SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINARSKI RAD

INFRASTRUKTURA JAVNOG KLJUČA, PKI – Public Key Infrastructure

Student: Franjo Rebac

Mentor: doc. dr. sc. Marin Golub

ZAGREB 2005

Sadržaj

1 **Uvod** 1
2 **Osnove kriptografije** 2
2.1 Sigurnosni zahtjevi 2
2.2 Simetrična kriptografija 3
2.3 Asimetrična kriptografija 5
2.4 Sažetak poruke 6
2.5 Digitalni potpis 6
2.6 Digitalni certifikat 8
3 **Infrastruktura javnog ključa** 11
3.1 PKI arhitektura 11
4 **Programsko ostvarenje PKI sustava** 13
4.1 PKI administracija 14
4.2 PKI korisnički dio 18
4.3 PKI baza podataka 22
5 **Zaključak** 26
6 **Literatura** 27
7 **Dodaci** 28
7.1 Dodatak A: Instalacija ostvarenog PKI sustava 28
7.2 Dodatak B: Primjena certifikata u Mozilli Thunderbirdu i S/MIME protokolu 30

1 Uvod

Infrastruktura javnog ključa (engl. ***Public Key Infrastructure*** - ***PKI***), je vrlo složen sustav temeljen na asimetričnoj kriptografiji. PKI objedinjuje certifikate, certifikacijsku ustanovu (certifikator), spremnik certifikata i opozvanih certifikata, korisnike certifikata, te sve njihove međusobne interakcije (interakcije između pojedinih elemenata sustava). Njegova osnovna namjena je sigurna komunikacija preko nesigurnih kanala.
Sama ideja o PKI-u nastala je sedamdesetih godina prošlog stoljeća. U to je vrijeme postojala simetrična kriptografija odnosno kriptografija temeljena na tajnom ključu, a algoritam DES kao standard i osnovni algoritam temeljen na simetričnoj kriptografiji. Glavni problem simetrične kriptografije bio je sigurna razmjena tajnog ključa preko nesigurnog kanala. Godine 1976. Whitfield Diffie i Martin Hellman u svojoj su publikaciji "*New Directions in Cryptography*" predstavili ideju razmjene tajnog ključa temeljenu na asimetričnoj kriptografiji (kriptografija temeljena na javnom i privatnom ključu). Asimetrična kriptografija omogućila je i digitalno potpisivanje podataka. Dvije godine poslije uveden je pojam digitalnog certifikata kao digitalno potpisanog podatka koji povezuje javni ključ s osobom kojoj taj ključ pripada. Sve ovo, kao i pojava suvremene komunikacije preko medija (ponajviše pojava Interneta) kao nesigurnog kanala, dovelo je do realizacije PKI-a kao sustava koji omogućuje sigurnu komunikaciju preko nesigurnog kanala.
Uz sve prednosti PKI-a, kao i velik broj standarda vezanih uz njega, on nije saživio u stvarnosti onako kako se očekivalo. Danas postoji veoma malen broj ostvarenih sustava temeljenih na infrastrukturi javnog ključa. Razloge tomu prvenstveno treba tražiti u samoj složenosti realizacije i velikim troškovima izgradnje ovog sustava.

2 Osnove kriptografije

2.1 Sigurnosni zahtjevi

Kriptografski postupci matematičke su funkcije, odnosno algoritmi kojima se nizovi bitova jasnog teksta preračunavaju u nizove bitova kriptiranog teksta i obratno. Kriptiranje je postupak prevođenja podatka u izvornom obliku (jasni tekst ili engl. *cleartext*) u oblik u kojem se taj podatak više ne raspoznaje (kriptirani tekst ili engl. *ciphertext*). Kriptiranje se formalno može zapisati u sljedećem obliku:

$$\boldsymbol{C = E(P, K_E)},$$

gdje su:
P – jasni tekst,
C – kriptirani tekst,
E – funkcija kriptiranja,
$\boldsymbol{K_E}$ – ključ kriptiranja.
Obrnuti postupak prevođenja kriptiranog teksta u jasni tekst naziva se dekriptiranje. Njegov formalni opis je:

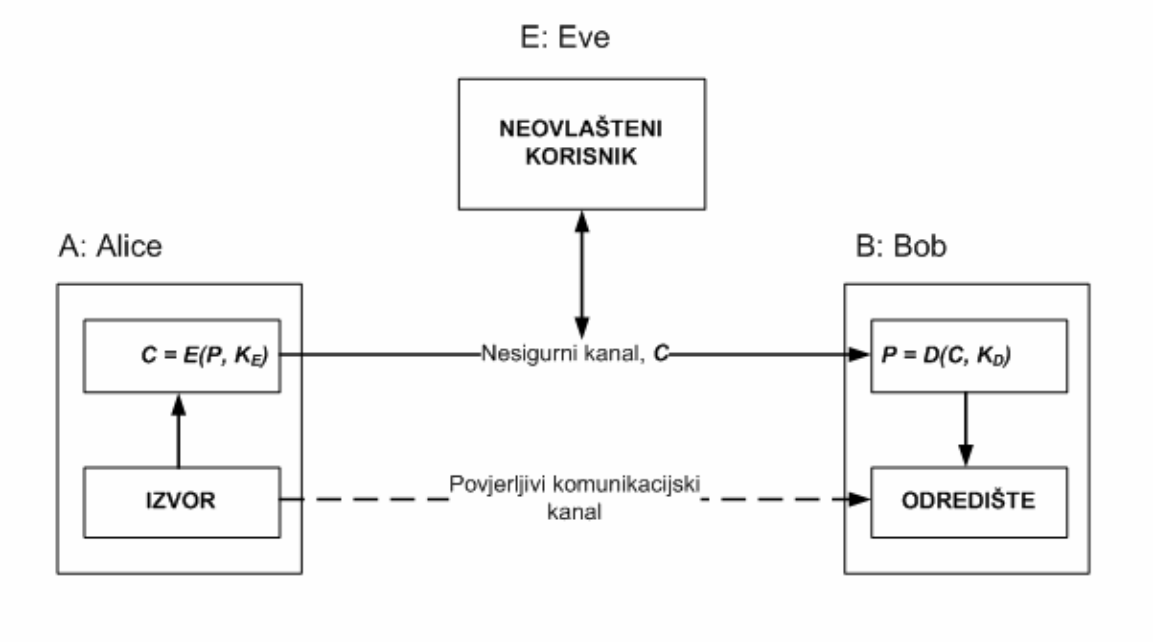
$$\boldsymbol{P = D(C, K_D)},$$

gdje su:
P – jasni tekst,
C – kriptirani tekst,
D – funkcija dekriptiranja,
$\boldsymbol{K_D}$ – ključ dekriptiranja.
Funkcije kriptiranja i dekriptiranja zajedno čine kriptosustav.

Glavni ciljevi kriptografije ili sigurnosni zahtjevi su povjerljivost, raspoloživost, besprijekornost, autentifikacija, autorizacija te neporecivost. Prva tri zahtjeva osnovni su sigurnosni zahtjevi.

1. Povjerljivost ili tajnost osigurava da sadržaj informacije bude pristupačan samo ovlaštenim korisnicima (korisnicima kojima je namijenjena), i nikomu drugomu.
2. Raspoloživost osigurava da informacije budu na raspolaganju ovlaštenim korisnicima.
3. Besprijekornost ili integritet osigurava da informacije u sustavu mogu mijenjati samo za to ovlašteni korisnici, odnosno osigurava nepromjenjivost podataka.
4. Autentifikacija je postupak provjere identifikacije odnosno utvrđivanje vjerodostojnosti korisničkog identiteta.
5. Autorizacija je postupak koji obuhvaća autentifikaciju i provjeru ovlasti odnosno provjeru prava pristupa.
6. Neporecivost predstavlja zaštitu od opovrgavanja, a to znači onemogućavanje negiranja prethodno počinjenog dijela od strane korisnika.

Sve sigurnosne zahtjeve osim raspoloživosti rješava kriptiranje.



Slika 2.1*: Prikaz sudionika komunikacije u kojoj se koristi kriptiranje. Alice šalje poruku Bobu kriptiranu ključem* K_E*, a Bob je dekriptira ključem* K_D*, dok Eve predstavlja neovlaštenog korisnika koji može prisluškivati nesigurni kanal.*

Važno je istaknuti da u prikazu na ***slici 2.1*** komunikacija između izvora i odredišta predstavlja sigurni kanal zahvaljujući kriptiranju poruka.
Osnovna podjela kriptografskih algoritama je na simetrične i asimetrične algoritme (simetrična i asimetrična kriptografija).

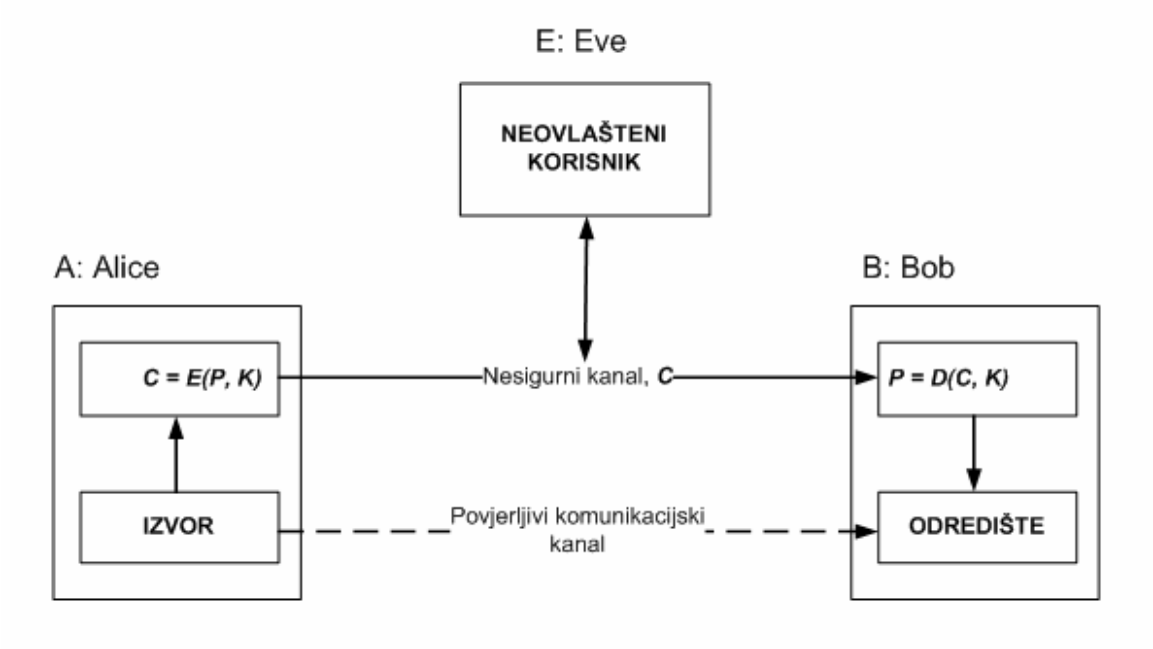
2.2 Simetrična kriptografija

Simetrična kriptografija je najstariji oblika kriptografije, stara gotovo koliko i ljudska komunikacija. Još se naziva i kriptografijom tajnog ključa jer se podatak kriptira i dekriptira istim ključem (tajni ključ, sjednički ključ). U simetričnim kriptosustavima ključ kriptiranja K_E jednak je ključu dekriptiranja K_D. Prema tome zajednički ključ se može označiti jednim simbolom K, te za takav sustav vrijedi:

$$C = E(P, K),$$
$$P = D(C, K),$$

odnosno:

$$P = D(E(P, K), K).$$

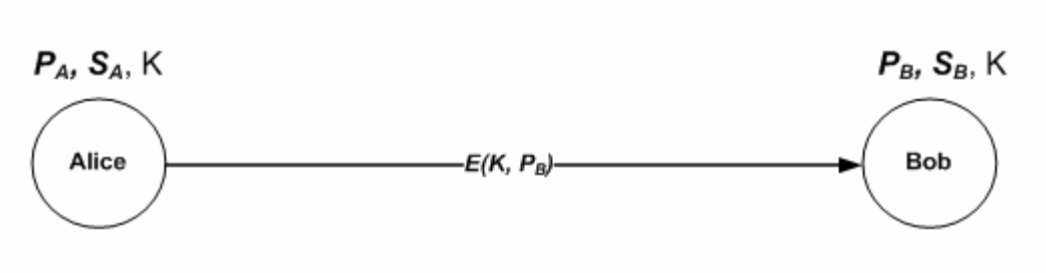


***Slika 2.2**: Simetrična kriptografija. Alice šalje poruku Bobu kriptiranu tajnim ključem **K**, a Bob je dekriptira tim istim ključem (**$K_E = K_D = K$**).*

Za proces kriptiranja u simetričnoj kriptografiji potrebno je znati algoritam kriptiranja i tajni ključ. Nekad su se algoritmi držali u tajnosti, ali se pokazalo da skrivanje algoritma ne doprinosi sigurnosti. Svi suvremeni simetrični algoritmi javno su obznanjeni. Zbog toga ih je u potpunosti moguće testirati i provjeriti njihovu otpornost na napade, odnosno moguće ih je analizirati (kriptoanaliza). Sigurnost simetričnih algoritama ovisi o sigurnosti samog algoritma i dužini ključa. Najpoznatiji simetrični algoritam je DES (Data Encryption Standard), kojeg je razvio IBM 1977. godine. Bio je standardni simetrični algoritam sve do 2000. godine kad ga je zamijenio AES (Advanced Encryption Standard), koji rukuje ključevima dužine 128, 192 i 256 bita. Glavni razlog zbog kojeg je DES zamijenjen AES-om je taj što DES ima dužinu ključa od 56 bita.
Osnovni nedostatak simetričnih algoritama, odnosno simetričnih kriptosustava, jest upravljanje ključevima, točnije njihova distribucija. Prije same sigurne komunikacije subjekti (sudionici komunikacije) moraju razmijeniti ključeve. Pošto se sigurnost svih zaštićenih (kriptiranih) informacija oslanja na sigurnosti ključa, sigurna razmjena ključeva može postati vrlo ozbiljan problem. On dolazi do izražaja još više što se komunikacija odvija na većoj udaljenosti, a u samoj komunikaciji sudjeluje više subjekata. Za ***n*** korisnika u komunikaciji potrebno je ***n(n - 1)/2*** ključeva. Generiranje i upravljanje ovako velikim brojem ključeva je najčešće nepraktično, a njihova razmjena nesigurna.
Rješavanje ovog problema, problema razmjene tajnih ključeva, dovela je do pojave asimetričnih algoritama odnosno asimetrične kriptografije.

