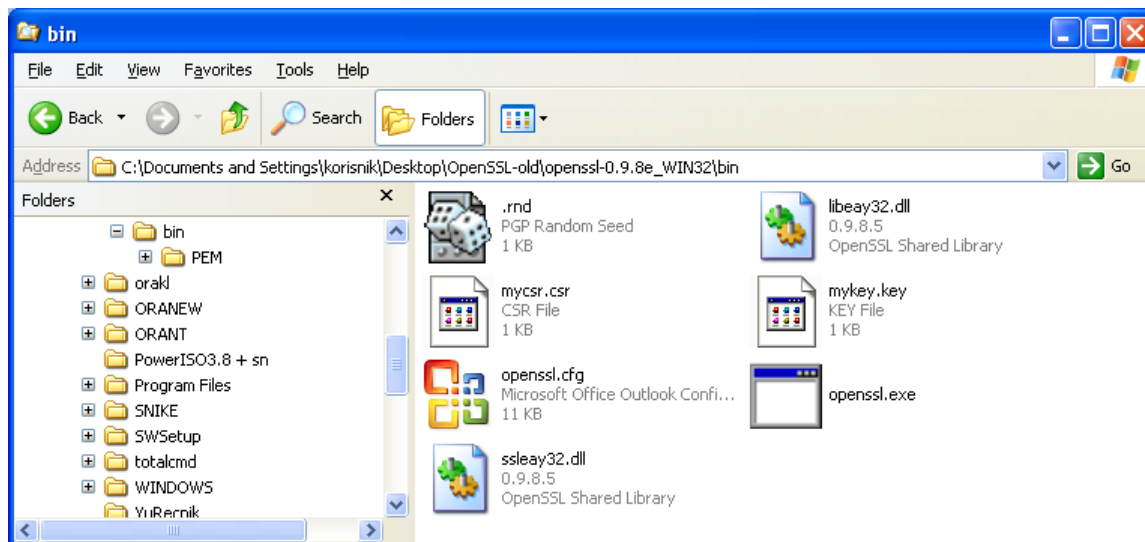
Morate voditi računa o upotrebi malih i velikih slova. Lokalni karakteri (tipa'ć' , 'š' i sl.) nisu dozvoljeni.

Ovi podatke će korisnik takođe dobiti mailom (zajedno sa prethodno pomenutim attachmentom).

```
C:\Documents and Settings\korisnik\Desktop\OpenSSL-old\openssl-0.9.8e_WIN32\bin\open...
OpenSSL> req -out MYCSR.csr -pubkey -new -keyout MYKEY.key
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'MYKEY.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
DomainComponent<me> [me]:
```

```
C:\Documents and Settings\korisnik\Desktop\OpenSSL-old\openssl-0.9.8e_WIN32\bin\open...
OpenSSL> req -out MYCSR.csr -pubkey -new -keyout MYKEY.key
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'MYKEY.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
DomainComponent<me> [me]:me
DomainComponent<ac> [ac]:ac
DomainComponent<MREN> [MREN]:MREN
Organization Name <univerzitetska jedinica> [CIS]:CIS
Common Name <ime i prezime, ili DNS> [l:Marko Markovic]
OpenSSL> _
```

Ovim je završeno generisanje zahtjeva za sertifikat (MYCSR.csr) i odgovarajućeg privatnog ključa (MYKEY.key). Oni su smješteni u C:\... \OpenSSL\bin :



Fajl mykey.key smjestite na sigurno mjesto na vašem kompjuteru , tako da bude dostupan samo vama, a fajl mycsr.csr pošaljite mailom (kao attachment) na mren-ca@ac.me da bi bio potpisan od MREN-CA.

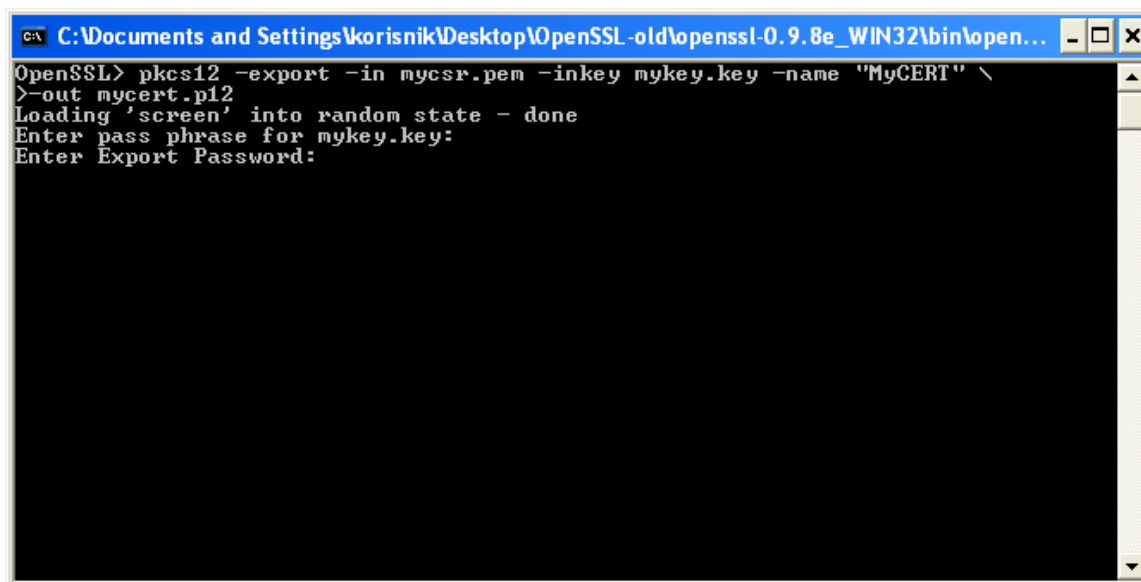
Nakon sprovođenja prethodna dva koraka ovlašćeni korisnik će biti obaviješten e-mailom od strane MREN CA da je dobio sertifikat (ili ako nije , biće obaviješten zašto nije), i u čijem će se attachmentu nalaziti sertifikat (mycsr.pem) potpisan od strane MREN-CA. Ovaj sertifikat treba sačuvati u C:\... \OpenSSL\bin.