2.3 Asimetrična kriptografija

Godine 1976. Whitfield Diffie i Martin Hellman u svojoj su publikaciji "*New Directions in Cryptography*" predstavili ideju razmjene tajnog ključa temeljenu na asimetričnoj kriptografiji, u kojoj je predočeno postojanje para ključeva: ključ za kriptiranje ***P*** i ključ za dekriptiranje ***S***, umjesto jednog istog ključa za kriptiranje i dekriptiranje ***K***. Jedan ključ je javno dostupan svima, naziva se *javni ključ*, i on služi za kriptiranje. Drugi ključ je poznat samo njegovom vlasniku, naziva se *privatni ključ*, i služi za dekriptiranje poruka.



Slika 2.3*: Razmjena tajnog ključa* ***K*** *između Alice i Boba asimetričnim kriptiranjem. Alice šalje tajni ključ* ***K*** *kriptiran Bobovim javnim ključem* $\boldsymbol{P_B}$*, a Bob ga dekriptira svojim privatnim ključem* $\boldsymbol{S_B}$*. Ključ* ***K*** *služi kao ključ kriptiranja u daljnjoj komunikaciji između Alice i Boba (taj ključ se još naziva i sjedničkim ključem).*

Osnova sigurnosti asimetričnih algoritama temelji se na nemogućnosti (ili vrlo teškoj mogućnosti) izračunavanja privatnog ključa iz javnog ključa. Prema najpoznatijim algoritmima koji se koriste u asimetričnoj kriptografiji ovaj se problem svodi na težinu faktorizacije prirodnih brojeva na proste faktore. Takav algoritam je i RSA (Rivest, Shamir, Adleman). Treba istaknuti da se asimetrični algoritmi ne koriste za kriptiranje velikog broja podataka. Njihova osnovna namjena je razmjena sjedničkih ključeva prije početka sjednice odnosno komunikacije između subjekata. Razlog ovome ponajviše je taj što je asimetrično kriptiranje za nekoliko redova sporije od simetričnog kriptiranja. Iz sigurnosnih razloga trajanje (misli se na vremensko razdoblje u kojem je ključ aktivan) sjedničkog ključa je relativno kratko, a najčešće je onoliko koliko traje sjednica. Trajanje javnog i privatnog ključa kod asimetrične kriptografije je znatno duže, i nije ga potrebno previše često mijenjati jer je količina podataka koja se kriptira asimetričnom kriptografijom znatno manja (to su u pravilu kratke poruke poput sjedničkog ključa), a to znatno otežava neke vrste napada.
Poželjno svojstvo asimetričnih algoritama je sljedeće: ako je poruka kriptirana javnim, njezino dekriptiranje obavlja se privatnim ključem, a ako se poruka kriptira privatnim ključem, njezino dekriptiranje obavlja se javnim ključem. To je svojstvo asimetričnog algoritma u kojem je svejedno koji ćemo ključ izabrati za kriptiranje (ali tada dekriptiranje obavljamo onim drugim ključem). Ovo važno svojstvo nekih asimetričnih algoritama jednostavno omogućava digitalno potpisivanja dokumenata ili digitalni potpis, bez kojeg bi bilo nemoguće ostvariti PKI sustav.

2.4 Sažetak poruke

Sažetak poruke osigurava sigurnosni zahtjev besprijekornosti odnosno integriteta poruke. Kriptografski sažetak izrađuje se ***jednosmjernom funkcijom*** koja iz poruke proizvoljne duljine izračunava sažetak stalne duljine. Ova je funkcija jednosmjerna stoga što je izračunavanje sažetka vrlo lako dok je iz sažetka praktički nemoguće izračunati izvornu poruku.
Razlog zbog kojeg se uvodi kriptografski sažetak bit će objašnjen na primjeru. Pretpostavimo da Bob i Alice žele komunicirati i da međusobno poznaju javne ključeve. Bob želi biti siguran:

- da je neki javni tekst koji mu je Alice poslala uistinu njezina poruka i
- da neki napadač (Eve) nije tijekom komunikacije mijenjao sadržaj poruke, odnosno da je primljenoj poruci sačuvan integritet.

Najjednostavniji oblik jednosmjerne funkcije je uzastopna uporaba ***XOR*** funkcije na nizu bitova koji se dobivaju dijeljenjem izvorne poruke na dijelove jednake duljine. Najpoznatiji algoritmi koji izračunavaju sažetak su ***MD5***, ***SHA-1*** te ***Tiger***. Standardne duljine sažetka se kreću od 64 bita pa do 256 bita (64, 128, 160, 256), a ovise o algoritmu sažimanja.

2.5 Digitalni potpis

Digitalni potpis mora imati sva svojstva vlastoručnog potpisa, a to su sljedeća:

1) vlastoručni potpis je autentičan, a to znači da ga može izdati samo potpisnik osobno,
2) vlastoručni potpis moguće je provjeriti usporedbom s prethodnim potpisima,
3) vlastoručni potpis izražava autorstvo ili slaganje sa sadržajem dokumenta i njegov je neodvojivi dio,
4) vlastoručni potpis ne može se poreći.

Ova svojstava ne znače da se vlastoručni potpis ne može krivotvoriti, ali postoje metode s kojim se može s velikom sigurnošću utvrditi da li je on krivotvoren.
Dokumente u digitalnom obliku lako je mijenjati, a da bi oni imali pravnu ili neku drugu vrijednost potrebno im je osigurati autentičnost. Ta autentičnost se osigurava digitalnim potpisivanjem dokumenta. Digitalni potpis je u osnovi funkcija sadržaja digitalnog dokumenta i privatnog ključa potpisnika. Vjerodostojnost potpisanog dokumenta se obavlja upotrebom sadržaja dokumenta i javnog ključa potpisnika.
Digitalni potpis se može izraziti formulom:

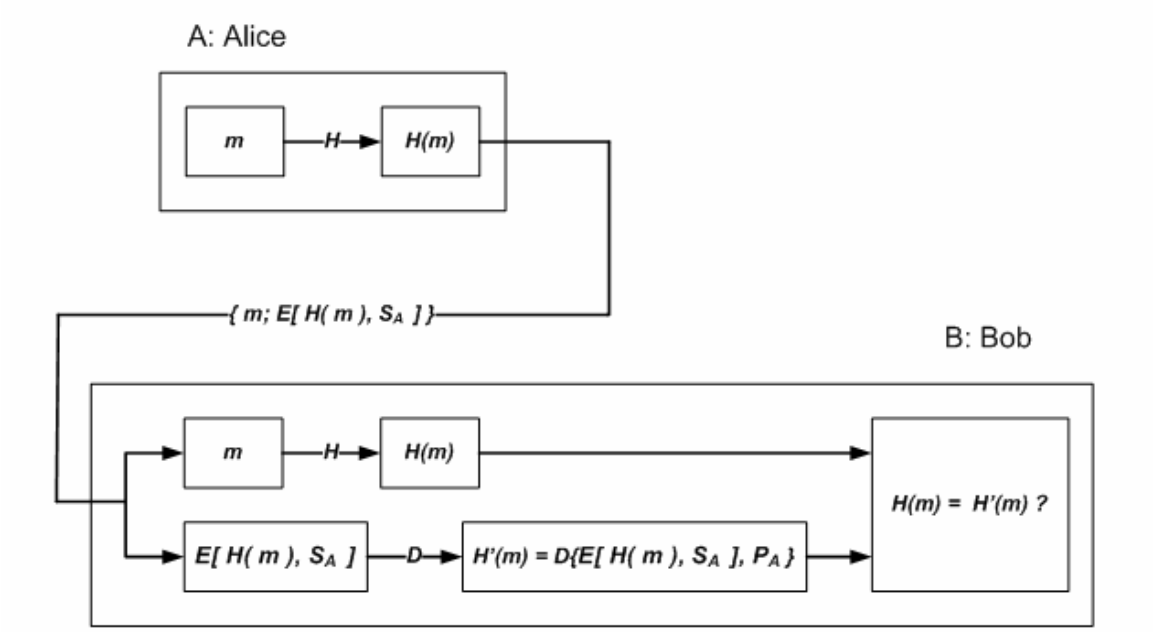
$$\textit{Digitalni potpis} = E[\, H(m),\, S_A \,]\ ,$$

a digitalno potpisani dokument:

$$\textit{Digitalno potpisani dokument} = \{\, m;\, E[\, H(m),\, S_A \,] \,\},$$

gdje su:
m – digitalni dokument koji se potpisuje,

H(m) – sažetak digitalnog dokumenta, a ***H*** funkcija sažetka,
S_A – privatni ključ potpisnika,
E – funkcija kriptiranja (asimetrično kriptiranje).



Slika 2.4*: Protokol digitalnog potpisivanja dokumenta: digitalni dokument potpisuje Alice te ga šalje Bobu, a Bob ga nakon primitka provjerava, gdje je* ***D*** *funkcija dekriptiranja,* P_A *javni ključ koji pripada Alice,* ***H'(m)*** *sažetak kojeg izračunava Bob iz primljenog digitalnog dokumenta kojem se provjerava autentičnost, a ostale oznake iz protokola su prethodno pojašnjene.*

Digitalno potpisivanje bit će objašnjeno na sljedećem primjeru (***slika 2.4***). Pretpostavimo da Alice šalje dokument Bobu. Ona nekim određenim algoritmom sažimanja sažme digitalni dokument. Taj sažetak kriptira svojim privatnim ključem (ovdje je potrebno istaknuti da asimetrični algoritam kriptiranja mora imati prethodno objašnjeno svojstvo koje omogućava i kriptiranje privatnim ključem, a dekriptiranje javnim ključem). Na taj način je digitalno potpisala dokument. Šalje dokument s digitalnim potpisom (digitalno potpisani dokument) Bobu. On po primitku digitalno potpisanog dokumenta izdvaja njegov sadržaj, sadržaj bez potpisa, te izračunava njegov sažetak istim algoritmom sažimanja koji je koristila Alice. S Aliceinim javnim ključem dekriptira digitalni potpis istim asimetričnim algoritmom kojim ga je Alice kriptirala. Dekriptirani sadržaj digitalnog potpisa uspoređuje sa sažetkom koji je on izračunao. Ako je usporedba uspjela onda se radi o autentičnom i besprijekornom dokumentu kojeg je uistinu poslala Alice. Bob zna da je taj dokument poslala Alice jer samo ona zna svoj privatni ključ. Na ovaj način je moguće postići osobine vlastoručnog potpisa:

1) digitalni potpis je autentičan, što znači da ga može napraviti samo posjednik privatnog ključa,
2) digitalni potpis je moguće provjeriti uporabom javnog ključa potpisnika,

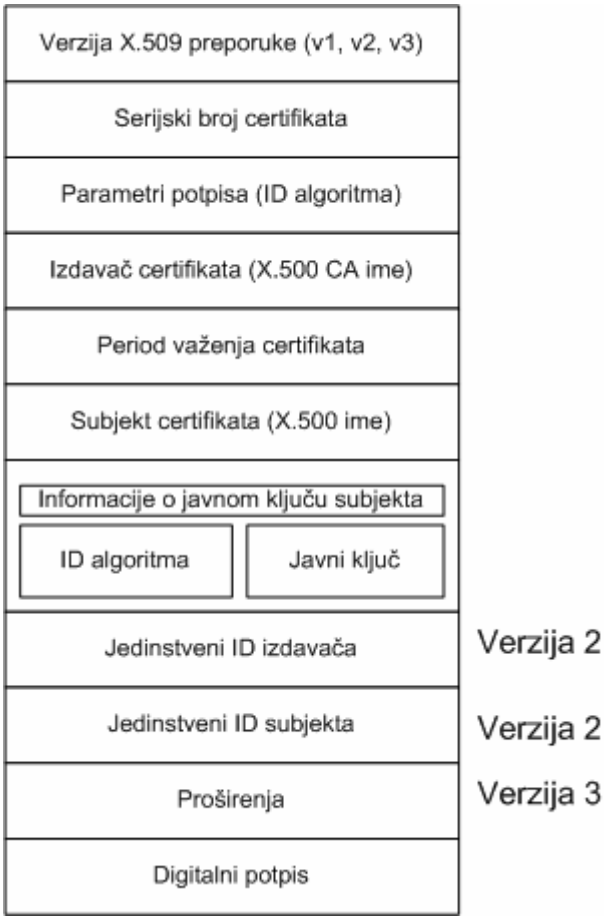
3) digitalni potpis izražava autorstvo ili slaganje sa sadržajem dokumenta, a pošto je funkcija dokumenta slijedi da je neodvojiv od sadržaja,
4) digitalni potpis se ne može poreći.

Važno je istaknuti da uz sve ove sigurnosne zahtjeve, integritet, autentičnost i neporecivost, digitalni potpis ne osigurava tajnost.

2.6 Digitalni certifikat

Digitalni certifikat je digitalno potpisani dokument koji povezuje javni ključ s osobom kojoj pripada (vlasnikom javnog ključa). Uveden je iz tog razloga što sudionici u komunikaciji, da bi uopće mogli komunicirati, moraju na neki način doznati ključeve svojih partnera. Osim toga, moraju biti uvjereni da partneri nisu uljezi koji se lažno predstavljaju. Ideju digitalnog certifikata predložio je L. Kohnfelder 1978. godine. Certifikat se digitalno potpisuje iz tog razloga što se osigurava njegov integritet, koji jamči potpisnik. Potpisnik digitalnog certifikata naziva se ***certifikacijski centar*** (engl. ***Certification Authority*** - ***CA***). Certifikacijski centar (***CA***) je ustanova ili tijelo kojoj svi korisnici certifikata vjeruju i čiji javni ključ, koji se koristi za provjeru potpisa na certifikatu, mora biti pouzdano ispravan. O certifikacijskim centrima bit će riječi u nastavku ovog rada.

Sve ove sigurnosne mehanizme navedene u ovom poglavlju (2. poglavlje) objedinjuje složeni sustav u kojem se odvija sigurna komunikacija, a koji se naziva ***infrastruktura javnog ključa*** (engl. ***Public Key Infrastructure*** - ***PKI***). Jedan od osnovnih modela certifikata koji čini osnovu za ostvarenje velikog broja sustava temeljenih na ***PKI*** – u ima oznaku ***X.509***. Taj je model uspostavljen u okviru Međunarodne telekomunikacijske unije (***ITU***), a nastao je na temelju standarda X.500 preporuka za direktorije i objavljen 1988 godine. ***X.509*** trenutno je u svojoj trećoj verziji. Verzija 1 nadopunjena je dvama dodatnim poljima (***slika 2.5***), te je nastala verzija 2. Ona je nadopunjena dodatnim poljem koje omogućava proširenja, s tim da ne zahtjeva njihovo postojanje, te je nastala verzija 3 (***slika 2.5***). Ovaj format definirali su ISO/IEC, ITU-T i ANSI X9 1996. godine.



Slika 2.5*: Verzija 3 digitalnog certifikata* ***X509****.*

Objašnjenja pojedinih polja X.509 certifikata (odozgo prema dolje):

1. Verzija – Moguće vrijednosti su v1, v2 i v3.
2. Serijski broj – Pozitivan cijeli broj koji je jedinstven unutar CA, a aplikacija koja ostvaruje CA brine se o ispunjenju ovih uvjeta.
3. Potpis – Identifikacija algoritma koji je korišten pri potpisivanju certifikata od strane CA.
4. Izdavač – Polje koje služi za identifikaciju izdavača certifikata, a ime organizacije koja se upiše u ovo polje mora biti javno registrirano ime organizacije, i u sklopu njega mora biti minimalno ime države izdavanja certifikata. Dozvoljeni su i drugi elementi koji pobliže definiraju organizaciju.
5. Period važenja (valjanosti) – U ovom polju se definira period valjanosti certifikata i u njemu su definirana dva datuma. To su datum početka valjanosti certifikata i datum prestanka valjanosti certifikata.
6. Subjekt – Ovo polje identificira entitet vezan sa javnim ključem. Za kvalificirani certifikat ovo polje mora imati vrijednost prepoznatljivog imena subjekta (definiranih u standardu X.500).
7. Informacija o javnom ključu subjekta – Ovo polje sadrži javni ključ subjekta i podatke o korištenom kriptografskom algoritmu.

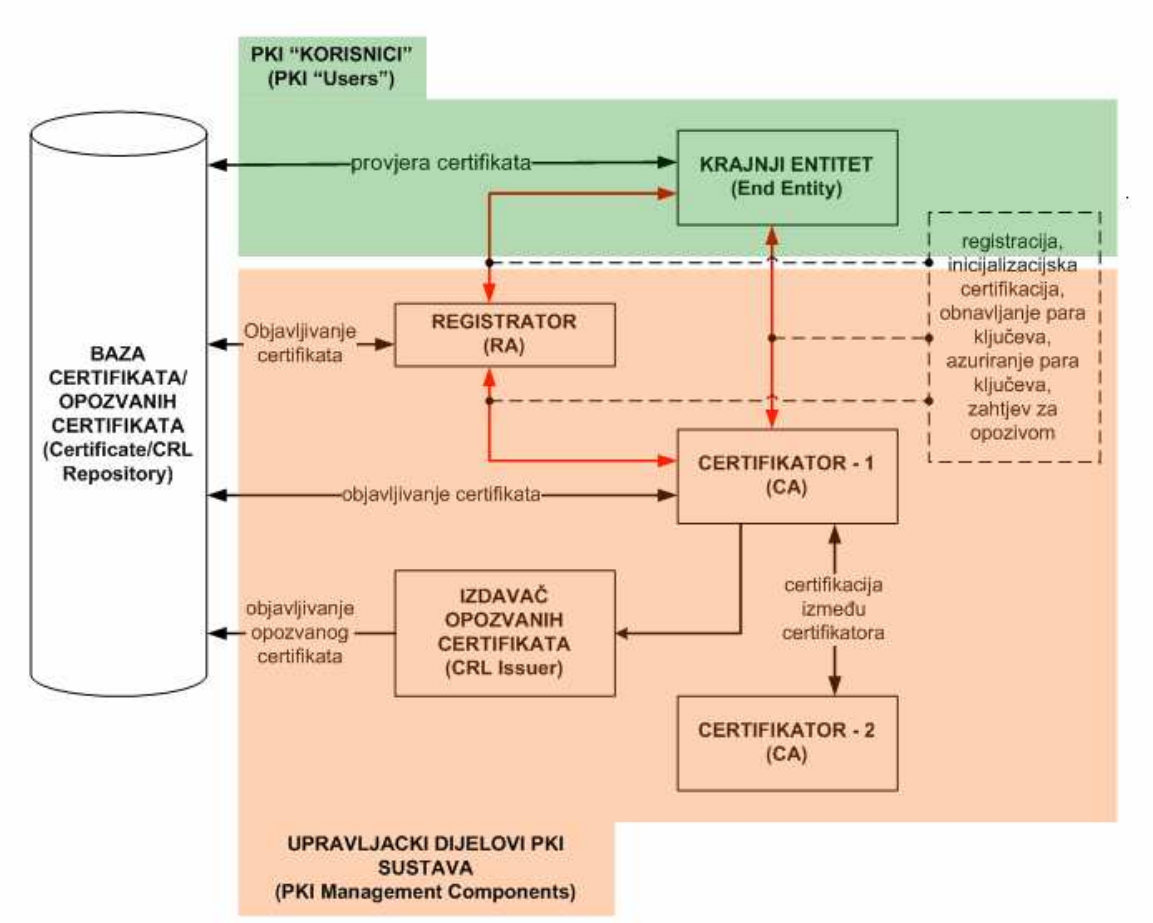
8. Jedinstveni ID izdavača – Ovo polje je opcionalno i RFC3280 ne preporučuje njegovo korištenje.
9. Jedinstveni ID subjekta – Ovo polje je također opcionalno i RFC3280 ne preporučuje njegovo korištenje.
10. Proširenje – Polje koje omogućuje proširenje, i opcionalno je.
11. Digitalni potpis – Digitalni potpis (prethodno opisana polja certifikata se digitalno potpišu) od strane CA.

3 Infrastruktura javnog ključa

Infrastruktura javnog ključa (PKI) složeni je sustav koji objedinjuje certifikate, certifikacijsku ustanovu (certifikator), bazu certifikata i opozvanih certifikata, korisnike certifikata, te sve njihove međusobne interakcije. Prije svega PKI je sustav koji omogućuje autentifikaciju. Koristeći simetričnu i asimetričnu kriptografiju osigura brojne usluge uključujući povjerljivost podataka, njihov integritet te upravljanje ključevima (*key managament*), odnosno certifikatima.

3.1 PKI arhitektura

Osnovne komponente PKI sustava **su krajnji entitet** ili korisnici PKI sustava, **certifikacijski centar** ili certifikator (engl. ***Certification Authority – CA***), **registracijski centar** ili registrator (engl. ***Registration Authority – RA***), **spremnik ili baza valjanih i opozvanih certifikata** (engl. ***Certificate/CRL Repository***), te **izdavač opozvanih certifikata** (engl. ***CRL Issuer***), ***slika 3.1***.



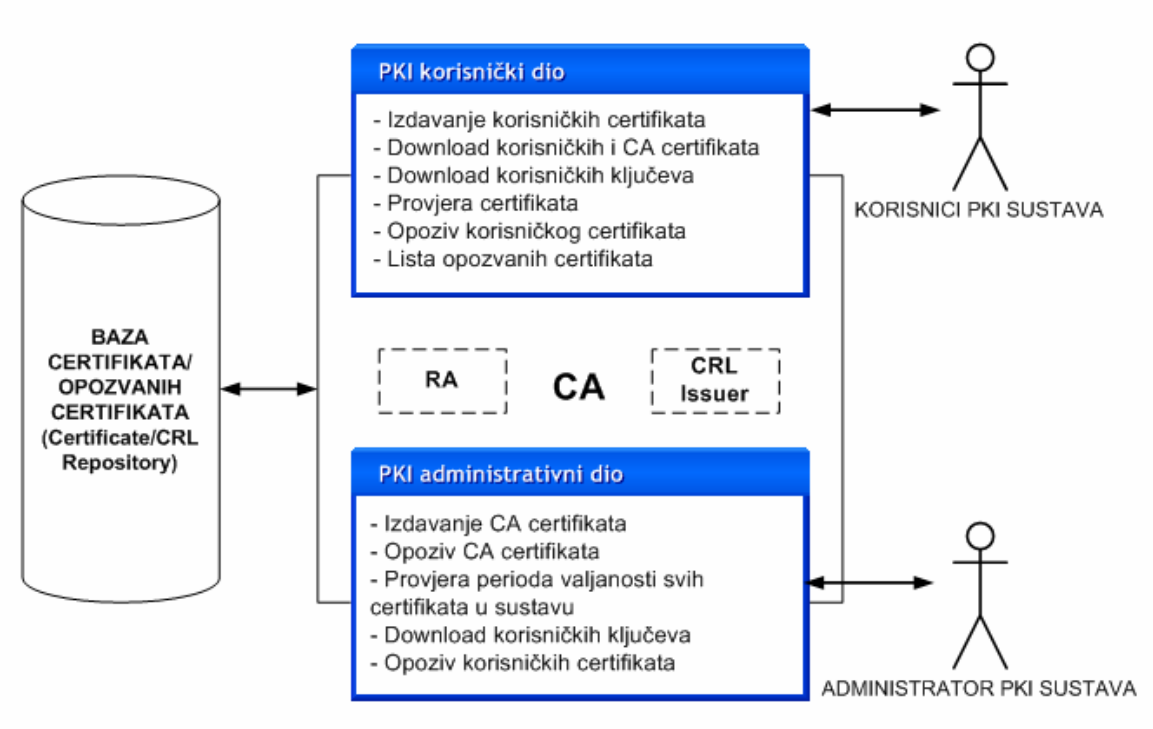
***Slika 3.1**: **PKIX** sustav, sustav infrastrukture javnog ključa temeljenog na **X.509**.*