3) Generisanje .p12 skupa

Sada treba da u OpenSSLu generišete .p12 skup, kako biste mogli importovati vaš sertifikat. U u C:\... \OpenSSL\bin moraju se nalaziti fajlovi mycsr.pem i mykey.pem . Unestite slijedeću liniju koda:

```
pkcs12 -export -in mycsr.pem -inkey mykey.pem -name "My Certificate" -out mycertificate.p12
```

Nakon toga biće vam zatražen password za private key (onaj koji ste zadali prilikom generisanja zahtjeva i private key-a)



```
C:\Documents and Settings\korisnik\Desktop\OpenSSL-old\openssl-0.9.8e_WIN32\bin\open...
OpenSSL> pkcs12 -export -in mycsr.pem -inkey mykey.key -name "MyCERT" \
>-out mycert.p12
Loading 'screen' into random state - done
Enter pass phrase for mykey.key:
Enter Export Password:
```

a nakon njega trebate zadati Export Password.

Tako ste kreirali mycert.p12 fajl, koji objedinjuje vaš private i public key, i bezbjednost vašeg sertifikata zavisi od bezbjednosti tog fajla.

Sljedeći korak je importovanje sertifikata .

4) Importovanje sertifikata :

- [Kako importovati sertifikat u Internet Explorer/Outlook Express](#)
- [Kako importovati sertifikat u Firefox / Thunderbird](#)
- [Konverzija sertifikata i ključeva](#)
- [gLite 3 User Guide](#) [.PDF format]

5) Prihvatanje sertifikata:

Svaki korisnik nakon dobijanja sertifikata mora da u roku od 5 dana od dana kad mu je izdat sertifikat na mren-ca@ac.me poslati mail u kome će izjaviti :

- Da je pročitao CP/CPS i da se obavezuje na njegovo poštovanje ;
- Da prihvata svoj sertifikat izdat od strane MREN CA ;
- Da prihvata odgovornost da obavjesti MREN CA momentalno u slučaju:
 - Moguće zloupotrebe privat key-a;
 - Ako mu sertifikat više nije potreban ;
 - Ako informacije u sertifikatu postanu nevažeće.

Ovaj e-mail mora biti potpisan private key-em (privatnim ključem) koji odgovara public key-u (javnom ključu) sertifikata koji je korisnik dobio, u slučaju user sertifikata. U slučaju server ili servis sertifikata ovaj e-mail mora biti potpisan private key-em (privatnim ključem koji odgovara public key-u (javnom ključu) user sertifikata administratora. Ukoliko subjekt ne postupi na ovaj način, njemu dodijeljen sertifikat biće opozvan.

E-mail mora sadržati sljedeću izjavu :

Za user sertifikate:

-----Cut here-----

To whom it may concern,

With this email I state that

1. I, "your name", accept my x509v3 digital certificate with

DN: /DC=me/DC=ac/ DC=MREN/O="your organization"/ CN="your name"
Serial Number: "your certificate serial number"
signed by /DC=me/DC=ac/DC=MREN/CN=MREN-CA
2. I adhere the MREN CA policy and usage rules found at:
<http://mren-ca.ac.me/policy%20document.php>
(O.I.D: 1.3.6.1.4.1. 29544.1.1.1.0)
-----Cut here-----

Za server/servis certifikate:

-----Cut here-----

To whom it may concern,

With this email I state that

1. I am the person responsible for the network entity "host/FQDN", and I accept the x509v3 digital certificate with

DN: /DC=me/DC=ac/ DC=MREN/O="your organization"/ CN="host/FQDN"
Serial Number: "certificate serial number"

signed by /DC=me/DC=ac/DC=MREN/CN=MREN-CA

2. I adhere the MREN CA policy and usage rules found at:

<http://mren-ca.ac.me/policy%20document.php>

(O.I.D: 1.3.6.1.4.1. 29544.1.1.1.0)
-----Cut here-----

Ovlašćeni korisnik svoj private key (privatni ključ) i certifikat može koristiti za:

- Potpisivanje/potvrđivanje e-maila i enkriptovanje/dekriptovanje (S/MIME);
- Potvrda autentičnosti servera i enkriptovanje komunikacija ;
- Generalna potvrda autentičnosti (npr. za web site);
- Potvrda autentičnosti korisnika.

5) Produžavanje roka važenja certifikata :

Rok važenja MREN CA certifikata je godinu dana , i da bi se produžio potrebno je najkasnije 30 dana prije njegovog isticanja poslati zahtjev za produženje na mren-ca@ac.me .

6) Opoziv certifikata

Ukoliko iz bilo kog razloga ovlašćeni korisnik ne želi više da koristi svoj certifikat, ili je njegov privatni ključ (private key) izgubljen, ili se sumnja da je neovlašćeno korišćen, potrebno je da pošalje zahjev za opoziv (revokation) na mren-ca@ac.me.

Certifikat će biti opozvan u bilo kom od slijedećih slučajeva :

- CA je informisan da ovlašćeni korisnik nije dao tačne informacije o svom učešću u aktivnostima MRENa.
- Private key (privatni ključ) je izgubljen, ili se sumnja da je dostupan nekom drugom.
- Informacije u certifikatu su pogrešne ili netačne, ili se sumnja da su pogrešne ili netačne.
- Ovlašćeni korisnik je prekršio svoje obaveze.
- Ovlašćeni korisnik nje koristi certifikat u skladu sa zakonom Crne Gore.
- Ovlašćeni korisniku više ne treba certifikat .

Kako importovati sertifikat u Internet Explorer/Outlook Express?

Korak 1 od 3: Prebacivanje PKCS#12 skupa na vaš kompjuter

Potrebno je da se mycertificate.p12 nalazi u vašem kompjuteru.

Korak 2 od 3: Importovanje CA ROOT sertifikata

- Otvorite <http://mren-ca.ac.me/ca%20root%20cert.php> u Internet Exploreru ;
- Kliknite na "CA certificate";
- Novi prozor će se otvoriti, kliknite "open" .