Objašnjenje pojedinih komponenti:

1. Krajnji entitet – subjekti certifikata, a ponekad se zovu i krajnji korisnici, koji ne moraju biti fizičke ili pravne osobe već i uređaji kao što su serveri i routeri, zatim programi i procesi, odnosno sve što može biti identificirano imenom na certifikatu.
2. Certifikacijski centar (CA) – ustanova koja potpisuje i izdaje certifikate. Osnovne operacije certifikacijskog centra su izdavanje certifikata, njihovo obnavljanje i po potrebi njihov opoziv. CA svojim potpisom jamči ispravnost podataka u certifikatu. CA izravno ili preko registracijskog centra (RA) registrira krajnje entitete ili korisnike i verificira njihov identitet na odgovarajući način. CA obavlja ponekad i funkciju sigurnog pohranjivanja ključeva. On je izvor povjerenja u PKI, a povjerenje je osnova na kojoj se zasniva PKI.
3. Registracijski centar (RA) – opcionalna komponenta PKI sustava, a može biti i dio certifikacijskog centra. Kao što mu i samo ime kaže, njegova uloga je vezana za registriranje krajnjih entiteta, odnosno korisnika PKI sustava. Osim ove uloge, RA može provjeravati posjeduje li korisnik privatni ključ koji odgovara javnom ključu koji će se nalaziti na certifikatu, ili može sam generirati par ključeva. On može biti i posrednik između korisnika certifikacijskog centra prilikom informiranja o kompromitiranju privatnog ključa. Sve ove funkcije su obavezni dio PKI sustava, te ako ih ne obavlja RA mora ih obavljati CA. RA je također i korisnik PKI sustava te ima svoj javni ključ i certifikat. RA ne smije obavljati funkcije izdavanja i opoziva certifikata.
4. Spremište ili baza certifikata – predstavlja sustav ili skup distribuiranih sustava koje pohranjuju certifikate i listu opozvanih certifikata, dostupnih svim unutarnjim ali i vanjskim korisnicima PKI sustava koji koriste certifikate za identifikaciju.
5. Izdavač opozvanih certifikata – komponenta PKI sustava koja izdaje listu opozvanih certifikata. Certifikati se izdaju s određenim periodom valjanosti. Certifikati iz raznih razloga mogu postati nevažeći i prije isteka tog perioda. Za primjer se može uzeti kompromitiranje privatnog ključa. Svaki opozvani certifikat identificiran je svojim serijskim brojem u listi opozvanih certifikata. Lista opozvanih certifikata je javno dostupna svima.

4 Programsko ostvarenje PKI sustava

U praktičnom dijelu seminarskog rada ostvaren je jedan općeniti PKI sustav. Iako se u praksi PKI realizira za konkretan sustav, a njegove osobine, složenost i cijena ovise o samom sustavu i primjeni, naglasak u ovom seminarskom radu stavljen je na prikazivanje i realizaciju glavnih usluga koje pruža PKI. Treba istaknuti da se taj sustav vrlo lako može prilagoditi stvarnim potrebama i integrirati u neki realni sustav.
PKI sustav je programski ostvaren u programskom jeziku Java, koristeći Java Servlet tehnologiju koja omogućuje integraciju Jave s web tehnologijama. Sustav koristi i MySQL bazu podataka u kojoj se čuvaju certifikati i drugi podaci potrebni za rad sustava, te dva besplatna Java paketa Bouncy Castle Crypto paket u verziji 1.27 i MultyPartRequest paket u verziji 1.30. Cijeli je sustav izgrađen na *open source* tehnologiji.
Zbog jednostavnije izvedbe sustava, registracijski centar i izdavač opozvanih certifikata su ostvareni u sklopu certifikacijskog centra. Ostvareni PKI sustav se sastoji od dvije cjeline, a to su **PKI administracijski dio** i **PKI korisnički dio** (***Slika 4.1***).



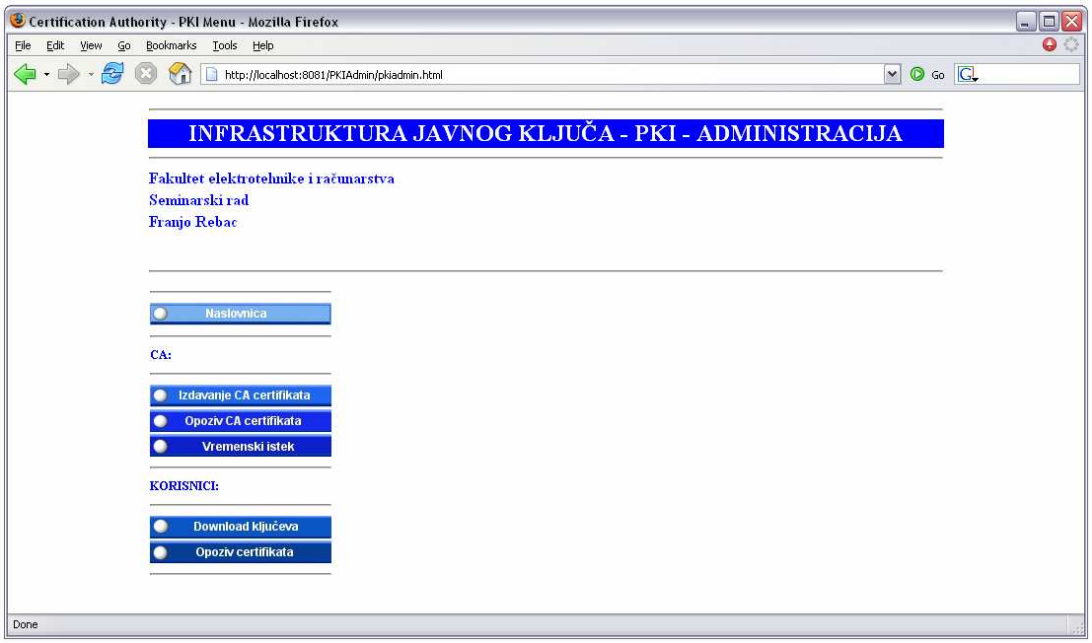
Slika 4.1: *Ostvareni PKI sustav.*

Uslugama PKI sustava kao i administracijskom dijelu se pristupa preko web preglednika. Pristup administracijskom dijelu moguć je samo lokalno, zbog sigurnosnih razloga. Svako neregularno stanje sustava se bilježi u bazi podataka, s informacijama o vremenu kad se dogodilo, s koje je IP adrese došao zahtjev, u kojem programskom modulu je detektirano neregularno stanje, kao i opis neregularnog stanja.

Kriptografski algoritmi koje koriste sustav su SHA1 za dobivanje sažetka, te RSA za digitalno potpisivanje certifikata. Prije izdavanja bilo kojeg certifikata (korisničkog ili CA certifikata), sustav generira par ključeva (javni i privatni ključ). Duljina ključa namijenjenog za CA iznosi 2048 bita, a duljina korisničkih ključeva 1024 bita. Period valjanosti CA certifikata iznosi deset godina, dok kod korisničkih on iznosi dvije godine. Svakom korisniku prilikom slanja zahtjeva za izdavanje certifikata nudi se opcija za izbor načina preuzimanja privatnog ključa (osobno preuzimanje ili download ključeva). Korisnički privatni i javni ključ sprema se u bazu podataka u PKCS#12 formatu, koji je zaštićen lozinkom koju korisnik unosi tijekom ispunjavanja zahtjeva za certifikatom. Lozinka je poznata samo korisniku i nigdje se ne čuva unutar sustava (nije poznata ni administratoru sustava).

4.1 PKI administracija

Administrativni dio sustava omogućava administraciju certifikacijskog centra, te administraciju vezanu za krajnje korisnike PKI sustava. PKI administraciji se iz sigurnosnih razloga može pristupiti samo lokalno. U slučaju stvarne ugradnje unutar realnog sustava, potrebne su minimalne nadogradnje programa kako bi se omogućio pristup administraciji samo ovlaštenim osobama (autentifikacija).



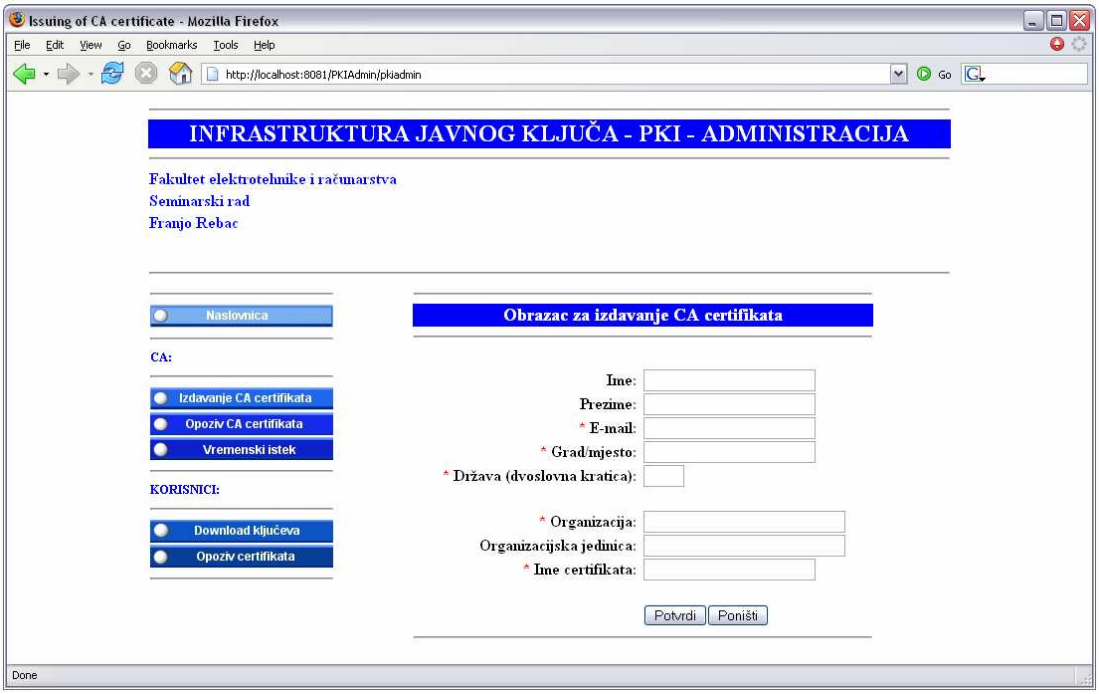
Slika 4.2: *Izgled programskog sučelja PKI administracijskog dijela.*

Funkcije koje obavlja administrativni dio su:

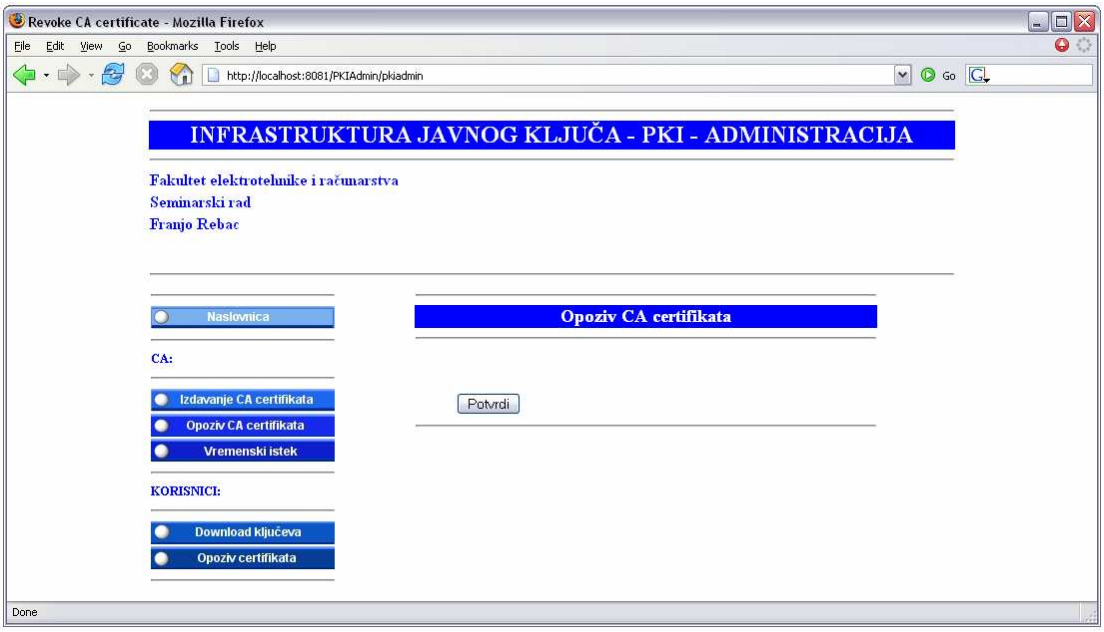
1. Izdavanje CA certifikata – Administrator popunjava obrazac za izdavanje CA certifikata s informacijama prikazanim na ***slici 4.3*** (crvenom zvjezdicom su označeni podaci koji se obvezno moraju unijeti). Poslije slanja zahtjeva za CA certifikatom, sustav generira javni i privatni ključ duljine 2048 bita. Nakon toga

se generira certifikat, i direktno sprema u bazu podataka, zajedno s privatnim ključem, u posebnu tablicu (relaciju baze podataka). Unutar PKI sustava može postojati samo jedan valjani CA certifikat.