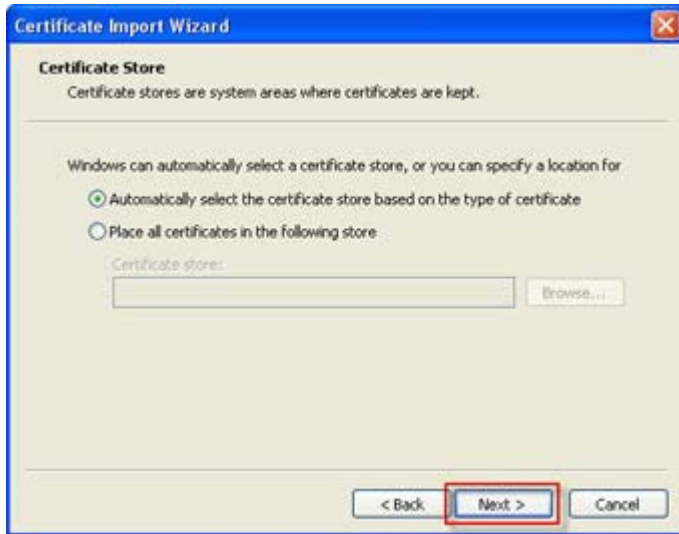


- Startujte import wizard tako što ćete kliknuti na "Install certificate"



- Kliknite "Next" dva puta.





- Kliknite "Finish"



- Kliknite "Yes" u Security prompt-u.



Korak 3 od 3: Importovanje vašeg private key-a (privatnog ključa) i sertifikata u Internet Explorer / Outlook Express

- Otvorite Internet Explorer
- Kliknite "File -> Open" i zatim otvorite lokaciju vašeg pkcs#12 skupa prethodno prebačenog na vaš kompjuter..



- Novi prozor će se pojaviti, kliknite "Next" u dva naredna prozora.



- U sljedećem koraku unesite vaš export password.
- Omogućite "Enable strong private key (privatni ključ) protection. You will be prompted every time the private key is used by an application, if you enable this option."
- Onemogućite "Mark this key as exportable. This will allow you to backup or transport your keys at a later time."



- Selektujte "Next" u dva sljedeća koraka, i onda "Finish";
- Selektujte "Ok" kad se sljedeći prozor pojavi.



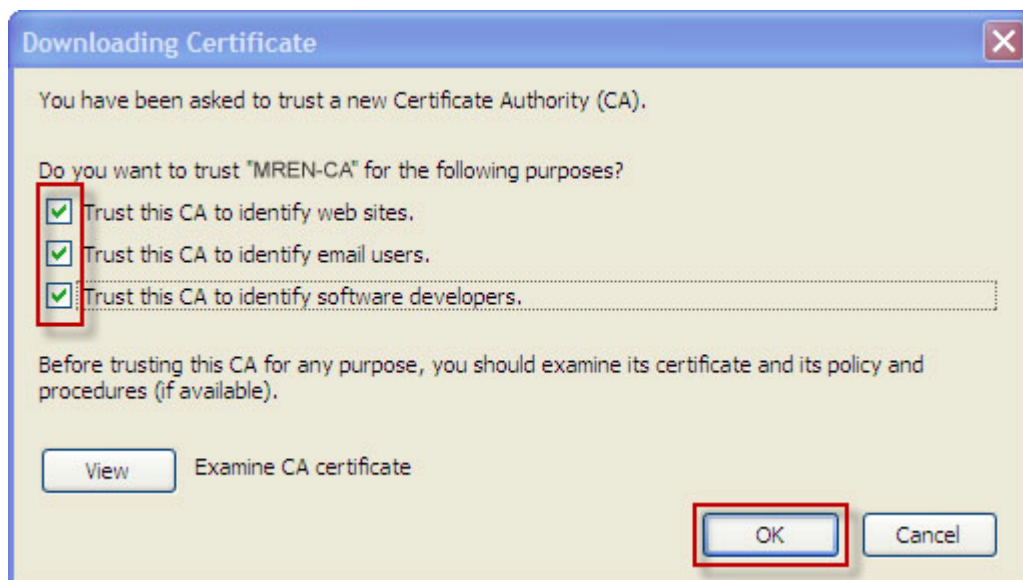
Kako importovati sertifikat u Firefox / Thunderbird?

Korak 1 od 4: Prebacivanje PKCS#12 skupa na vaš kompjuter

Potrebno je da mycertificate.p12 bude sačuvan u vašem kompjuteru.

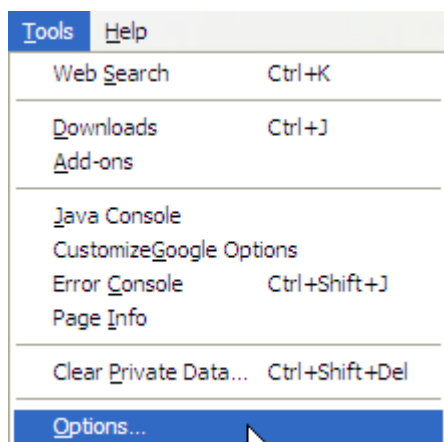
Korak 2 od 4: Importovanje CA ROOT sertifikata u Firefox

- Otvorite <http://mren-ca.ac.me/ca%20root%20cert.php> u Firefoxu.
- Kliknite na "CA certificate"
- Novi prozor će se otvoriti, čekirajte sva tri boksa i kliknite "ok". Root sertifikat je instaliran u Firefoxu.

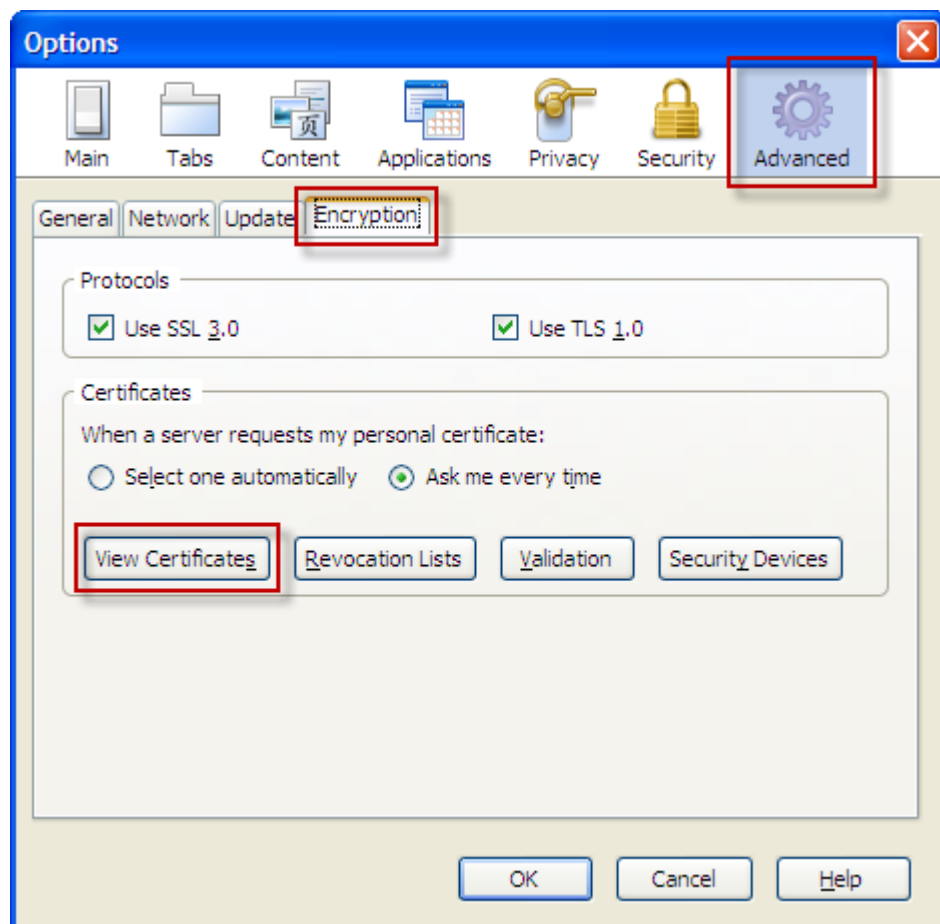


Korak 3 od 4: Importovanje vašeg private key-a (privatni ključ) i sertifikata u Firefox

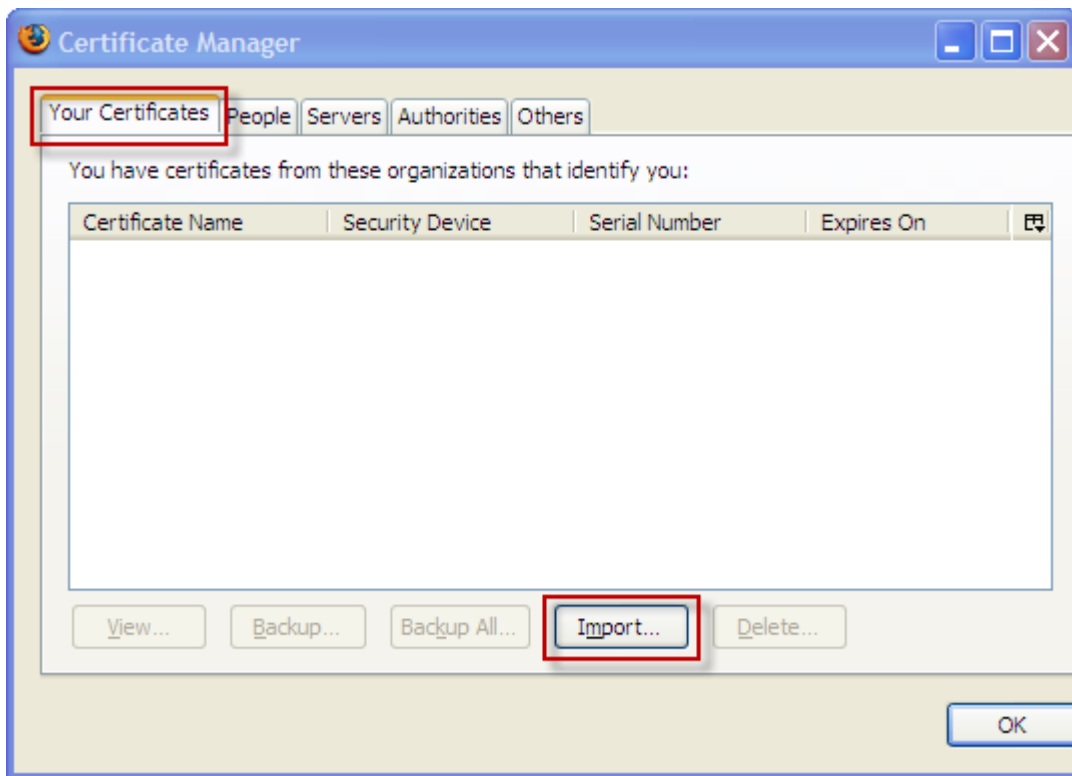
- Otvorite meni "Tools / Options"