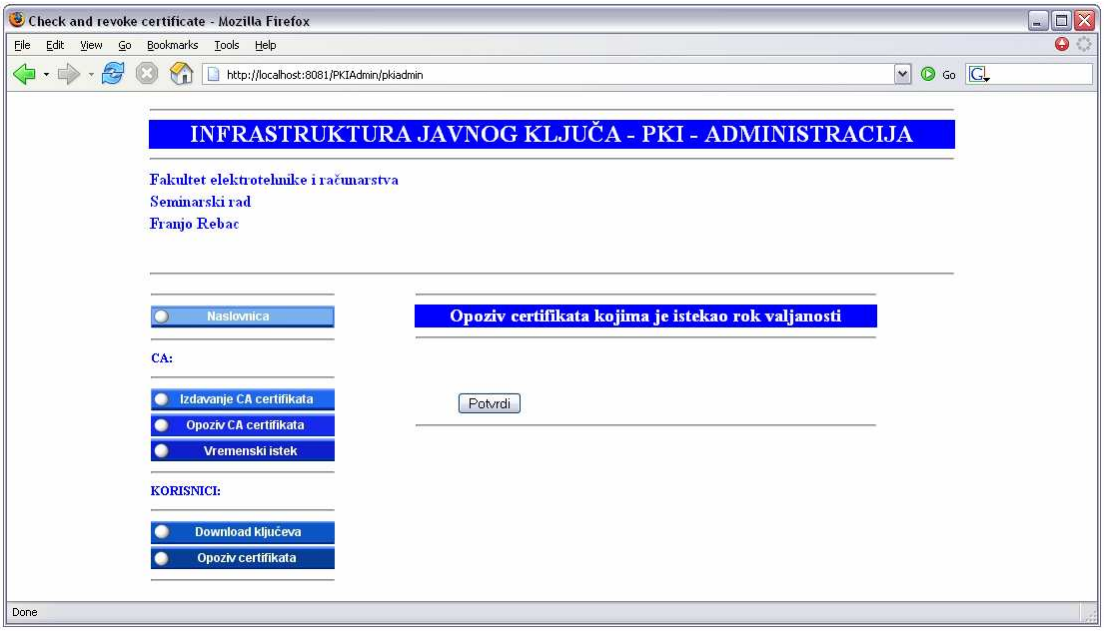
2. Opoziv CA certifikata – Opozivom CA certifikata (***slika 4.4***), automatski se opozivaju i svi certifikati unutar PKI sustava. Opozvani CA certifikat kao i sve certifikate koje je CA izdao s tim certifikatom sustav automatski stavlja u listu opozvanih certifikata.
3. Vremenski istek – Ovo je funkcija (***slika 4.5***) koja provjerava period valjanosti svih certifikata u sustavu (provjerava i CA certifikat), te one certifikate kojima je istekao period valjanosti opoziva i stavlja u listu opozvanih certifikata.
4. Download korisničkih ključeva – Ova opcija (***slika 4.6***) se koristi ukoliko je korisnik PKI sustava, prilikom zahtjeva za izdavanje certifikata, izabrao opciju osobnog preuzimanja para ključeva. Ključevi (javni i privatni) čuvaju se u formatu certifikata PKCS#12, koji je zaštićen korisničkom lozinkom, te se prilikom njegovog downloada stvara datoteka s ekstenzijom *pfx*.
5. Opoziv korisničkog certifikata – Ova opcija (***slika 4.7***) koristi se ukoliko je došlo do kompromitiranja certifikata, a korisnik, vlasnik kompromitiranog certifikata, iz nekih razloga nije opozvao svoj certifikat (npr. korisnik je zaboravio lozinku svog certifikata u kojem se čuva privatni i javni ključ te ne može opozvati certifikat - da bi opozvao certifikat u PKI korisničkom dijelu sustava, korisnik mora između ostalog unijeti i lozinku certifikata).



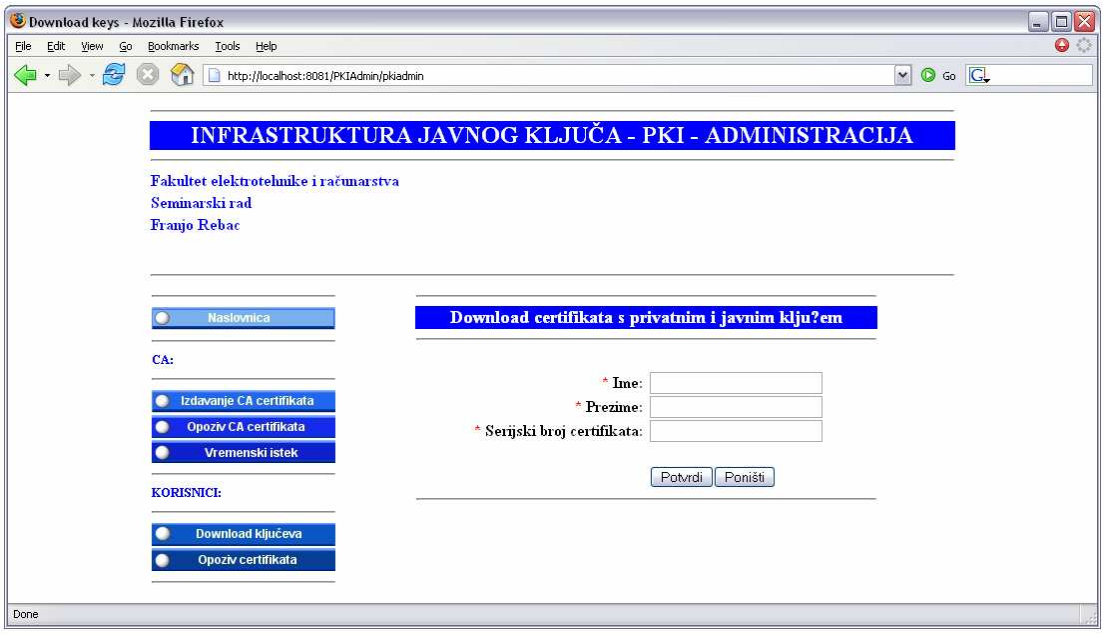
Slika 4.3*: Zahtjev za izdavanje CA certifikata.*



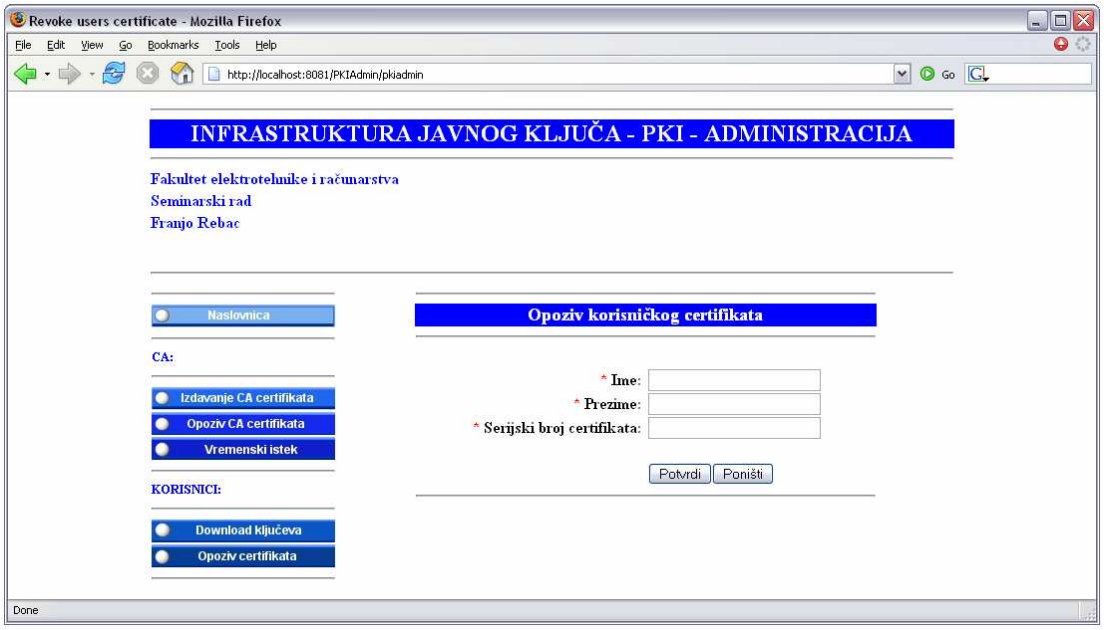
***Slika 4.4**: Opoziv CA certifikata.*



***Slika 4.5**: Provjera perioda valjanosti svih certifikata u sustavu.*



***Slika 4.6**: Download korisničkog certifikata s privatnim i javnim ključem.*

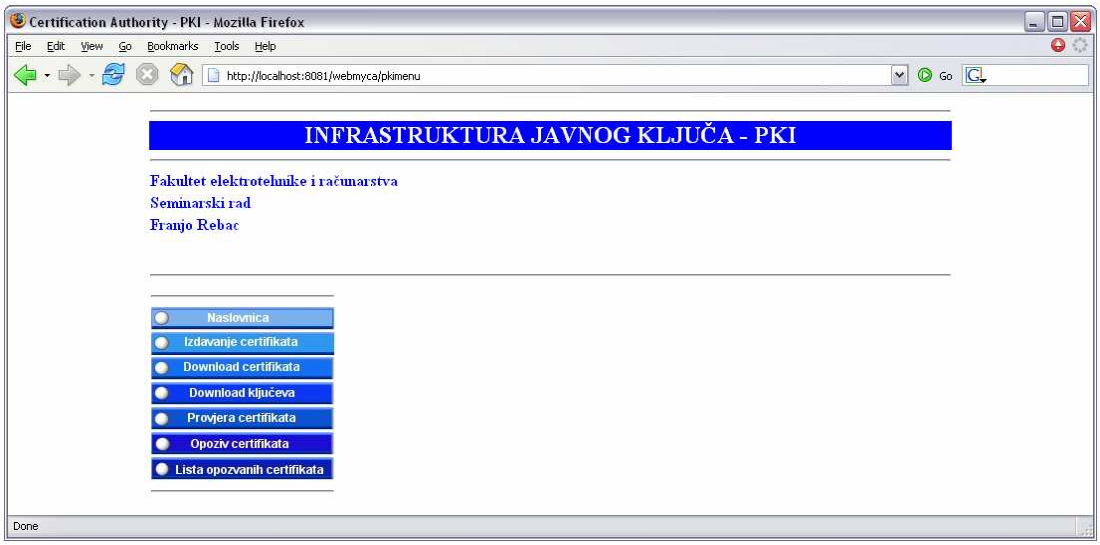


***Slika 4.7**: Opoziv korisničkog certifikata.*

Prilikom uporabe bilo koje opcije PKI administratorskog dijela, sustav obavještava administratora o rezultatima izvršavanja, s obavijesti je li naredba uspjela ili ne, te razlozima neuspjeha operacije. Sva neregularna stanja zapisuju se u posebnu relaciju baze podataka.

4.2 PKI korisnički dio

Korisnički dio PKI sustava pruža usluge korisnicima sustava. Preko njega se korisniku omogućuje slanje zahtjeva za izdavanje certifikata, download certifikata (ne samo svog nego i certifikata i drugih korisnika sustava, kao i CA certifikata), download svog certifikata u kojem se čuva javni i privatni ključ, provjera valjanosti certifikata, opoziva svog certifikata, te prikaz liste opozvanih certifikata.