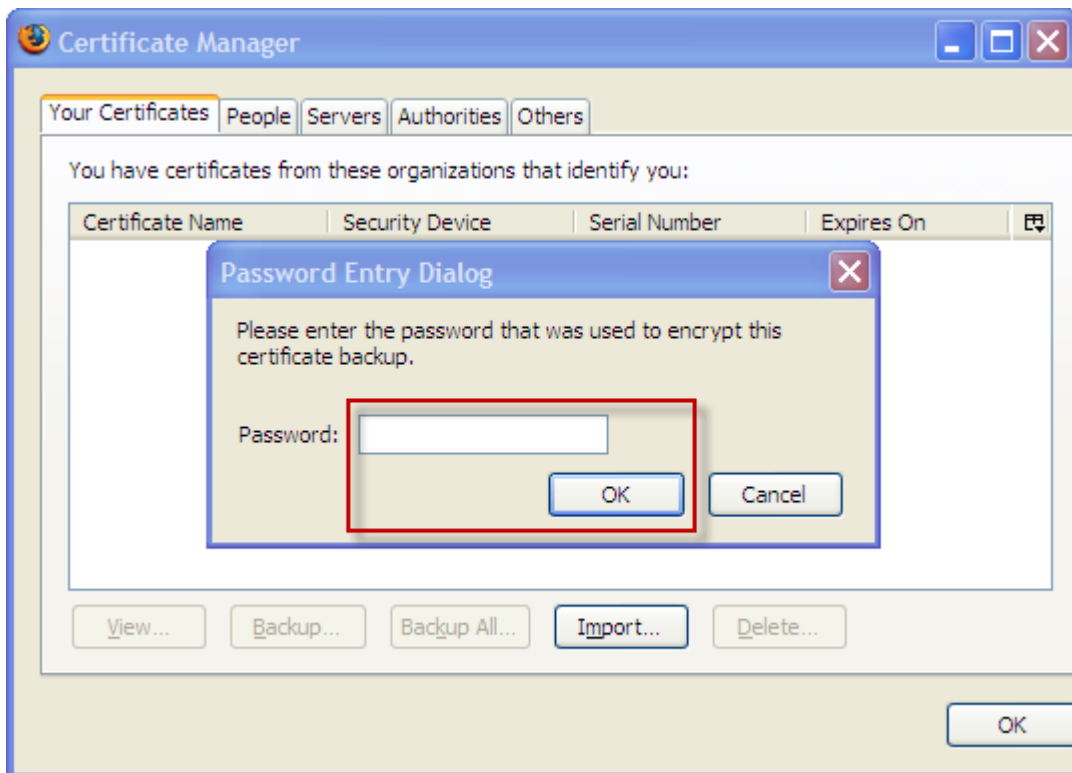
- Novi prozor će se otvoriti, kliknite "Advanced / Encryption / View Certificates"



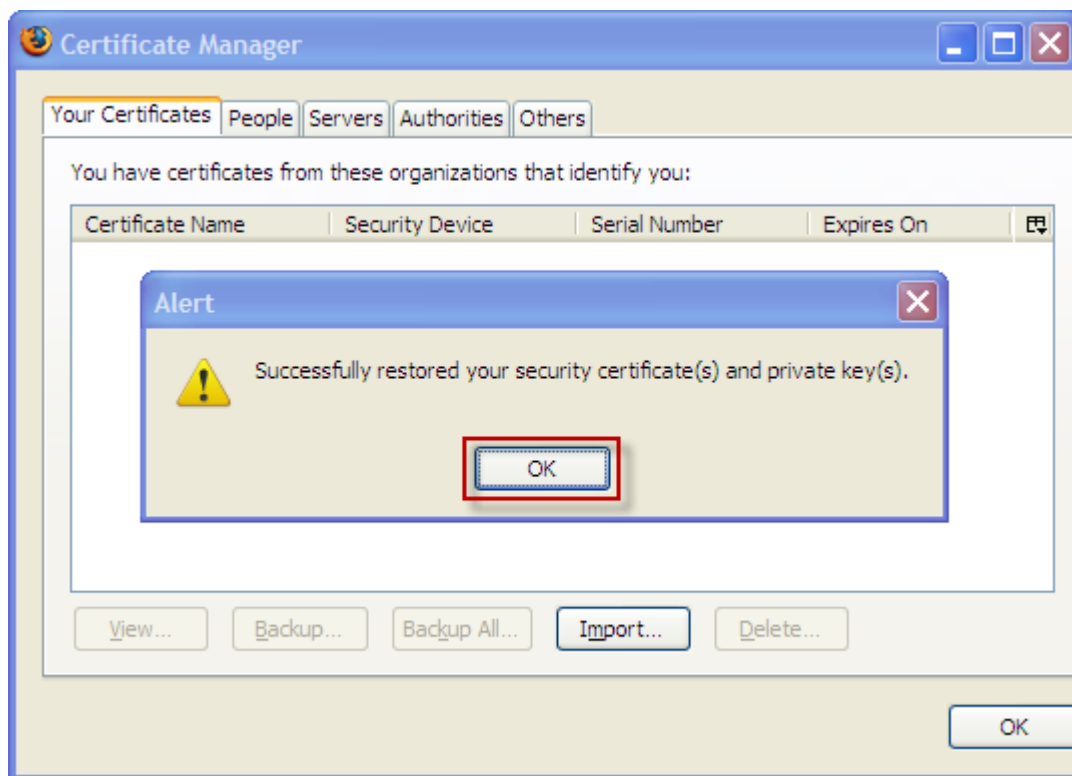
- Novi prozor će se otvoriti, kliknite "Your certificates / Import"



- Otvorite lokaciju vašeg PKCS#12 sertifikata, kliknite "Open", unesite password i kliknite "Ok"

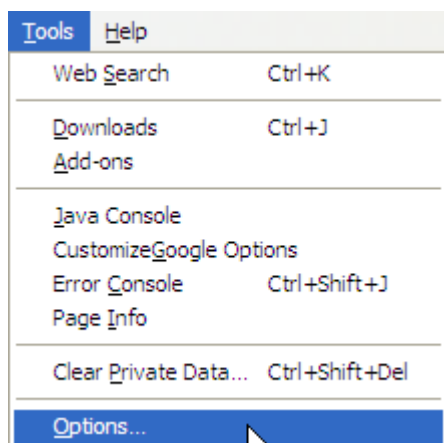


- Vaš sertifikat je sada importovan, kliknite "Ok"

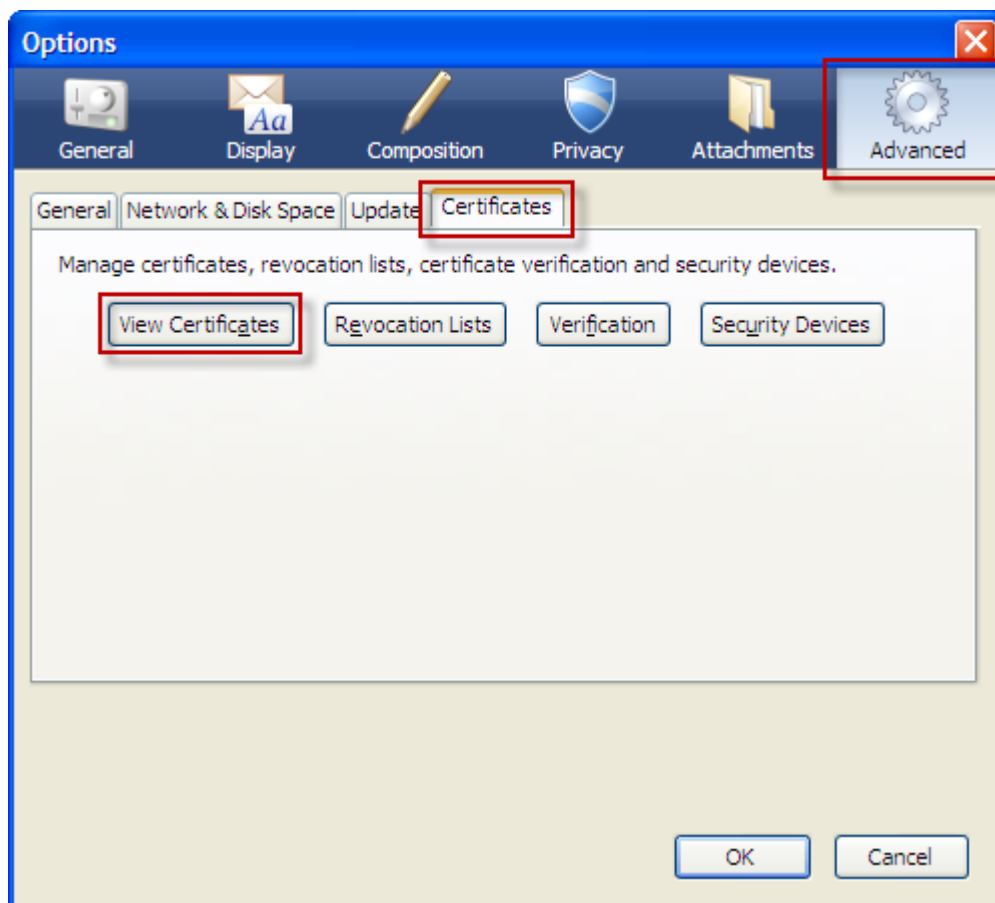


Korak 4 od 4: Importovanje vašeg private key-a (privatni ključ) i sertifikata u Thunderbird

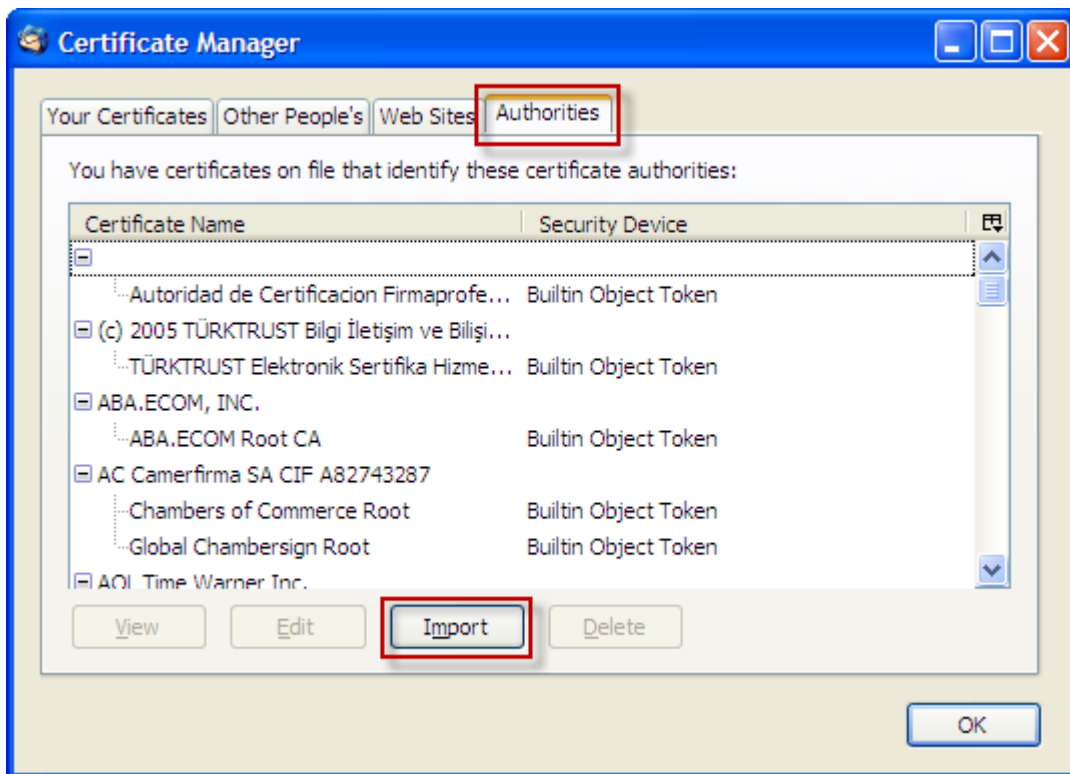
- Otvorite <http://mren-ca.ac.me/ca%20root%20cert.php> u vašem browser-u
- Kliknite na "CA certificate", i sačuvajte ga na željenoj lokaciji
- Otvorite Thunderbird i otvorite meni "Tools / Options"