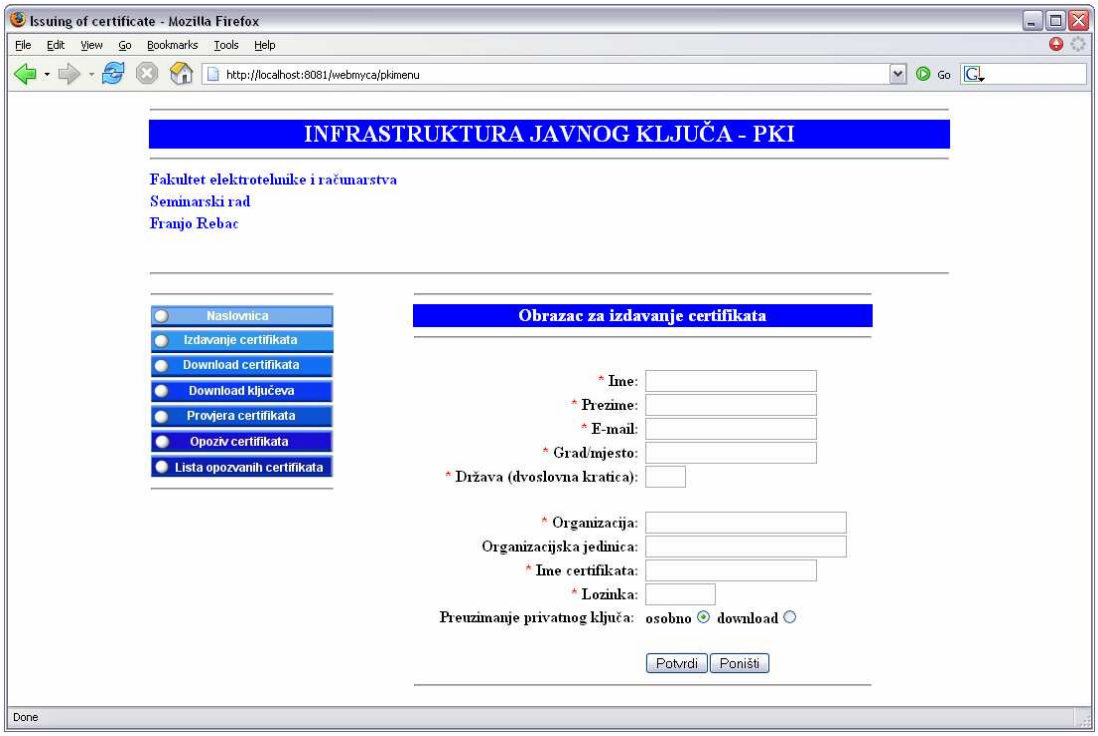


***Slika 4.8**: Izgled programskog sučelja PKI korisničkog dijela.*

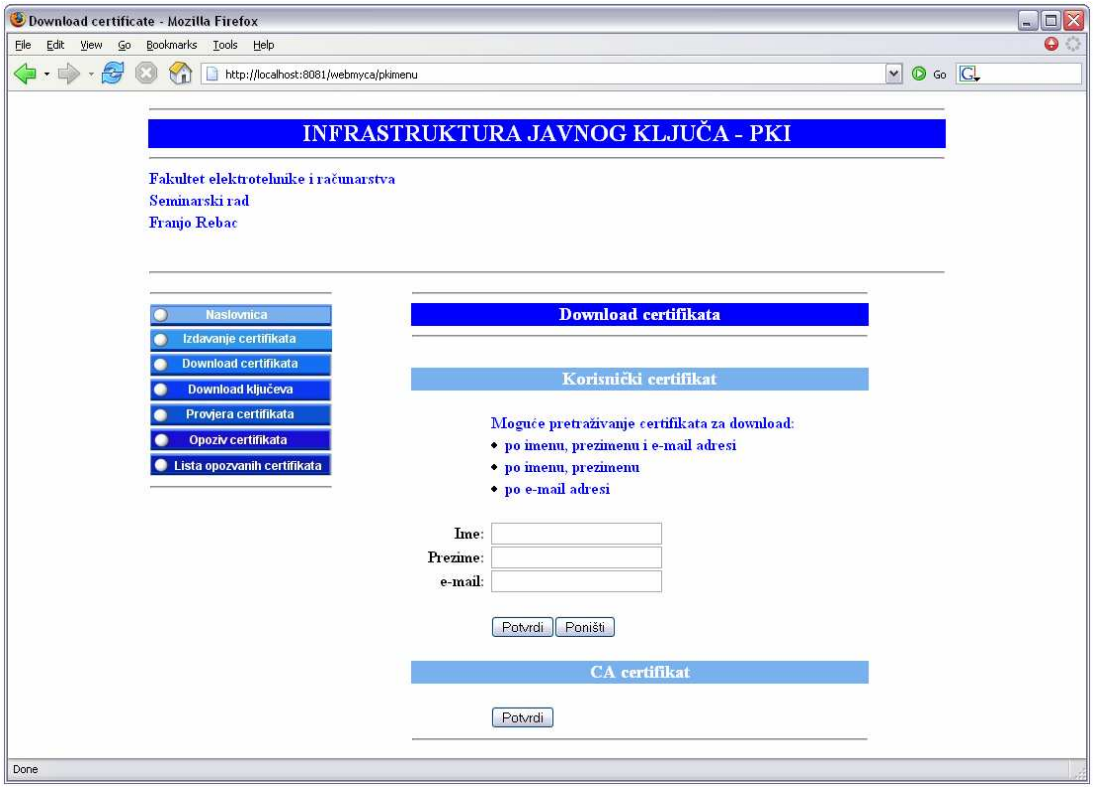
Funkcije koje obavlja korisnički dio PKI sustava:

1. Izdavanje certifikata – Korisnik popunjava zahtjev za izdavanje certifikata (***slika 4.9***, gdje su crvenom zvjezdicom označene informacije koje korisnik obvezno mora unijeti). Nakon uspješnog slanja zahtjeva, za korisnika sustav generira par ključeva duljine 1024 bita, stvara certifikat i pohranjuje ga u određenu relaciju baze podataka. Osim toga, sustav kreira i certifikat u kojem se nalazi javni i privatni ključ, u formatu PKCS#12, zaštićen lozinkom koju je korisnik unio tijekom popunjavanja zahtjeva, te ga također sprema u bazu podataka. Korisnik je prilikom popunjavanja zahtjeva za certifikatom morao izabrati i opciju preuzimanja para ključeva. Dozvoljene opcije su osobno preuzimanje (ako korisnik drugačije ne izabere, ta se opcija podrazumijeva) i mogućnost downloada ključeva unutar certifikata u formatu PKCS#12. Ukoliko korisnik izabere prvu opciju, sustav će mu zabraniti download ključeva, te korisnik mora doći osobno kod administratora sustava i podići certifikat s javnim i privatnim ključem.
2. Download certifikata – Korisnik ima na izboru dvije opcije (***slika 4.10***), a to su download korisničkih certifikata i download CA certifikata. Za korisničke certifikate na raspolaganju mu stoji pretraživanje po imenu, prezimenu i e-mail adresi, samo po imenu i prezimenu, te samo po e-mail adresi osobe čiji certifikat želi downloadirati. Certifikati su Base64 kodirani DER kodirani X.509 certifikati, i imaju *cer* ekstenziju datoteke.

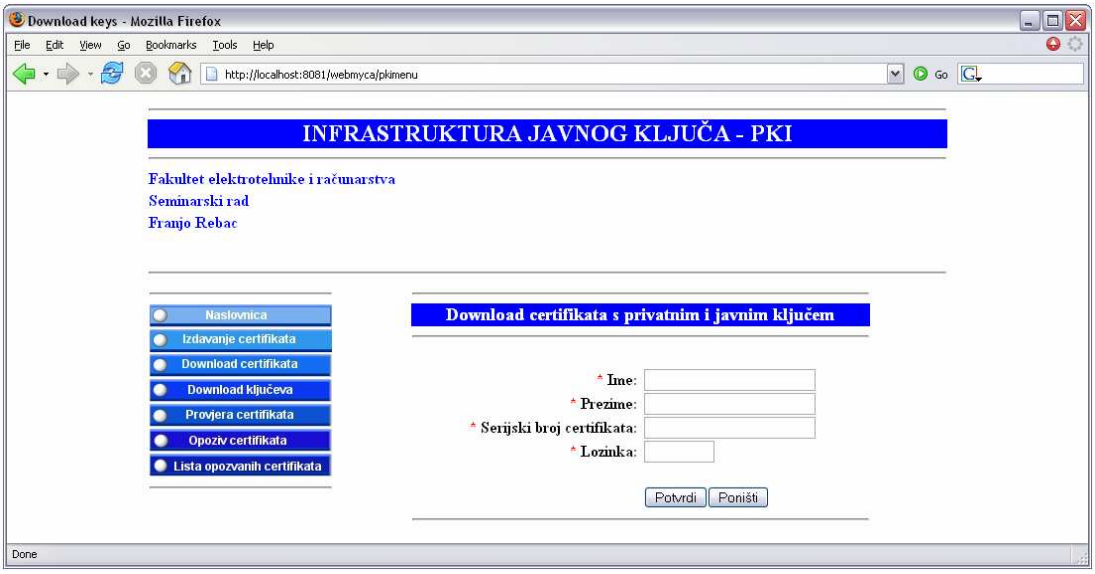
3. Download certifikata s ključevima – Ovu opciju moguće je koristiti ako je korisnik izabrao mogućnost downloada ključeva, prilikom popunjavanja zahtjeva za izdavanje certifikata. Da bi korisnik mogao downloadirati certifikat s privatnim i javnim ključem, od njega se traži unos lozinke koju je koristio prilikom popunjavanja zahtjeva za izdavanje certifikata. Pokušaj zlouporabe ove opcije, sustav bilježi u bazu podataka.
4. Provjera certifikata – Korisniku se omogućava provjera određenog certifikata, na principu njegovog uploada u PKI sustav (***slika 4.12***). Korisnik označi određeni certifikat na svom računalu i uploada ga, sustav primi certifikat, provjeri ga (provjera je li uploadairna datoteka u opće certifikat, je li certifikat izdao ovaj CA, provjera perioda valjanosti, provjera je li u listi opozvanih certifikata, provjera njegove općenite valjanosti kao npr. je li korišten odgovarajući algoritam potpisivanja itd.). Sustav obavještava korisnika o rezultatu provjere. Zbog sigurnosnih razloga, maksimalna veličina certifikata koji se provjerava može biti 5 kB. Sustav uopće neće uploadirati datoteke veće od ove vrijednosti. Pokušaj zlouporabe ove opcije, sustav bilježi u bazu podataka.
5. Opoziv certifikata – Korisnik može opozvati svoj certifikat (***slika 4.13***), ako je on iz nekih razloga kompromitiran (npr. kompromitiranost privatnog ključa). Da bi mogao opozvati svoj certifikat, korisnik mora znati lozinku koju je koristio prilikom slanja zahtjeva za izdavanjem certifikata. Kao i u prethodnoj opciji, svaki pokušaj zlouporabe, sustav bilježi u bazu podataka.
6. Lista opozvanih certifikata – Ova opcija (***slika 4.14***) omogućuje prikaz liste svih opozvanih certifikata, s prikazom njihovih serijskih brojeva, datuma i vremena izdavanja, do kada su trebali vrijediti te kad su opozvani.



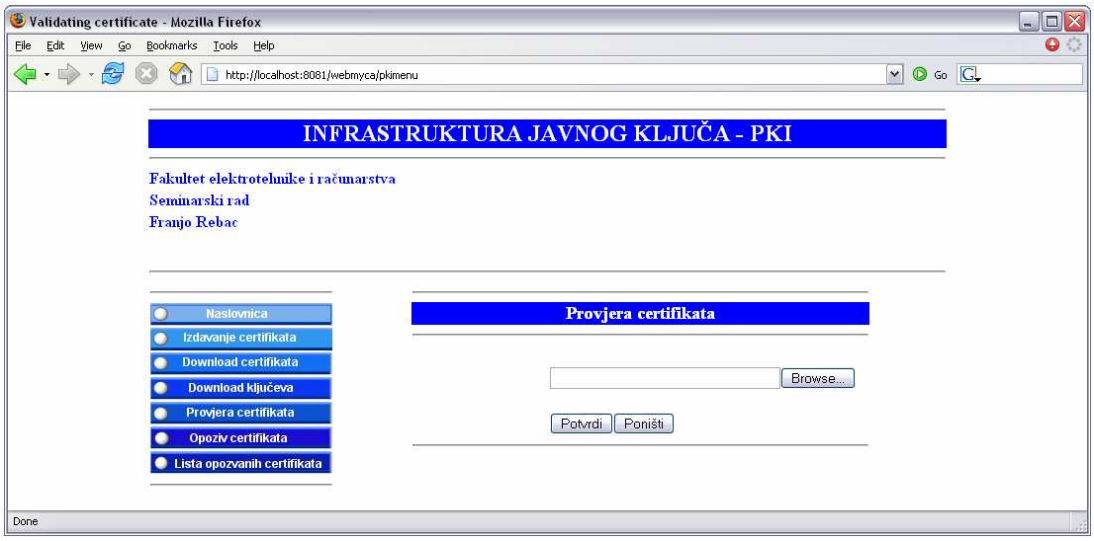
Slika 4.9*: Zahtjev za izdavanje korisničkog certifikata.*



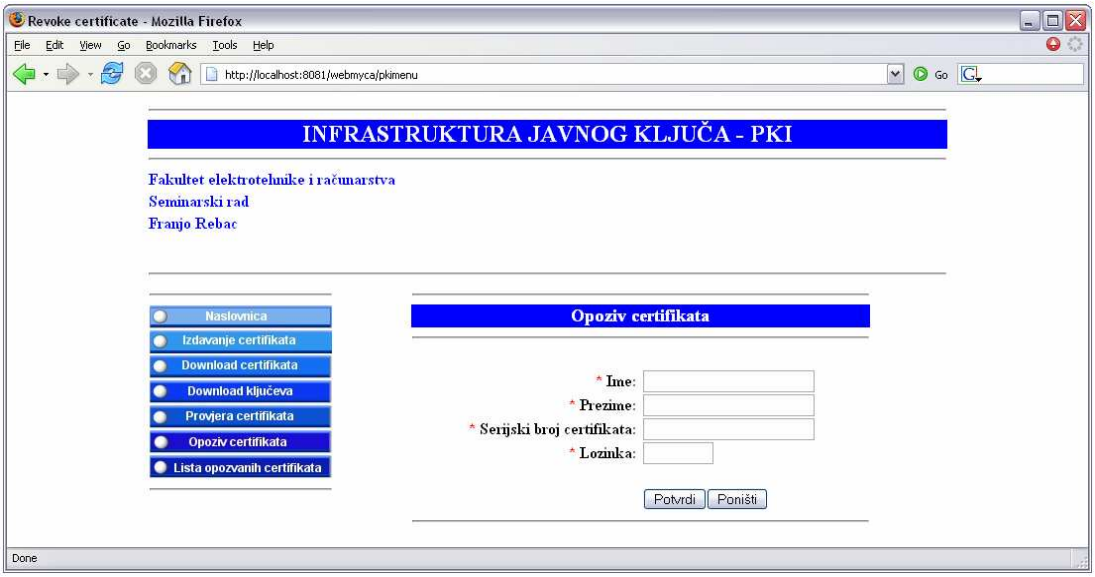
***Slika 4.10**: Download certifikata.*



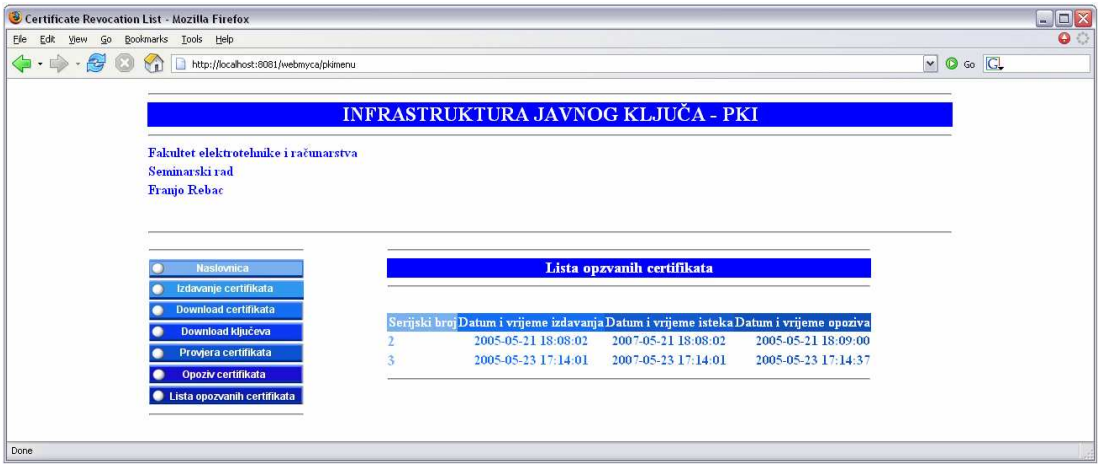
***Slika 4.11**: Download certifikata s privatnim i javnim ključem.*



***Slika 4.12**: Provjera certifikata.*



***Slika 4.13**: Opoziv korisničkog certifikata.*

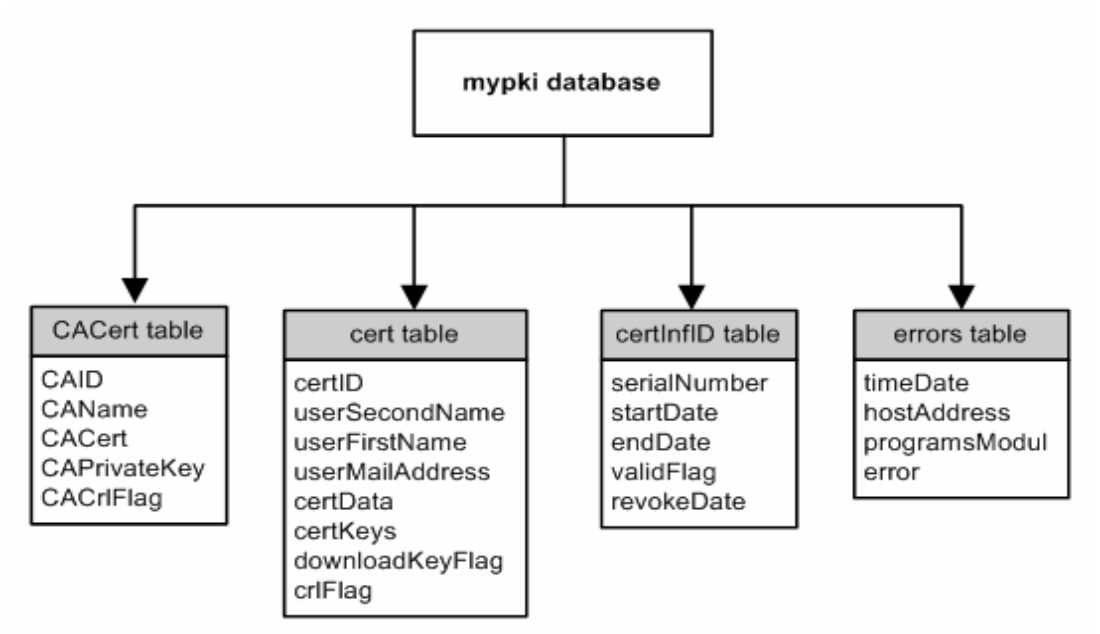


***Slika 4.14**: Lista opozvanih certifikata.*

Kao i u slučaju PKI administrativnog dijela, sustav obavještava korisnika o svim opcijama koje koristi, te jesu li uspjele ili nisu, te razlog neuspjeha. Sve nedopuštena stanja sustav bilježi u za to predviđenu relaciju unutar baze podataka, što je prikazano u sljedećem poglavlju o PKI bazi podataka.

4.3 PKI baza podataka

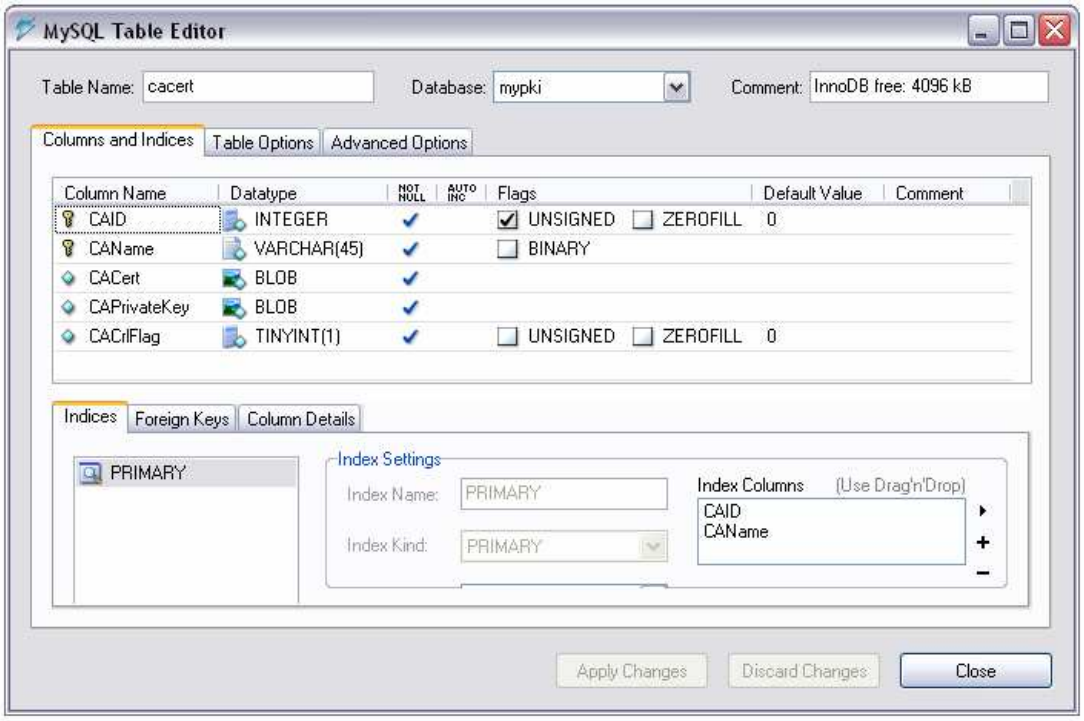
Baza podataka PKI sustava naziva se ***mypki***. Sadrži četiri relacije (tablice): ***CACert***, ***cert***, ***certInfID*** i ***errors*** (***slika 4.15***).



***Slika 4.15**: Prikaz baze podataka s relacijama i atributima unutar relacija.*

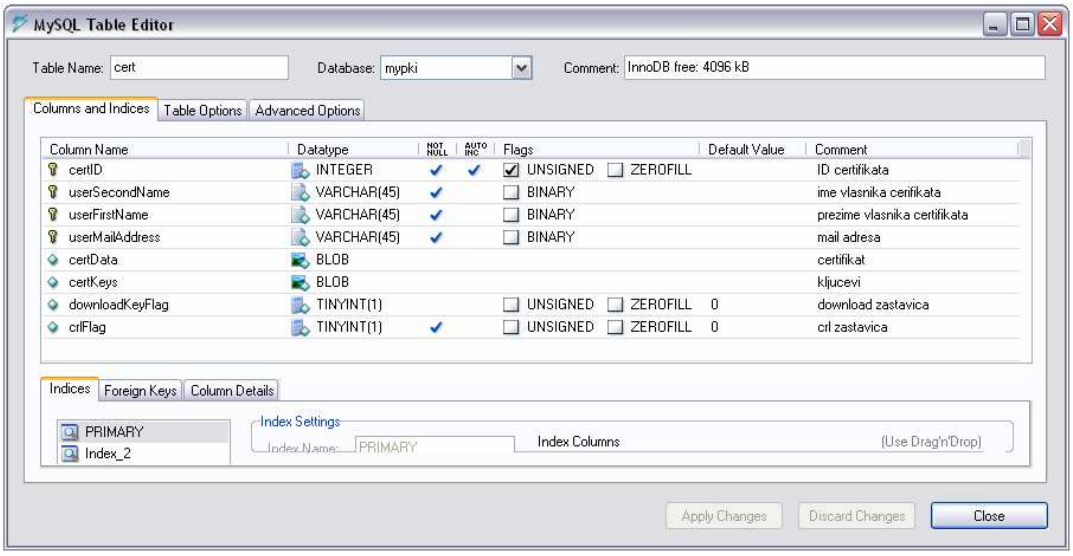
Objašnjenje pojedine relacije *mypki* baze:

1. Relacija *CACert* – U ovu relaciju (***slika 4.16***), spremaju se podaci o CA certifikatu. Ti podaci su: *CAID* – serijski broj certifikata, *CAName* – ime certifikata, *CACert* – certifikat, *CAPrivateKey* – privatni ključ CA te *CACrlFlag* – indikator opoziva CA certifikata (vrijednost 1 znači da je certifikat opozvan, a 0 da nije opozvan). U ovoj relaciji smije biti samo jedan valjani certifikat (*CACrlFlag* za taj certifikat ima vrijednost 0). Primarni ključ relacije su atributi *CAID* i *CAName*.



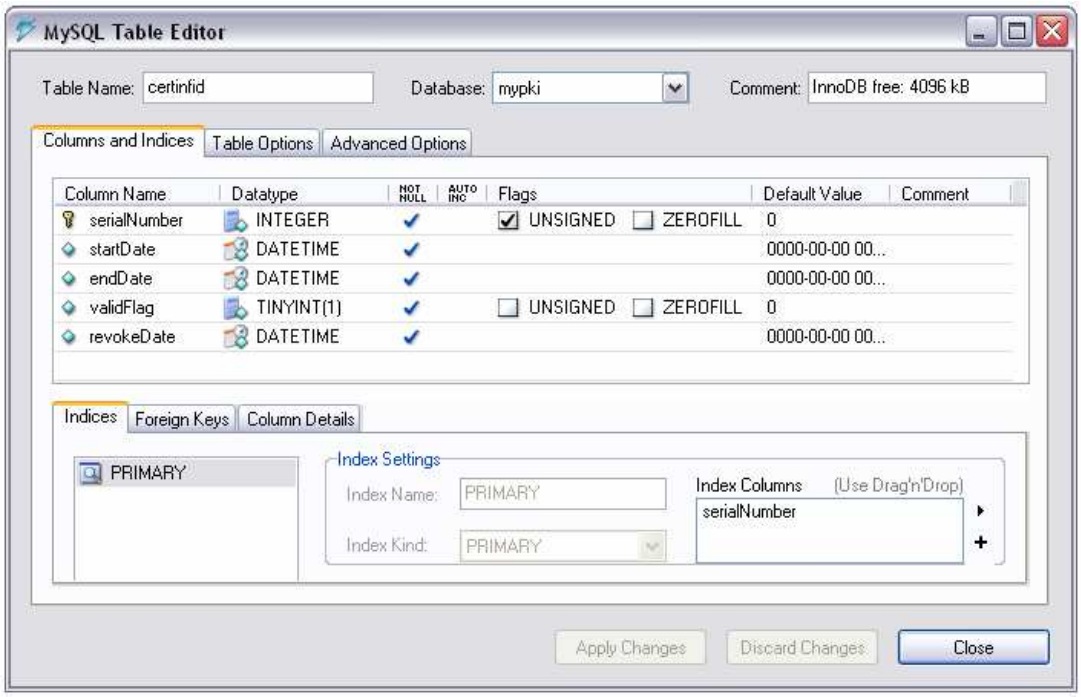
Slika 4.16*: Relacija CACert.*

2. Relacija *cert* – U relaciji *cert* čuvaju se podaci o korisničkim certifikatima. Ti podaci su *certID* – serijski broj certifikata, *userSecondName* – prezime korisnika, *userFirstName* – ime korisnika, *userMailAddress* – korisnikova e-mail adresa, *certData* – korisnikov certifikat, *certKeys* – certifikat u kojem se čuva korisnikov privatni i javni ključ, *downloadKeyFlag* – indikator mogućnosti downloadiranja certifikata s privatnim i javnim ključem (vrijednost 1 znači da je omogućen download, a 0 da nije moguć), *crlFlag* – indikator opoziva certifikata. Primarni ključ relacije su atributi *certID*, *userSecondName*, *userFirstName* i *userMailAddress*.



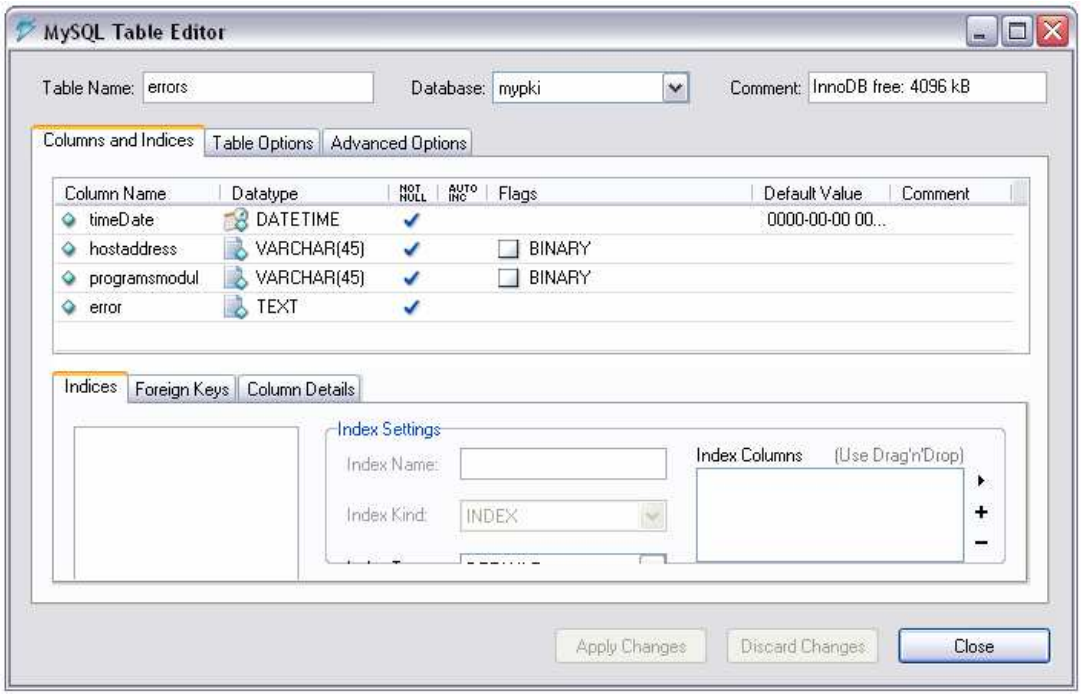
***Slika 4.17**: Relacija cert.*

3. Relacija *certInfID* – U ovoj relaciji nalaze se informacije o svim certifikatima (korisnički ili CA) koji su izdani u sustavu, bilo opozvani ili oni koji još vrijede. Svi opozvani certifikati u ovoj relaciji predstavljaju listu opozvanih certifikata. Podaci u relaciji su: *serialNumber* – serijski broj certifikata, *startDate* – datum kreiranja certifikata, *endDate* – datum prestanka valjanosti certifikata, *validFlag* – indikator opoziva certifikata, te *revokeDate* – datum opoziva certifikata. Ključ relacije je atribut *serialNumber*.



***Slika 4.18**: Relacija certInfID.*

4. Relacija *errors* – U ovoj relaciji bilježe se sve nepredviđene pogreške sustava kao i svi pokušaji zlouporabe i kompromitiranja sustava (***slika 4.19***). Podaci u relaciji su: *timeDate* – vrijeme i datum događanja pogreške nedozvoljenog stanja, *hostAddress* – IP adresa korisnika koji je izazvao to stanje, *programsModul* – programski modul u kojem je nastalo nedozvoljeno stanje te *error* – opis nedozvoljenog stanja.



Slika 4.19*: Relacija errors.*

5 Zaključak

Treba naglasiti da se prije ostvarenja nekog PKI sustava, treba pažljivo razmotriti koja je njegova uloga, u kojem okruženju će djelovati, koje su stvarne potrebe sustava, isplativost njegovog ostvarenja, kakvu će sigurnost i povjerenje imati takav sustav. Tek poslije razmatranja svih ovih aspekata treba krenuti u konkretno ostvarenje koje će zadovoljiti ove potrebe. U ovom seminarskom radu cilj je prvenstveno bio prikazati mogućnosti i funkcije koje jedan PKI, koji djeluje u nekom konkretnom sustavu, mora imati. Sam rad ostvarenog PKI-a je zamišljen u nekom zatvorenom sustavu, kao dodatna usluga korisnicima tog sustava, u cilju njihove sigurne međusobne komunikacije. Na taj način sustav je sigurniji (pristup njegovim uslugama imaju samo registrirani korisnici) i lakše se može kontrolirati, a veće je i samo povjerenje korisnika u njega. Daljnji koraci nadogradnje ovog PKI-a, u smislu povećanja njegove sigurnosti, bi bila kriptografska zaštita baze podataka, kao i sigurna internet komunikacija preko SSL protokola.

6 Literatura

[1] Budin, L.: Predavanja iz predmeta Operacijski sustavi 2, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, Zagreb 2003.

[2] Golub, M., bilješke s predavanja i auditornih vježbi iz Operacijskih sustava 2, Zagreb 2004.

[3] Mrdović, S.: Izgradnja infrastrukture javnih ključeva (PKI), Elektrotehnički fakultet u Sarajevu, Sarajevo 2004,
http*://www.etf.unsa.ba/~smrdovic/publications/Magistarski-Mrdovic.pdf*

[4] Shashi K., Patricia L., Steve L.: PKI Basics - A Technical Perspective, November 2002, *http://www.pkiforum.org/pdfs/PKI_Basics-A_technical_perspective.pdf*

[5] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, *http://rfc.sunsite.dk/rfc/rfc3280.html*

[6] Java 2 SDK, v 1.4 Security Documentation,
http://java.sun.com/j2se/1.4.2/docs/guide/security/index.html

7 Dodaci

7.1 Dodatak A: Instalacija ostvarenog PKI sustava

Uputa za instalaciju PKI sustava, kao i priloženi instalacijski programi namijenjeni su za operacijski sustav Windows XP. Instalacija za druge operacijske sustave je ista, uz instalacijske programe namijenjene za taj sustav (Java, MySql itd.), te umjesto pokretanja *createDbMypki.bat* datoteke treba ručno izvršiti naredbe iz komandne linije, napisane u toj datoteci, za kreiranje baze podataka PKI sustava i potrebnih relacije.

Preduvjeti za instalaciju:

1. Instalirana Java jdk 1.4 (ili novija verzija npr. 1.5).
2. Instalirana MySql Server 4.1 (ili novija verzija).
3. Instaliran MySql jdbc driver za Javu (smjestiti npr. mysql-connector-java-3.1.6-bin.jar jar arhivu u poddirektorij *ext* java instalacije, npr. *C:\Program Files\Java\jdk1.5.0_02\jre\lib\ext*).
4. Instaliran Apache Tomcat Server (npr. verzija 5.5.9), koji je potreban za izvršavanje java servleta.
5. Postavljen Bouncy Castle Cryptography paket (npr. bcprov-jdk15-127.jar) u "lib\ext" direktoriju Java instalacije.

Za instalaciju PKI sustava, preporučeni redoslijed instalacije je: instaliranje baze podataka, instalacija PKI administratorskog dijela, instalacija PKI korisničkog dijela sustava.
Poslije instalacije Jave i MySql-a, potrebno je namjestiti *environment* varijablu *path* na odgovarajući način (u *environment* varijablu *path, System Propertis -> Advanced -> Environment Variables -> path,* dodati put do *bin* direktorija Java i MySql instalacije)

Instalacija baze podataka:
Pokrenuti datoteku ***createDbMypki.bat***. U istom direktoriju, u kojem se pokreće ova datoteka treba biti smještena datoteka ***mypki.sql***. Ukoliko je za MySql potrebna lozinka, u *createDbMypki.bat* datoteci je potrebno umjesto *mysqladmin -u root create mypki* naredbe zapisati *mysqladmin -u root -p create mypki* te unijeti odgovarajuću lozinku, a u konfiguracijskoj datoteci *pki.ini,* administratorskog i korisničkog dijela unijeti za parametar *dbPassword* odgovarajuću lozinku (datoteka *pki.ini* se nalazi u WEB-INF direktoriju PKI administratorskog i korisničkog dijela).

Instalacija PKI administratorskog dijela:
Kopirati ***PKIAdmin*** direktorij (u njemu se nalazi poddirektoriji WEB-INF i *pki_admin_menu_slike* te html datoteka *pkiadmin.html*) u direktorij *webapps* Apache Tomcat servera (npr. *C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps\webmyca*). Program se poziva iz web preglednika, unosom url-a: ***http://localhost:8081/PKIAdmin/pkiadmin.html***. U ovom url-u umjesto 8081 stavite onaj broj porta na kojem radi vaš Apache Tomcat server (broj porta koji ste unijeli pri instalaciji Apache Tomcat servera).

Instalacija PKI korisničkog dijela:

Na sličan način kao i u administratorskom dijelu, kopirati direktorij ***webmyca*** (u njemu se nalazi poddirektoriji WEB-INF i *menu_slike* te html datoteka *pkimenu.html*) u direktorij *webapps* Apache Tomcat servera. Program se poziva iz web preglednika, unosom url-a: ***http://localhost:8081/webmyca/pkimenu.html***, s tim da vrijedi ista opaska za broj porta u url-u kao i za administratorski dio.

7.2 Dodatak B: Primjena certifikata u Mozilli Thunderbirdu i S/MIME protokolu

Nakon instaliranja PKI sustava, potrebno je u administratorskom dijelu izdati CA certifikat. Nakon toga, u korisničkom dijelu možete izdati svoj korisnički certifikat i downloadirati certifikat s privatnim i javnim ključem u PKCS#12 formatu (opcija *Download ključeva*, a downloadirani certifikat imat će ekstenziju *pfx*), te downloadirati CA certifikat (opcija *Download certifikata – CA certifikat*).

U Mozilli Thunderbirdu u izborniku *Tools -> Options -> Advanced -> Certificates* izabrati opciju *Manage certificates*. Nakon ovog koraka, otvorit će se prozor *Certificate Manager*. U izborniku izabrati *Authorities*, zatim kliknuti na *Import*, i izabrati datoteku CA certifikata PKI sustava. Nakon toga u izborniku prozora *Certificate Manager* izabrati opciju *Your Certificate, Import,* te izabrati vaš certifikat s privatnim i javnim ključem i unijeti lozinku certifikata.

Poslije ovih koraka, u izborniku *Tools -> Account Settings* izabrati opciju *Security*, za vašu e-mail adresu. Za digitalno potpisivanje elektroničke pošte je potrebno pod *Digital Signing*, označiti svoj certifikat, kao i za kriptiranje pošte pod *Encryption* opcijom.

Tijekom slanja poruke, za njezino digitalno potpisivanje je potrebno je izabrati opciju S/MIME -> *Digitally Sign This Message*, a za njezino kriptiranje opciju S/MIME -> *Encrypt This Message*.