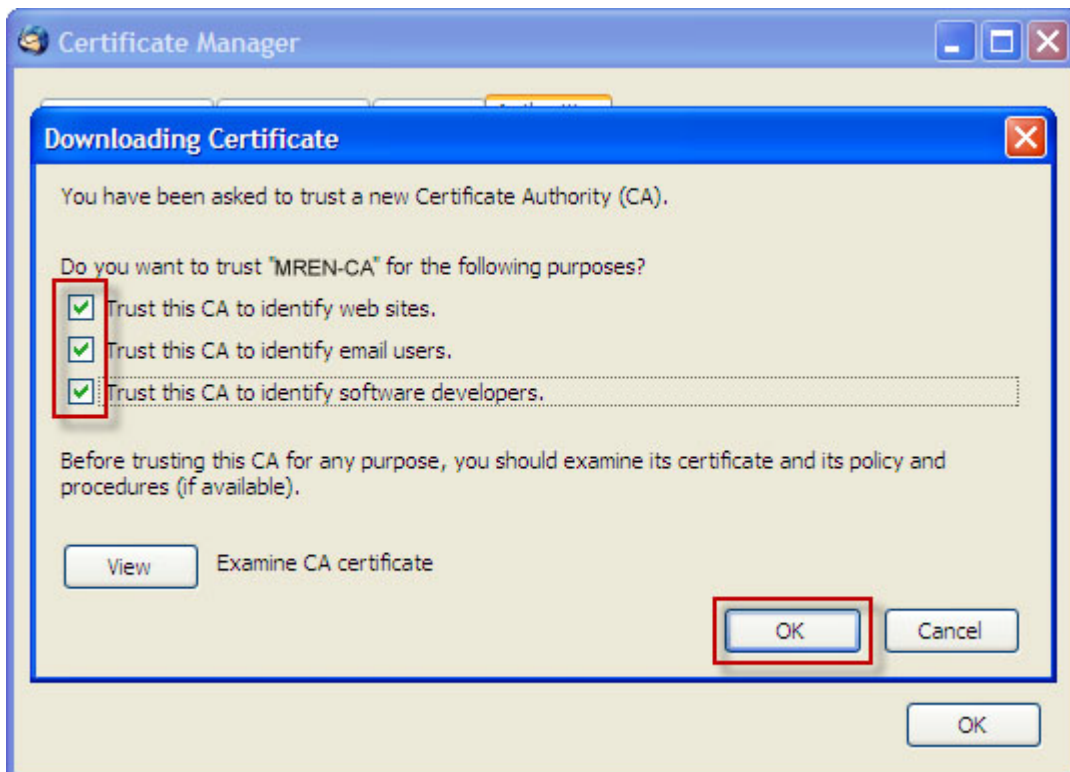
- Kliknite na "Advanced / Certificates / View certificates"



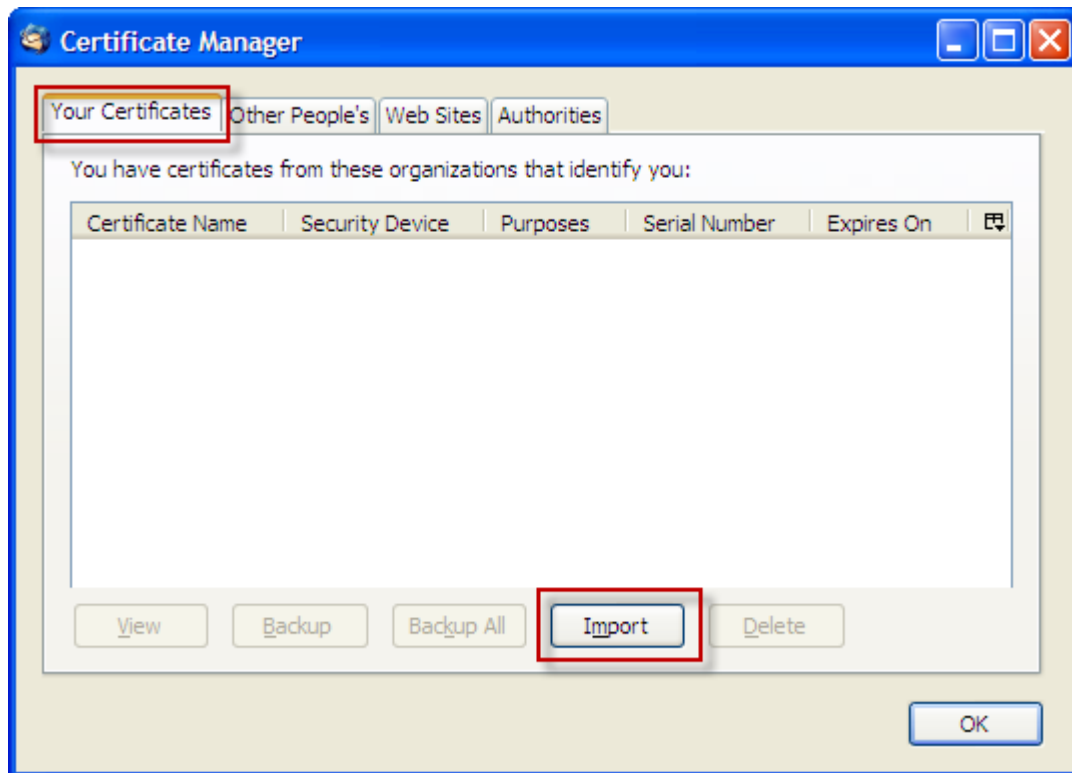
- Novi prozor će se otvoriti, kliknite na "Authorities / Import"



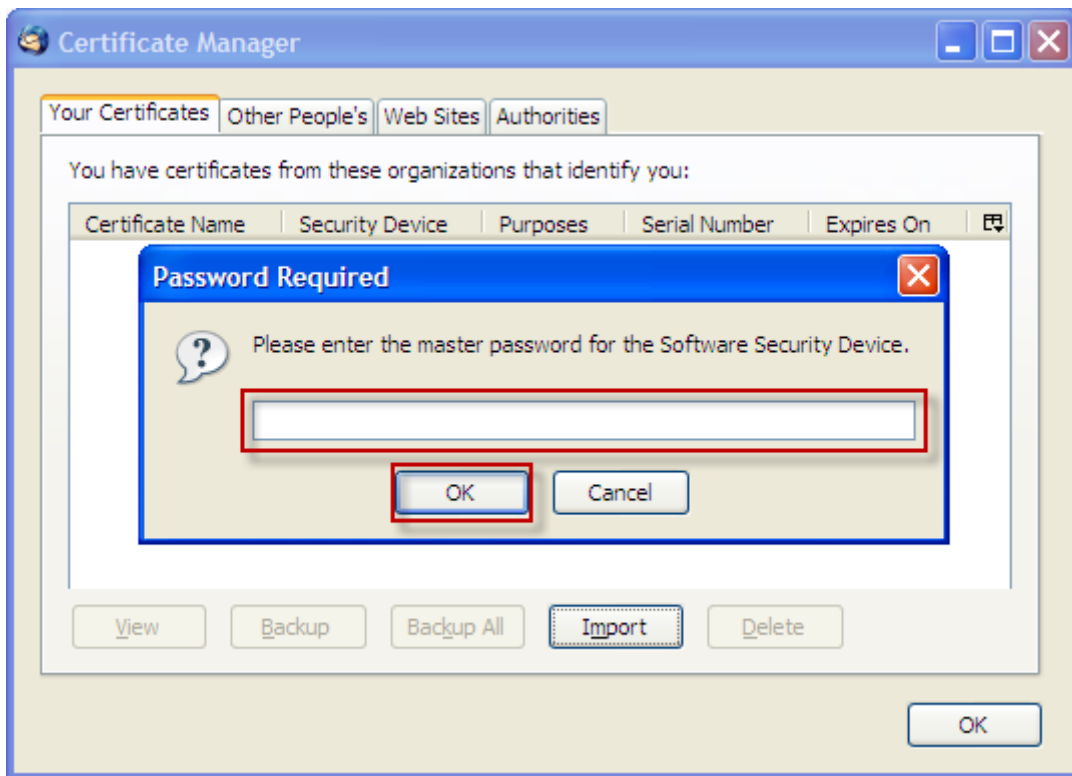
- Otvorite lokaciju na kojoj ste prethodno sačuvali ROOT sertifikat I kliknite "Open", čekirajte sva tri boksa, i kliknite "Ok"



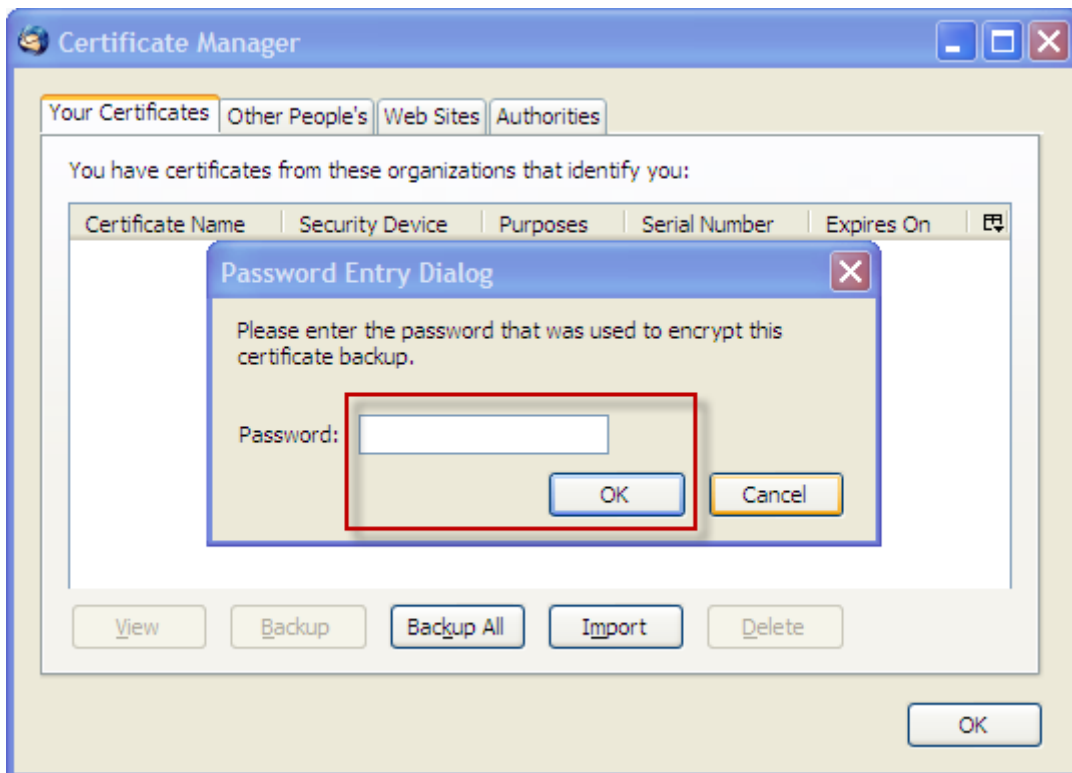
- Kliknite "Your certificates / Import", otvorite likaciju vašeg PKCS#12 skupa I kliknite "Open"



- Unesite master password za Thunderbird (izabrali ste master password koji će biti korišćen za otvaranje svih sertifikata smještenih u Thunderbird-u)



- Unesite vaš certifikat password



Konverzija sertifikata i ključeva

PKC12 (browser friendly) -> PEM (Globus friendly)

- user sertifikat
\$ openssl pkcs12 -in usercert.p12 -out usercert.pem -nokeys -clcerts
Enter Import Password:
MAC verified OK
- user key (ključ je enkriptovan)
\$ openssl pkcs12 -in usercert.p12 -out userkey.pem -nocerts
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
- host & servise sertifikat
\$ openssl pkcs12 -in hostcert.p12 -out hostcert.pem -nokeys -clcerts
Enter Import Password:
MAC verified OK
- host & service key (ključ nije enkriptovan)
openssl pkcs12 -in hostcert.p12 -out hostkey.pem -nocerts -nodes
Enter Import Password:
MAC verified OK

PEM (Globus friendly) -> PKC12 (browser friendly)

- \$ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -certfile /etc/grid-security/certificates//serial-number.pem -out usercert.p12
Enter pass phrase for userkey.pem:
Enter Export Password:
Verifying - Enter Export Password: