Univerzitet u Sarajevu

ELEKTROTEHNIČKI FAKULTET U SARAJEVU

Saša Mrdović

IZGRADNJA INFRASTRUKTURE JAVNIH KLJUČEVA (PKI)

(Magistarski rad)

Sarajevo, juli 2004.

Rad je izrađen na Elektrotehničkom fakultetu u Sarajevu.

Mentor: Akademik red. prof. dr Branislava Peruničić., dipl.el.ing

Rad ima: 126 stranica

Redni broj:

Abstract

In this thesis building of public key infrastructure (PKI) at a higher education institution is considered. PKI resolves many of the problems in the area of secure computer communications but it is expensive and complex to implement. This thesis suggests a feasible approach to creating PKI. Specific needs, environment and administration of a school at university are taken as a basis to create custom made PKI. Given approach lowers the cost and level of building complexity of PKI and puts them within the reach of an academic institution.

Kratak sadržaj

Ovaj rad se bavi izgradnjom infrastrukture javnih ključeva (PKI) u visokoškolskoj ustanovi. PKI rješava mnoge probleme u oblasti sigurnih računarskih komunikacija ali je skupa i kompleksna za implementaciju. Ovaj rad predlaže izvodljiv pristup izgradnji PKI. Posebne potrebe, okruženje i administracija fakulteta na univerzitetu su uzeti kao osnova za izgradnju njima prilagođenog PKI. Navedni pristup snižava troškove i kompleksnost izgradnje PKI i čini je dostupnom akademskoj instituciji.

SADRŽAJ

P o g l a v l j e 1

1 UVOD

Od kada su 1976 Diffie i Hellman u svom članku [1] predstavili ideju kriptografije u kojoj nije bilo neophodno da dvije strane u šifriranoj komunikaciji imaju isti ključ otvoreno je novo poglavlje u teoriji i praksi sigurnih komunikacija. Dvije godine kasnije je Kohnfelder u svojoj diplomskoj tezi [2] uveo pojam certifikata kao digitalno potpisanog podatka koja veže javni ključ sa imenom onog kome taj ključ pripada. Ovo su bile osnovne teoretske ideje koje su uz pojavu Interneta, odnosno prednosti koje on donosi i zahtjeva koje postavlja, dovele do mogućnosti realizacije sistema koji omogućava sigurne komunikacije preko nesigurnih medija. Ovaj sistem nazvan je Infrastruktura javnih ključeva (Public Key Infrastructure – PKI).

U posljednjih desetak godina uloženi su veliki napori kroz ANSI, ITU-T i IETF u standardizaciju pojmova i procedura iz ove oblasti kako bi se omogućila šira implementacija olakšavanjem interakcije različitih PKI sistema. Samo IETF radna grupa PKIX je od svog osnivanja 1995 napravila 18 Internet nacrta (*Internet drafts*) i 22 RFC (*Request For Comments*) [3]. Teoretski je izgledalo da je PKI pogodno rješenje, ali je broj praktičnih izvedbi sistema bio mnogo manji nego što se očekivalo. Za to postoje dva osnovna razloga. Prvi je velika složenost praktičnih izvedbi PKI, a drugi visoki troškovi izgradnje ili kupovine ovakvog sistema [4]. Troškovi samostalne izgradnje PKI unutar neke organizacije se kreću od nekoliko stotina hiljada do nekoliko miliona Eura u zavisnosti od veličine i željenih karakteristika, dok se troškovi angažovanja specijalizovane kompanije procjenjuju na 50 Eura po certifikatu [5]. U međuvremenu su se pojavile nove teoretske ideje o načinima korištenja kriptografije sa javnim ključevima. Neke se bave prvenstveno novim načinima zaštite ključeva [6], dok druge predlažu sasvim novi koncept potpuno bez certifikata [7].

Dodatna otežavajuća okolnost za brže uvođenje PKI u svijetu često je i zakonska regulativa, odnosno nepostojanje iste. U Bosni i Hercegovini postoje dvije odluke Centralne banke iz 2002 godine iz ove oblasti. Jednom se regulišu pravila vezana za elektronski potpis [8]. Druga govori o uslovima za kvalificiranje kao Certifikacijsko tijelo (CA) [9]. Po posljednjim informacijama iz Centralne banke do sada niti jedno certifikacijsko tijelo nije kvalificirano.

Ovaj rad će da ispita mogućnosti i predloži rješenje za PKI na visokoškolskoj ustanovi. Ovo rješenje mora prije svega biti izvodivo, odnosno dovoljno jednostavno i prihvatljivo. Ovo uzima u obzir ograničene hardverske, softverske, finasijske i ljudske resurse dostupne fakultetu. Takođe je potrebno da rješenje bude dovoljno fleksibilno da omogući PKI i na širem nivou, recimo univerziteta. Rješenje mora biti u skladu sa standardima koji su još u razvoju čime bi se omogućilo uvezivanje sa drugim PKI, pogotovo drugim evropskim i svjetskim univerzitetima, te međusobna certifikacija.

Rad će se sastojati od dva glavna dijela. Prvi dio sa neophodnim teoretskim osnovama i drugi u kome će biti izložen plan izgradnje infrastrukture javnih ključeva.

U prvom dijelu će biti izložene teoretske osnove na kojim se zasniva infrastruktura javnih ključeva. Ukratko će biti navedena uloga i namjena kriptografije kroz istoriju do danas. Biće predstavljeni osnovi simetrične kriptografije sa značajnim algoritmima. Asimetrična kriptografija, kao temelj infrastrukture javnih ključeva, biće takođe opisana. Digitalni potpis, kao nadgradnja asimetrične kriptografije i protokol koji omogućava infrastrukture javnih ključeva, biće u nastavku detaljno obrađeni. Nakon ovoga sve osnovne komponenete infrastrukture javnih ključeva i prinipi rada biće izloženi do nivoa detalja potrebnog za sagledavanje pitanja vezanih za izgradnju ovakve infrastrukture. Na kraju poglavlja će biti izloženo postojeće stanje izgradnje infrastrukture javnih ključeva.

Plan izgradnje infrastrukture javnih ključeva biće podijeljen na četiri glavna dijela:

Prvi dio će definisati potrebe za digitalnim certifikatima na visokoškolskoj ustanovi. Definisanje potreba je zapravo utvrđivanje usluga koje sistem treba da pruži svojim korisnicima. Usluge informacionog sistema pružaju se korisnicima putem računarskih aplikacija, te je definisanje usluga zapravo definisanje aplikacija koje će pružati te usluge. Pored definisanja usluga, odnosno računarskih aplikacija koje ih pružaju, biće utvrđeni i korisnici tih usluga - aplikacija. Korisnici ne moraju biti svi jednaki po svojim pravima, odnosno ne moraju svi korisnici imati pristup svim uslugama sistema. Korisnike je moguće svrstati u grupe sa istim nivoom potreba. Biće utvrđeno koje će aplikacije sistem nuditi kojim korisnicima. U ovom postupku potrebno je utvrditi i uticaj odluka o aplikacijama i korisnicima na to koji će resursi biti potrebni.

U drugom dijelu plana izgradnje će na osnovu definisanih aplikacija i grupa korisnika biti definisana infrastruktura potrebna za podršku utvrđenim ciljevima. Osnova PKI je Certifikacijska ustanova (*Certification Authority* - CA). Pošto je CA osnova PKI prvi korak u izgradnji PKI nakon definisanih potreba je utvrđivanje kakva CA je potrebna da bi se zadovoljile definisane potrebe. Biće razmotreni svi aspekti uspostavljanja CA i predložena potrebna konfiguracija CA.

Na osnovu definisane konfiguracije CA, u trećem dijelu će biti razmotrena konfiguracija digitalnih certifikata. Biće detaljno razmotren format certifikata koji bi odgovarao njihovoj planiranoj namjeni. Pored formata certifikata, sigurnosne opcije certifikata će biti razmotrene. Biće predloženi kriptografski algoritimi, dužine ključeva i period valjanosti certifikata i odgovarajućih ključeva.

U posljednjem dijelu rada koji se bavi planom izgradnje PKI biće, na osnovu definisane konfiguracije CA i digitalnih certifikata, razmotreno upravljanje certifikatima. Razmotriće se metode dobijanja i obnavljanja certifikata i mogućnost njihove integracije sa postojećom administrativnom infrastrukturom na visokoškolskim ustanovama. Sigurnost privatnih ključeva, kao osnova sigurnosti PKI, će biti detaljno izložena i biće predloženo odgovarajuće rješenje. Na kraju će biti izložena problematika spremišta certifikata i opozivanja certifikata, koji su najproblematičniji aspekt PKI. Biće predloženo sigurno i praktički izvodivo rješenje.

Kroz pomenuta razmatarnja će biti definisani svi elementi PKI sa međusobnim interakcijama. Na osnovu ovih definicija biće moguće pristupiti izgradnji konkretnog sistema kroz korake koji će biti opisani u radu. U prilogu rada će biti dat i prikaz ogledne implementacije rješenja predloženog u radu koja će pokazati izvodljivost nevedenih rješenja.

Očekivani rezultat rada je prijedlog rješenja infrastrukture javnih ključeva na visokoškolskoj ustanovi. Ova infrastruktura daće svim korisnicima sistema digitalni identit. Ovaj identitet će im omogućiti sigurne komunikacije i upotrebu računarskog sistema zasnovane na osnovnim postulatima sigurnosti: autentikacija, povjerljivost podataka, integritet podataka i nemogućnot poricanja učešća u transakciji. Pošto u BiH još ne postoji registrovana certifikacijska ustanova (CA) rad bi trebao biti podsticaj u pravcu šire implemetacije PKI.

P o g l a v l j e 2

2 TEORETSKE OSNOVE

Kako je u uvodu već najavljeno u ovom poglavlju će biti izložene teoretske osnove na kojim se zasniva infrastruktura javnih ključeva. Na ovaj način se odvaja teoretsko objašnjenje pojmova i principa rada od praktičnih pitanja izgradnje infrastrukture javnih ključeva kojima se bavi u trećem poglavlju. Ukratko će biti navedena uloga i namjena kriptografije kroz istoriju do danas. Biće predstavljeni osnovi simetrične kriptografije sa značajnim algoritmima. Asimetrična kriptografija, kao temelj infrastrukture javnih ključeva, biće takođe opisana. Digitalni potpis, kao nadgradnja asimetrične kriptografije i protokol koji omogućava infrastrukture javnih ključeva, biće u nastavku detaljno obrađeni. Nakon ovoga sve osnovne komponenete infrastrukture javnih ključeva i prinipi rada biće izloženi do nivoa detalja potrebnog za sagledavanje pitanja vezanih za izgradnju ovakve infrastrukture. Na kraju poglavlja će biti izloženo postojeće stanje izgradnje infrastrukture javnih ključeva.

2.1 Istorija

Zbog uloge koju je kriptografija igrala kroz vrijeme njena istorija može biti zanimljiva i široj netehničkoj publici. Kriptografija je imala bitan uticaj na ishode mnogih vojnih sukoba još od vremena starih Egipćana uključujući i oba svjetska rata. Knjiga Davida Khan-a "The Codebreakers" [10] daje vrlo kompletan netehnički prikaz ove istorije. Upotreba kriptografije je, sve do pojave savremenih elektronskih komunikacija 1960-ih, bila vezana za vojsku i diplomatiju. Pošto je kriptografija korištena za čuvanje vojnih i nacionalnih tajni objavljivanje literature iz ove oblasti gotovo da je prestalo u periodu od početka prvog svjetskog rata do sredine 1960-tih, mada nikad nije bilo zvanično zabrananjeno. Izuzetak čine dva istorijska članka koji su postavili

neke od temelja savremene kriptografije. Prvi je William Friedman-ov "The Index of Coincidence and Its Applications in Cryptography", objavljen 1920 [11]. Drugi članak je Claude Shannon-ov "The Communication Theory of Secrecy Systems," objavljen 1949 [12]. Oba članka nastala su kao plod aktivnog angažmana autora u ovoj oblasti tokom prvog, odnosno drugog svjetskog rata. Nedostatak javno dostupne literature nije značio da se ova oblast nije razvijala, već samo da su informacije bile dostupne zatvorenim krugovima unutar raznih vojnih i državnih obavještajnih službi koje su se bavile ovim istraživanjima.

Sredinom 1960-tih računari i elektronske komunikacije su počeli ozbiljnije da se koriste u poslovnom svijetu. Kompanije su imale potrebu da zaštite svoje podatke na računarima i prilikom transfera između računara. Kriptografija je postala neophodna van krugova obavještajnih službi. Prvi praktični, zvanično objavljeni, rezultati kriptografskog rada u privatnom sektoru bili su postignuti u IBM-u početkom 1970-tih. Ekipa naučnika pod vođstvom Horst Feistel-a razvila je simetrični blok šifrator Lucifer [13]. Značaj Lucifera je u tome što je na osnovu njega razvijen šifrator koji je 1977. usvojen kao američki standard za šifriranje podataka DES, *Data Encryption Standard* [14]. DES je postao *defacto* standard u poslovnom svijetu i najpoznatiji kriptografski mehanizam u istoriji. Tek nedavno, 2002., je na međunarodno otvorenom natjecaju za novi američki standard izabran Rijndael, dvojice belgijskih naučnika Joan Daemen i Vincent Rijmen. Zvanični naziv ovog standarda je AES, *Advanced Encryption Standard* [15]. Na osnovu istorije, za očekivati je da AES u narednom periodu pruzme ulogu DES-a

Izuzetno važan događaj desio se 1976 kada su Diffie i Hellman objavili članak "New Directions in Cryptography" [1]. Članak je predstavio sasvim novi koncept kriptografije, asimetričnu kriptografiju. Za razliku od svih do tada poznatih metoda šifriranja, po ovom konceptu bilo je moguće poruku šifrirati jednim, a dešifrirati drugim ključem. Drugi značajan doprinos ovog

rada je bio siguran način razmjene ključeva za klasičnu, simetričnu, kriptografiju. Diffie i Hellman su iznijeli koncept asimetrične kriptografije, ali nisu imali odgovor na to kako ga i relizovati. Međutim nova ideja je pokrenula istraživanja u pravcu realizacije. Nakon dvije godine Rivest, Shamir i Adleman su pronašli metod praktične realizacije asimetrične kriptografije [16]. Ovaj članak je ponudio i metod kreiranja digitalnog potpisa. Na ovim idejama u kombinaciji sa napretkom u klasičnoj kriptografiji zasnovana je i infrastruktura javnih ključeva čija je realizacija tema ovog rada.

U ovom kratkom istorijskom pregledu potrebno je reći da je dalji razvoj elektronskih komunikacija doveo do njihove široke upotrebe među običnim ljudima. Ljudi su počeli koristiti elektronsku poštu za privatne komunikacije. Međutim elektronske komunikacije, u svom izvornom obliku, su mnogu nesigurnije od običnih poštanskih komunikacija. Elektronska poruka može biti pročitana ili čak i promijenjena na svom putu od pošiljaoca do primaoca, a da je to teško ili gotovo nemoguće otkriti. Vlade ili druge moćne organizacije mogu organizovati prilično efikasan sistem nadziranja komunikacija u kom bi građanska privatnost prestala da postoji. Whitfield Diffie je rekao da su u prošlosti dvije osobe mogle obaviti privatan razgovor jednostavnom vizuelnom provjerom da oko njih nema nikoga, a da je to u doba elektronskih komunikacija postalo gotovo nemoguće [17]. Pojavila se potreba za kriptografijom za svakoga. Metode su postojale, ali je tehnologija uglavnom bila prekomplikovana, a često i zaštićena patentima. Phil Zimmermann je napravio proizvod koji je na jednostavan način omogućavao šifriranje i digitalno potpisivanje poruka elektronske pošte. Ovaj program se zvao PGP, *Pretty Good Privacy*. Zimmermann je namjeravo prodavati PGP, ali pošto je izgledalo da će američka vlada zabraniti upotrebu kriptografiju za široke narodne mase, on je program 1991. preko *Usenet bulletin board*-a dao svijetu na besplatno korištenje [17]. Ovim je praktična kriptografija postala dostupna svima. Danas postoje mnogi proizvodi koji omogućavaju jednostavnu upotrebu kriptografije za lične potrebe za osiguranje elektronskih

komunikacija, ali ih ipak veoma mali postotak ljudi koristi. Planirana infrastruktura javih ključeva bi svim korisnicima pored sigurnih poslovnih omogućila i sigurne privatne komunikacije.

2.2 Namjena kriptografije

Nakon što su izloženi najvažniji događaji u istoriji kriptografije potrebno je i jasno definisati njenu namjenu. Jedna od definicija kriptografije bazirana na njenoj namjeni kaže da je kriptografija izučavanje matematičkih tehnika vezanih za aspekte sigurnosti informacija kao što su povjerljivost, integritet podataka, autentikacija entiteta i porijekla podataka [18]. Ova definicija obuhvata tri od četiri funkcije ili cilja kriptografije koji se najčešće navode u literaturi. Ove četiri funkcije su: povjerljivost (*confidentiality*), integritet podataka (*data integrity*), autentikacija (*authentication*) i neporicanje (*non-repudiation*).

1. Povjerljivost znači obezbjeđivanje da sadržaj informacija nije dostupan nikome drugom od onoga kome su informacije namjenjene. Ovo je najstarija namjena kriptografije. Ponekad se ovu namjenu koriste termini privatnost ili tajnost.

2. Integritet podataka znači osiguravanje nepromijenjivosti podataka. Da bi se osigurao integritet potrebno je obezbijediti otkrivanje bilo kakve promjene podataka. Pod promjenama podataka se podrazumijevaju radnje kao što su dodavanje, uklanjanje ili zamjena. Uobičajeno je da se detektuju promjene podataka od strane neovlaštenih lica.

3. Autentikacija je vezana za razmjenu informacija. Namjena autentikacije je identifikacija subjekata razmjene informacija i same informacije. Elementi autentičnosti informacije su njeno porijeklo, vrijeme nastajanja i vrijeme slanja. Ponekad se autentikacija dijeli na dvije klase: autentikacija entiteta i autentikacija porijekla podataka.

4. Neporicanje onemogućava negiranje prethodno učinjenih djela od strane bilo kog učesnika u njima. Sa aspekta razmjene informacija ovo znači da ni jedna strana u toj razmjeni ne može poreći svoje učešće u razmjeni i sadržaj razmjenjenih informacija.

Jednostavno rečeno kriptografija treba da omogući da subjekti učesnici u sigurnoj komunikaciji znaju da su podaci koje razmijenjuju dostupni samo njima, da su nepromijenjeni tokom prenosa, da se može ustanoviti identitet druge strane i znati da se ova komunikacija i njen sadržaj ne mogu poreći. Kriptografija treba da spriječi i otkrije bilo kakvu vrstu varanja ili nedobronamjernog ponašanja u ovoj sferi.

Postoje različite metode kojima se ostvaruju neke ili sve od ove četiri osnovne funkcije kriptografije. Namjena kriptografije nije vezana za tipove kriptografije, simetričnu ili asimetričnu. Oba tipa mogu pružiti sve navedene funkcije. Infrastruktura javnih ključeva o kojoj se govori u ovom radu predstavlja sistem koji pruže sve četiri usluge.

2.3 Simetrična kriptografija

Simetrična kriptografija je tradicionalni način zaštite podataka koji se prenose od jednog do drugog učesnika u komunikaciji. Ovaj način zaštite podataka star je gotovo koliko i ljudska komunikacija. Suština simetrične kriptografije je da je za sigurnu komunikaciju neophodno da oba učesnika imaju istu tajnu informaciju koja im omogućava šifriranje i dešifriranje podataka. Ova informacija se najčešće naziva ključ jer omogućava "zaključavanje" sadržaja prilikom šifriranja i njegovo "otključavanje" prilikom dešifriranja.

U osnovi svi simetrični kriptografski algoritmi obavljaju dvije operacije substituciju i transpoziciju. Prvi šifratori su obavljali samo jednu od ovih operacija i to samo jednom. Savremeni šifratori kombinuju ove dvije operacije ponavljajući ih više puta. Međutim, filozofija je ista Substitucija predstavlja

zamjenu simbola drugim simbolima. Simboli su nekada bili slova, a danas su uglavnom *bit*-i. Prva dokumentovana upotreba substitucionog šifratora za vojne svrhe je od strane Julija Cezara [17]. Ovaj rimski vladar i vojskovođa je koristio više substitucionih šifratora od kojih je najpoznatiji onaj u kom je svako slovo alfabeta bilo zamijenjeno slovom koje sa nalazilo tri mjesta dalje u alfabetu. Ova zamjena je predstavljala šifriranje. Za dešifriranje je bilo potrebno znati da je vršena ovakva vrsta substitucije (algoritam) i da je pomjeranje bilo za tri mjesta (ključ). Primjer:

```
TATAZOVEMAMU
ZDZDBSAHODOŽ
```

Transpozicija je permutacija simbola u poruci. Transpozicija je korištena u prvom vojnom kriptografskom uređaju spartanskom *scytale* (drvena palica) u petom vijeku prije nove ere [17]. Duž ove palice bi se namotala traka širine jednog slova i poruka napisala u redovima koji su išli dužinom palice. Kada bi se traka odmotala na njoj je bio niz slova originalne poruke ali ispremještan. Za dešifriranje je bilo potrebno znati način na koji je izvršena transpozicija (algoritam) te prečnik palice (ključ). Primjer:

```
TATA
ZOVE          TZMAOATVMAEU
MAMU
```

Substitucija i transpozicija se mogu obavljati na razne načine, a ne samo na ove pomenute ovdje. Bitno je da postoji algoritam i ključ koji su poznati učesnicima u sigurnoj komunikaciji. Teoretsko značenje ove dvije operacije je dao Shannon [12]. On je ukazao na to da su ove dvije operacije zapravo vezane za tehnike za prikrivanje redundantnosti u izvornom tekstu koja se koristi u kriptoanalizi. Ove tehnike su konfuzija i difuzija:

1. Konfuzija prikriva vezu između izvornog i šifriranog teksta, odnosno čini je što je moguće kompleksnijom, jer je nemoguće ukloniti. Ovim

se otežava analiza šifrirarnog teksta zasnovana na redundantnosti i statističkim osobinama jezika. Substitucija je najjednostavniji način postizanja konfuzije.

2. Difuzija razuđuje redundantnost izvornog teksa rasišrujući je po šifrirarnom tekstu. Ovim se otežava kriptoanaliza bazirana na redundantnosti jezika. Transpozija je najjednostavniji način za postizanje difuzije.

Simetrični šifratori se dijele na blok i *stream* šifratore. Blok šifratori transformišu izvorni tekst u šifrirani obavljajući transformaciju na blokovima izvornog teksta jednake dužine. *Stream* šifratori obavljaju transformaciju svake jedinične informacije izvornog teksta. Jedinična informacija može biti bit, simbol i slično. Razlika između savremenih blok i *stream* šifratora je da blok šifratori rade fiksne transformacije velikih blokova izvornih podataka dok *stream* šifratori rade vremenski promjenjive transformacije individualnih jedinica izvornih podataka[19]. *Stream* šifratori koriste samo konfuziju, a blok šifratori koriste i konfuziju i difuziju [20].

Kako je već rečeno, za proces šifriranja i dešifriranja u simetričnoj kriptografiji potrebno je znati algoritam i ključ. U prošlosti su se algoritmi držali u tajnosti, ali je praksa pokazala da prikrivanje algoritma ne doprinosi sigurnosti. Sigurnost dobrog sistema zasnovana je na dužini i sigurnosti ključa, a ne na navodnoj tajnosti algoritma. Svi savremeni kriptografski algoritmi su javno dostupni. Na ovaj način ih je moguće u potpunosti testirati na sve vrste napada, odnosno kriptoanalize. Dobri algoritmi, kao što je DES vrlo dobro odolijevaju svim testovima i većina navodnih nedostataka su puno više od akademske nego praktične važnosti. Razlog iz kog je DES zamijenjen AES-om kao novim standardom je prvenstveno dužina ključa od 56 bita. Ovaj ključ je, sa današnjim nivoom razvoja računara i računarskih mreža, postao podložan napadima ispitivanjem svih njegovih kombinacija (*brute* force) 2^{56}. Electronic Frontier Foundation je 1998 godine za manje od $250,000 izgradila

računar specijalne namjene za pronalaženje DES ključa koji je za manje od tri dana uspio otkriti ključ. [21].

Savremeni simetrični kritpografski algoritmi su vrlo dobri i sigurni jer su još uvijek sve vrste njihove kriptoanalize po potrebnim reursima bliske resursima potrebnim za ispitivanje svih kombinacija ključa. Sa današnjim dužinama ključa, od 128 bita i više, broj kombinacija je isuviše veliki da bi kratkoročna sigurnost algoritama bila ugrožena. Za dugoročniju analizu dobro razmatranje se može naći u [20]. Nedostaci simetričnih kriptosistema su vezani za ključeve, tačnije upravljanje ključevima [20]:

- Potrebno je naći siguran način distribucije ključeva od jedne do druge strane u komunikaciji prije nego što sigurna komunikacija može početi. Pošto je sigurnost svih šifriranih informacija zasnovana na sigurnosti ključa otkrivanjem ključa otkrivaju se i sve informacije šifrirane tim ključem. Sigurna razmjena ključeva pogotovo na velike daljine može predstavljati vrlo ozbiljan problem

- Ako je potrebno, a uglavnom jeste, za svaki par subjekata u sistemu koji žele sigurno komunicirati imati poseban ključ, broj ključeva veoma brzo raste sa rastom broja korisnika sistema. Za n korisnika potrebno je imati $n(n - 1)/2$ ključeva. Generisanje ovolikog broja ključeva i upravljanje njima postaje vrlo nepraktično za veliki broj korisnika kakav je danas uobičajen u sistemima komunikacije.

2.4 Asimetrična kriptografija

Razvoj savremenih elektronskih komunikacija, a pogotovo računara i računarskih mreža učinili su problem distribucije ključeva simetrične kriptografije još većim. Računarske mreže omogućavaju brzu razmjenu podataka, ali u svojim počecima nisu pravljene da budu veoma sigurne. Činjenica da je za sigurnu upotrebu računarskih mreža bilo potrebno

organizovati distribuciju ključeva na neki drugi način, te da je broj potencijalnih korisnika stalno rastao uticali su na shvatanje potrebe da se nešto promijeni. Kako je u istorijskom pregledu rečeno, 1976 su Diffie i Hellman predložili sasvim novi koncept asimetrične kriptografije [1]. Umjesto jednog istog ključa za šifriranje i dešifriranje predloženo je postojanje para ključeva: javnog i privatnog. Javni ključ je dostupan svima i to je ključ koji se koristi za šifriranje podataka. Odgovarajući privatni ključ je tajan i samo taj ključ omogućava dešifriranje podataka šifriranih javnim ključem iz para. Na ovaj način se rješava problem distribucije ključeva i njihovog broja. Svaki subjekat koji želi sigurnu komunikaciju može objaviti svoj javni ključ i svako ko mu želi poslati šifriranu poruku koristi taj ključ za šifriranje. Pošto jedino ovaj subjekt ima privatni ključ koji može dešifrovati podatke obezbijeđena je povjerljivost podataka. Nema potrebe za posebne kanale za sigurnu distribuciju ključeva i generisanje ključeva za svaki par koji komunicira.

Ideja asimetrične kriptografije rješava problem distribucije ključeva ali Diffie i Hellman nisu predložili konkretan način realizacije. Da bi ovakav sistem radio neophodno je obezbijediti da se na osnovu znanja javnog ključa ne može izračunati privatni ključ. Ova dva ključa moraju biti matematički povezana tako da će uvijek biti teoretski moguće izračunati jedna iz drugog, ali ovo treba učiniti računski neisplativim. Odnosno resursi potrebni za izračunavanje privatnog ključa iz javnog treba da budu nesrazmjerno veći od vrijednosti informacija koje se šifriraju. Sa druge strane potrebno je obezbijediti jednostavno i brzo šifriranje i dešifriranje. Za ovo je potrebna takozvana "jednosmjerna funkcija sa tajnim prolazom" (*trap-door one-way function).* Funkcija je jednosmjerna jer je lako izračunati u jednom pravcu (šifriranje), a nesrazmjerno teže u drugom (dešifriranje). "Tajni prolaz" znači da je funkciju lako izračunati i u težem pravcu ako se posjeduje tajna informacija (privatni ključ).

Prvu ovakvu transformaciju su objavili Rivest, Shamir i Adleman, u prethodno pomenutom članku, 1978. [16]. Njihove originalne metode šifriranja i dešifriranja su kako slijedi:

Poruku koja se šifrira potrebno je predstaviti kao cijeli broj između 1 i *n*-1. Zapravo poruku je potrebno razbiti u blokove koji se mogu predstaviti na ovaj način. Ovo predstavljanje niza karaktera preko cijelog broja nije predmet algoritma, već standardna transformacija. Broj *n* će biti kasnije precizno definisan.

Šifriranje poruke se obavlja dizanjem poruke, odnosno broja M kojim je ona predstavljena, na *e*-ti stepen moduo *n*. Rezultat, ostatak dijeljenja M^e na *n* je šifrirana poruka, C.

Dešifriranje se obavlja dizanjem šifrirane poruke, odnosno broja kojim je ona predstavljena, na *d*-ti stepen moduo *n*. Odnosno, ostatak dijeljenja C^d na *n* je originalna poruka M.

Matematički zapisano:

$$C \equiv E(M) \equiv M^e \pmod{n}$$; šifriranje poruke M u C.

$$M \equiv D(C) \equiv C^d \pmod{n}$$; dešifriranje C u originalnu poruku M.

Javni ključ, koji se koristi za šifriranje, je par cijelih brojeva (*e; n*).

Privatni ključ, koji se koristi za dešifriranje, je par cijelih brojeva (*d; n*).

Vrijednosti za *n*, *e* i *d* se biraju na slijedeći način:

- *n* je proizvod dva vrlo velika "slučajna" prosta broja:

  $$n = p * q$$

  Iako je *n* javno, faktori *p* i *q* ostaju tajni zbog velike težine rastavljanja broja na proste faktore. Na ovaj način je onemogućeno dobivanje *d*, drugog dijela privatnog ključa, iz *e*, drugog dijela javnog ključa.
- *d* se bira da bude veliki, slučajan cijeli broj koji nema zajedničkih faktora sa $(p - 1) * (q - 1)$, odnosno da *d* zadovoljava:

  $$\text{najveći\_zajednički\_djelilac}(d; (p - 1) * (q - 1)) = 1$$

- e se računa iz p, q i d da bude "multiplikativna inverzija" d moduo $(p-1) * (q-1)$, što znači

$$e * d \equiv 1 \pmod{(p-1) * (q-1)}$$

Matematski dokaz ispravnosti metoda je dat u navedenom radu [16]. Ovaj algoritam nazvan je RSA po inicijalima prezimena autora.

RSA algoritam je realizovao koncept asimetrične kriptografije. Šifriranje je bilo vrlo jednostavno, a dešifriranje neuporedivo teže bez poznavanja privatnog ključa *d*. Za one koji znaju *d* dešifriranje je jednako jednostavno kao i šifriranje. Dešifriranje bez poznavanja *d* postaje praktično nemoguće ako su *p* i *q*, odnosno *n* dovoljno veliki. Rivest, Shamir i Adleman su predložili 100 cifrene *p* i *q*, odnosno 200 cifreni *n*. Veći *n* donosi veću sigurnost, ali usporava šifriranje i dešifriranje. U dijelu rada koji se bavi izgradnjom infrastrukture javnih ključeva biće detaljno razmatrana potrebna dužina *n* za savremene sisteme. Pitanje izbora velikih prostih brojeva *p* i *q*, pitanje izbora *d*, te pitanje računanja *e* su obrađeni još u izvornom članku [16], a i mnogo puta kasnije. Ispostavilo se da nijedna od ovih operacija ne predstavlja ozbiljniji problem, te da je RSA vrlo praktičan i upotrebljiv algoritam šifriranja i dešifriranja. Sigurnost RSA algoritma je zasnovana na težini rastavljanja broja na proste faktore. Ovo se smatra jednim od teških problema (*hard problem*) za koje ne postoji brz i jednostavan algoritam već samo poboljšanja u odnosu na pretraživanje svih mogućih kombinacija. Ovim problemom se matematičari bave preko 300 godina i smatra se da je prilično dobro izučen. Od 1978 kada je RSA predstavljen nije bilo dovoljno značajnog napredka u ovoj oblasti koji bi ugrozio sigurnost RSA. Ne postoji nikakva garancija da se jednom, možda čak i u skoroj budućnosti neće naći brza i jednostavna metoda za rastavljanje velikih brojeva na proste faktore, ali to razmatranje već izlazi iz okvira ovog rada.

Od 1978. objavljeno je više algoritama koji implementiraju ideju asimetrične kriptografije. Svi oni su bazirani na pomenutim teškim (*hard*) problemima. Svi

predloženi algoritmi nisu jednako sigurni ni praktični. U široj upotrebi se pored RSA koriste još i ElGamal algoritam [22] , te kriptografski sistemi bazirani na eliptičkim krivim [23], [24]. Ovi asimetrični kriptografski algoritmi se uglavnom nazivaju algoritmi sa javnim ključem. Asimetrična kriptografija je riješila problem distribucije ključeva, ali i ona ima svoje nedostatke [20]:

- Algoritimi sa javnim ključem su 100 do 1000 puta sporiji od simetričnih algoritama.

- Kriptosistemi sa javnim ključem su podložni jednoj vrsti kriptoanalize koja se naziva napad na izabrani izvorni tekst (*chosen-plaintext attack*).

U savremenoj praktičnoj upotrebi algoritmi sa javnim ključem nisu zamijenili simetrične algoritme već se koriste za različite namjene. Algoritmi sa javnim ključem se koriste najčešće za šifriranje ključeva koji se koriste za šifriranje podataka koji se razmjenjuju simetričnim algoritmima. Primjer ovoga su vrlo korišteni, takozvani, hibridni kriptosistemi kod kojih se simetrični algoritam sa slučajnim sesijskim ključem koristi za šifriranje poruka, a algoritam sa javnim ključem za šifriranje tog slučajnog sesijskog ključa.

2.5 Digitalni potpis

Kriptografski algoritmi sa javnim ključem su u mnogome olakšali, ako ne i riješili, razmjenu ključeva. Međutim, ovi algoritmi su omogućili i digitalno potpisivanje elektronskih dokumenata. Istini za volju, teoretski je moguće organizovati i digitalno potpisivanje koristeći simetričnu kriptografiju i arbitratora od povjerenja [20], ali je vrlo nepraktično i gotovo neupotrebljivo. Sa druge strane kriptosistemi sa javnim ključem su vrlo pogodni za ovu namjenu.

Papirni dokument sa nečijim svojeručnim potpisom se smatra autentičnim. Ovakav dokument je čak prihvatljiv kao dokaz na sudu. Prije definisanja digitalnog potpisa potrebno je utvrditi šta je to što svojeručni potpis čini tako važnim.

1. Svojeručni potpis je autentičan, odnosno može ga napraviti samo potpisnik lično.
2. Svojeručni potpis je moguće provjeriti poređenjem sa prethodnim potpisima.
3. Svojeručni potpis izražava autorstvo ili slaganje sa sadržajem dokumenta i neodvojivi je dio dokumenta
4. Svojeručni potpis se ne može poreći.

Mora se naglasiti da ovi iskazi o svojeručnom potpisu nisu u potpunosti tačni, odnosno da su prevare moguće i da su se dešavale. Međutim, s obzirom na potrebne napore i mogućnost otkrivanja može se reći da prethodno rečeno važi u opštem slučaju.

Da bi elektronski dokumenti zamijenili papirne neophodno je osigurati njihovu autentičnost. Dokumente u elektronskom obliku je mnogo lakše mijenjati nego papirne i to na način da to može biti teško ili gotovo nemoguće otkriti. Zbog ovoga je potreban mehanizam koji će osigurati integritet i autentičnost elektronskih dokumenata. Digitalni potpis bi trebao imati iste osobine kao i svojeručni. Postoji veći broj algoritama digitalnog potpisivanja u upotrebi. Ovi algoritmi se u nekoliko razlikuju ali zajedničko im je da je potpis funkcija sadržaja dokumenta i privatnog ključa, a verifikacija potpisa se obavlja korištenjem sadržaja poruke i javnog ključa potpisnika. Na ovaj način je moguće postići osobine svojeručnog potpisa:

1. Digitalni potpis je autentičan, odnosno može ga napraviti samo posjednik privatnog ključa.
2. Digitalni potpis je moguće provjeriti korištenenjem javnog ključa potpisnika.

3. Digitalni potpis izražava autorstvo ili slaganje sa sadržajem dokumenta i funkcija je ovog sadržaja čime je neodvojiv od sadržaja.
4. Digitalni potpis se ne može poreći.

Procedura digitalnog potpisivanja koja se najčešće primjenjuje u praksi je slijedeća:

1. Izračuna se jednosmjerni *hash* dokumenta.
2. Ovaj *hash* se propusti kroz funkciju čiji je parametar privatni ključ potpisnika.
3. Rezultat ove operacije je digitalni potpis koji se čuva ili šalje zajedno sa dokumentom.

Odgovarajuća procedura provjere je:

1. Verifikator izračuna jednosmjerni *hash* dokumenta.
2. Verifikator nad digitalnim potpisom obavi operaciju koja je u suštini inverzija funkcije koju je obavio potpisnik i čiji je parametar javni ključ potpisnika.
3. Rezultat ove operacije bi trebao biti jednak hash-u dokumenta čime se potvrđuje da je potpis autentičan i da dokument nije izmijenjen od potpisivanja.

Hash je funkcija koja string varijabilne dužine pretvara u string fiksne dužine takozvani *hash* ulaza. Jednosmjerni *hash* je funkcija koju je lako izračunati u jednom pravcu, odnosno lako je naći *hash* ulaza, ali je vrlo teško, odnosno računski neisplativo, pronaći ulaz na osnovu *hash*-a, odnosno naći ulaz koji bi proizveo isti *hash*. Jednosmjerne *hash* funkcije nemaju tajnih parametara njihova sigurnost je u njihovoj jednosmjernosti. Zavisnost njihovog izlaza, *hash*-a, od ulaza nije ni na koji način predvidiva. Promjena jednog bita ulaza u prosjeku mijenja polovinu bita *hash*-a. Ovakve funkcije imaju veliku primjenu u kriptografiji. Tri najčešće korištena algoritma za jednosmjeren hash funkcije su: MD2, MD5 i SHA-1. MD2 [25] i MD5 [26] daju kao rezultat 128 bitni

hash i njihov autor je Ron Rivest. SHA-1 [27] je razvila vlada SAD. Ovaj algoritam proizvodi 160 bitni *hash*.

Operacija koja se obavlja nad *hash*-em dokumenta prilikom potpisivanja zavisi od izabranog algoritma za digitalno poptpisivanje. U praksi se uglavnom koriste tri algoritma: RSA [16], ElGamal [22] i DSA [28]. Kod RSA algoritma potpisivanje je zapravo šifriranje *hash*-a privatnim ključem, a verifikacija dešifriranje javnim ključem. Kod ElGamal šeme potpisivanja postoji poseban algoritam za potpisivanje i verifikaciju, različit od onog za šifriranje i dešifriranje, ali se i kod njega koristi privatni kjuč za potpisivanje, a javni za verifikaciju potpisa. DSA, *Digital Signature Algoritam*, je standard vlade SAD i zasnovan je na Schnorr [29] i ElGamal algoritmima za digitalno potpisivanje. DSA definiše isključivu upotrebu SHA-1 *hash* funkcije.

Potrebno je naglasiti da digitalno potpisivanje nije šifriranje dokumenta i da su kriptografske namjene digitalnog potpisa: integritet, autentikacija i neporicanje. Kao što se na potpisane dokumente često stavlja i datum potpisivanja, moguće je dodati vremensku oznaku (*timestamp*) i prilikom digitalnog potpisivanja. Ovo se postiže dodavanjem datuma i vremena u sadržaj dokumenta koji se *hash*-ira.

2.6 Infrastruktura javnih ključeva

Simetrična kriptografija omogućava brzo i sigurno šifriranje podataka. Asimetrična kriptografija rješava problem distribucije ključeva i omogućava digitalno potpisivanje dokumenata. Na ovaj način ostvaruje se povjerljivost podataka, autenticira njihov autor, osigurava integritet i onemogućava poricanje autorstva. Sve ranije navedene namjene kriptografije postaju ostvarive. Međutim, iako je pitanje sigurne distribucije ključeva riješeno time što postoje dva ključa javni i tajni, postavlja se novo pitanje autenetičnosti javnog ključa. Da bi javni ključ bio dostupan i upotrebljiv potrebno ga je na neki način objaviti sa podacima o tome kome on pripada. Ovi podaci o

javnim ključevima mogu biti promijenjenji zlonamjerno ili čak slučajno i pošiljalac može poslati povjerljivu poruku nekome drugom od onoga kome je namjeravao i mislio da šalje. Potrebno je osigurati da javni ključ zaista pripada onome za koga registar javnih ključeva kaže da mu pripada, kao i obezbijediti otkrivanje bilo kakve promjene podatak. Navedeno je tipičan kriptografski zadatak autentikacije i integriteta podataka što se može postići digitalnim potpisivanjem. Ovo je prvi još 1978. godine predložio Kohnfelder [2]. On je uveo termin certifikat kao digitalno potpisan elektronski dokument koji povezuje javni ključ sa onim kome pripada. Digitalnim potpisom se osigurava integritet podataka, a za njihovu autentičnost jamči potpisnik. Znači da potpisnik certifikata mora biti neko kome svi korisnici certifikata vjeruju i čiji javni ključ, koji se koristi za provjeru potpisa na certifikatima, mora biti pouzdano ispravan. Potrebno je imati neku certifikacijsku ustanovu ili tijelo. Da bi certifikati bili dostupni potrebno je imati mehanizam njihovog objavljivanja odnosno neku vrstu njihovog javno dostupnog spremišta. Pošto je situacija kompromitacije ili gubitka privatnog ključa realno moguća potrebno je imati mehanizam opozivanja odgovarajućeg javnog ključa i certifikata. Potrebna je neka lista opozvanih certifikata. Da bi sistem bio kompletan potrebno je naravno imati i subjekte certificiranja kojima se izdaju digitalni certifikati. Navedeni elementi: certifikati, certifikacijske ustanove, spremišta certifikata, liste opozvanih certifikata i subjekti certifikata zajedno sa procedurama međusobne interakcije i aplikacijama koje ih koriste čine infrastrukturu javnih ključeva (Public Key Infrastructure - PKI). Izgradnja ovakve infrastrukture je predmet ovog rada.

2.6.1 Osnovne komponente

Ovdje će ukratko biti opisani osnovni elementi PKI dok će detaljnije razmatranje implementacije svakog od njih bit dato u slijedećem poglavlju.

1. Certifikati

Digitalni certifikati ili certifikati javnih ključeva su strukture podataka koje povezuju javni ključ sa subjektom certifikata. Ova veza se potvrđuje digitalnim potpisom certifikacijske ustanove koja ih je izdala [30]. Najrašireniji format certifikata koji se koriste u PKI je X.509. Ovaj format je definišu ISO i ITU-T [31]. X.509 format podržavaju vodeći PKI-omogućeni protokoli i aplikacije kao što su SSL, IPSec, S/MIME, *Privacy Enhaced Mail* (PEM) i SET. Neki od ovih protokola će biti posebno predstavljeni kasnije. Drugi format certifikata koji nije standardizovan od strane zvaničnih standardizacijskih institucija ali je dovoljno raširen da ga je neophodno spomenuti je PGP [32]. Ovaj format se koristi u vrlo raširenom softverskom paketu istog naziva PGP (*Prety Good Privacy*). X.509 format je trenutno u svojoj trećoj verziji, originalna prva verzija je objavljena od strane ITU-T 1988. Verzija 2 ime dva dodatna polja u odnosu na prvu verziju: identifikatore izdavača i subjekta. Verzija 3 uvela je grupu opcionih polja nazvanu proširenjima (*extensions*). Na slici 1. je prikazan X.509 format certifikata verzija 3. Detaljniji opisi i značenja pojedinih polja biće izloženi prilikom definisanja potrebnih vrijednosti za konkretan PKI. Ovdje je samo potrebno reći da certifikat, pored toga što povezuje javni ključ sa subjektom certifikata jedinstveno definiše sam certifikat, serijskim brojem, i izdavača certifikata, X.500 ime, kao i kriptografski algoritam korišten za potpisivanje. Kompletan sadržaj certifikata, sva polja, predstavljaju podatak koji je digitalno potpisan što znači da bi promjena bilo kojeg polja učinila potpis i certifikat nevažećim.

2. Subjekti certifikata (*End Entities*)

Subjekti certifikata se ponekad nazivaju i krajnjim korisnicima, ali oni ne predstavljaju samo korisnike kao što su osobe već i uređaje kao što su server ili ruter, ili procese kao što su programi ili bilo šta što može biti identificirano imenom na certifikatu[33]. Subjekti certifikata se moraju registrovati da bi dobili certifikat i postali dio PKI.

Verzija certifikata (v1, v2, v3)	
Serijski broj certifikata	
Parametri potpisa (ID algoritma)	
Izdavač certifikata (X.500 CA ime)	
Period važenja certifikata	
Subjekat certifikata (X.500 ime)	
Informacije o javnom ključu subjekta ID algoritma | Javni ključ	
Jedinstveni ID izdavača	Verzija 2
Jedinstveni ID subjekta	Verzija 2
Proširenja	Verzija 3
Digitalni potpis	

Slika 1

3. Certifikacijska ustanova ili tijelo (*Certification Authority* - CA)

CA je potpisnik i izdavač certifikata. Primarne operacije CA su izdavanje certifikata, njihovo obnavljanje i po potrebi opozivanje. CA svojim potpisom garantuje ispravnost podataka u certifikatu. CA direktno ili preko registracijske ustanove registruje krajnje krosinike, subjekte certifikata, i verificira njihov identitet na odgovarajući način. CA ponekad obavlja i funkciju sigurnosnog pohranjivanja ključeva. CA su izvor povjerenja u PKI. Povjerenje je osnova na kojoj se zasniva PKI. Povjerenje se odnosi kako na CA tako i na sve procedure unutar PKI.

4. Registracijska ustanova ili tijelo (*Registration Authority* – RA)

Registracijska ustanova je opcionalna komponenta PKI. U zavisnosti od izvedbe PKI, CA može delegirati RA neke od administrativnih funkcija ili CA može sama obavljati sve te funkcije u kom slučaju je RA nepotrebna. Ako se RA koristi, uobičajena uloga joj je, kako i ime kaže, vezana za registraciju subjekata certificiranja. Ovo uključuje verificiranje identiteta subjekata koji se registriraju u PKI. Pored ove uloge RA može verficirati i ostale atribute subjekta certifikata, provjeriti da subjekat zaista posjeduje privatni ključ koji odgovara javnom ključu koji će se nalaziti na certifikatu ili čak generisati par ključeva za subjekta i predstavljati posrednika između subjekata i CA prilikom informisanja o kompromitovanju privatnog ključa. Sve ove administrativne funkcije su obavezan dio PKI i ako nema RA onda ih CA mora sama obavljati. Funkcije koje RA ne može obavljati su izdavanje cerifikata i lista opozvanih certifikata. I RA je subjekat certifikata koji ima svoj javni ključ i certifikat koji je potpisala CA..

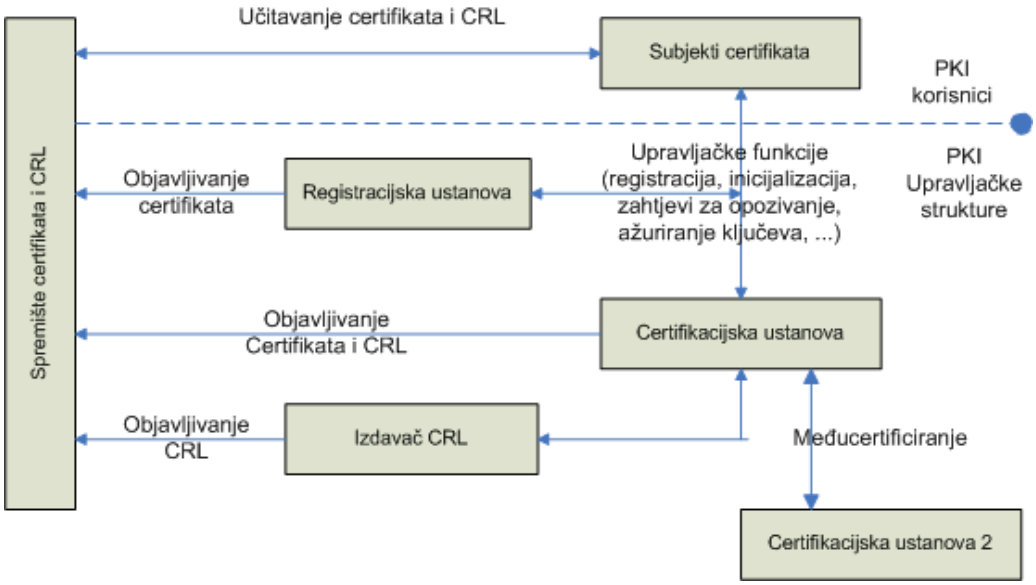
5. Spremište certifikata (*Certificate Repository*)

Certifikati moraju biti dostupni svim korisnicima PKI kako subjektima certifikata tako i aplikacijama i trećim stranama koje koriste certifikate za provjeru identiteta ili šifriranje poruka subjektima certifikata. Za ovo se koriste spremišta certifikata koja predstavljaju sistem ili skup distribuiranih sistema koji pohranjuju certifikate i liste opozvanih certifikata i služe kao sredstvo za na njihovu distribuciju krajnjim korisnicima [30]. Spremišta certifikata nisu obavezna komponenta PKI, ali se zbog svog doprinosa raspoloživosti i upravljivosti PKI gotovo podrazumijevaju. Pod spremištima certifikata se obično podrazumijevaju X.500 direktoriji, ali to ne mora biti slučaj. Spremišta mogu biti jednostavnije strukture kao što su obične datoteke na serveru dostupne preko FTP ili HTTP protokola. Pošto se X.509 format certifikata u potpunosti uklapa u X.500 direktorije ovo je i najbolji način za izvedbu spremišta certifikata. U tom slučaju se za pristup spremištu, direktoriju, uglavno koristi dominantni protokol za pristup direktorijima *Lightwaight*

Directory Access Protocol (LDAP) [34]. Postoje i drugi operativni protokoli koji se koriste za omogućavanje distribucije certifikata i lista opozvanih certifikata.

6. Liste opozvanih certifikata (*Certificate Revocation Lists* - CRL)

Certifikati se izdaju sa periodom važenja, ali pod različitim okolnostima oni mogu postati nevažeći i prije isticanja perioda važenja. Ovi razlozi mogu biti administrativni, kao što je promjena imena subjekta ili veze sa CA, ili sigurnosni kao što je kompromitovanje privatnog ključa subjekta. Liste opozvanih certifikata (CRL) su jedan od uobičajenih načina objavljivanja opozvanih certifikata zajedno sa razlogom za opozivanje. CRL je vremenski označena lista koja identificira opozvane certifikate potpisana od strane CA ili ovlaštenog izdavača CLR i slobodno dostupna u spremištu certifikata. Svaki opozvani certifikat je u CLR identificiran svojim serijskim brojem.[30]. Po novijoj literaturi [33], i standardizaciji [30] kao komponenta PKI se navodi Izdavač CLR, a ne sam CLR. Uobičajeno je da CA koja je izdala certifikate objavljuje i informacije o opozivanju tih certifikata. Međutim X.509 preporuke predviđaju mogućnost indirektnih CLR koje ne izdaje CA već neki drugi entitet kome je CA delegirala tu funkciju. Drugi, nešto noviji metod, objavljivanja opozvanih certifikata koji je u nekim slučajevima zamijenio CLR je *Online Certificate Status Protocol* (OCSP) [35].



Slika 2

2.6.2 Administracija

Na slici 2 je data struktura PKI sa osnovnim komponentama i interakcijama između njih. Interakcije se mogu podijeliti na administrativne i operativne protokole. Standardni administrativni protokoli u PKI su [36]:

1. Inicijalna registracija i certifikacija

Ovo je proces u kom se budući subjekat certificiranja registrira kod CA ili RA i dokazuje svoj identitet i druge atribute koji će se nalaziti na certifikatu. Ako se proces uspješno okonča CA izdaje certifikat sa javnim ključem subjekta koji se predaje subjektu certifikata i/ili objavljuje u javno dostupnom spremištu certifikata.

2. Sigurnosno pohranjivanje i oporavak parova ključeva

U zavisnosti od PKI politike i dizajna sistema privatni ključevi svih ili samo nekih subjekata mogu biti sigurnosno pohranjeni od strane CA ili RA. U tom slučaju moguće je napraviti oporavak ključeva koji su izgubljeni.

3. Ažuriranje parova ključeva

Parove ključeva je potrebno povremeno ažurirati. Ovo se radi u slučajevima kompromitovanja privatnog ključa ili zbog napredka tehnologije i potrebe za dužim ključevima. Ovo ažuriranje znači zamjenu starog para ključeva novim i izdavanje novog certifikata.

4. Ažuriranje certifikata (obnavljanje)

Pošto certifikati imaju period valjanosti potrebno ih je obnavljati na kraju tog perioda, ako nema razloga protiv toga ili bitnih promjena u sadržaju certifikata.

5. Zahtjevi za opozivanje certifikata

Zahtjeve izdaje ovlaštena osoba u slučaju potrebe za opozivanjem certifikata. Ove zahtjeve je neophodno odmah obraditi i ažurirati CLR.

6. Međucertificiranje

Dvije CA koje se nalaze u različitim sigurnosnim domenima mogu se uzajamno certificirati i time ostavarit lanac povjerenja između korisnika iz jednog i drugog domena.

Osnovne operativne funkije u PKI su vezane za spremišta certifikata i CRL i one su [36]:

1. Čitanje
2. Pretraživanje
3. Ažuriranje

2.6.3 Aplikacije

Aplikacije daju svrhu infrastrukturi javnih ključeva. One stvaraju upotrebnu vrijednost PKI. Ne postoji standardni skup aplikacija koje su dio PKI, ali bez bar jedne od njih PKI nema smisla. Svaka konkretna izvedba PKI uključuje skup aplikacija potrebnih za namjenu PKI. U izgrađenu PKI mogu se dodavati nove aplikacije koje imaju podršku za PKI. Aplikacije mogu biti iz

skupa standardnih aplikacija koje se kupuju od proizvođača softvera ili biti aplikacije razvijene unutar organizacije ili samo za organizaciju kojoj se PKI nalazi. Neke od aplikacija kao što su *Web browser*-i i e-mail klijenti standardno podržavaju certifikate i PKI. Ova podrška se zasniva na protokolima koji se oslanjaju na asimetričnu kriptografiju i certifikate. Ovi protokoli su:

1. S/MIME (*Secure Multi-Purpose Internet Mail Extensions*)

S/MIME je protokol koji dodaje mogućnost šifriranja i digitalnog potpisivanja e-mail poruka. S/MIME koristi RSA algoritam i *de facto* je standard za sigurnu e-mail komunikaciju podržan od većeg broja proizvođača softvera. Podrška za S/MIME je ugrađena u sve savremene *Web browser*-e.

2. SSL (*Secure Socket Layer*)

SSL [37] je protokol koji je razvila firma Netscape Communications Corporation i on omogućava siguran prenos podataka preko Interneta. SSL koristi mrežni nivo lociran između TCP (*Transport Control Protocol*) nivoa i aplikacijskog nivoa. SSL protokol obezbjeđuje sigurnost i integritet transmisionog kanala za podatke koje razmjenjuju aplikacije višeg nivoa kao što su HTTP, FTP i Telnet. SSL *Handshake* protokol sastoji se od dvije faze: autentikacije servera i opcionalno autentikacije klijenta. U prvoj fazi, server, u odgovoru na zahtjev klijenta šalje svoj certifikat i informaciju o preferiranom algoritmu šifriranja. Klijent generiše master ključ koji šifriran javnim ključem servera šalje nazad serveru. Server dešifruje master ključ i autenticira sebe klijentu vraćajući poruku autenticiranu master ključem. Dalje šifriranje i autentikacija se obavlja se sa ključevima koji su izvedeni iz master ključa. U drugoj opcionalnoj fazi server provjerava klijenta šaljući mu podatak na potpis. Klijent se autenticira serveru digitalno potpisujući podatak i prilažući svoj certifikat. SSL je bio *de facto* standard, ali se sada zamjenjuje zvaničnim standardom TLS.

3. TLS (*Transport Layer Security*)

TLS [38] je protokol koji je baziran na SSL verzija 3.0 i vrlo mu je sličan. TLS i SSL nisu interoperabilni. Ipak, poruke poslate koristeći TLS mogu obraditi i klijenti koji podržavaju SSL, a ne TLS.

Samo korištenjem savremenih *Web browser*-a i e-mail klijenata koji se isporučuju kao standardni dio svih savremenih operativnih sistema moguće je iskoristiti PKI. Moguće je ostvariti sigurno slanje elektronske pošte i sigurnu *Web* komunikaciju koja se oslanja na PKI i ove aplikacije. Pored ovih aplikacija novije verzije programskih paketa za rad sa dokumentima nude mogućnost njihovog digitalnog potpisivanja. Microsoft Office paket, od verzije XP podržava digitalno potpisivanje dokumenata koristeći X.509 PKI. Adobe Acrobat od verzije 4 takođe omogućava digitalno potpisivanje dokumenta. Oba paketa podržavaju i provjeru digitalnog potpisa nekog drugog subjekta.

2.7 Pregled postojećeg stanja u oblasti PKI

PKI nudi osnovu za praktičnu upotrebu kriptografije sa javnim ključem. Neke od mogućnosti PKI su, kroz pomenute protokole i aplikacije, iskorištene. Širu upotrebu PKI, kao i svake druge tehnologije, olakšavaju i stimulišu standardi. Standardizacija nekih aspekata PKI je data u International Telecommunications Union - Telecommunications (ITU-T) preporukama. Najvažnija od ovih preporuka je pomenuti format certifikata X.509 [31]. Internet *Request for Comments* (RFC) su formalni i neformalni standardi koje definiše *Internet Engineering Task Force* (IETF). Radna grupa za PKIX, što je skraćenica za *Public-Key Infrastructure* (X.509), pri IETF bavi se implementacijom Internet i X.509 baziranim PKI standardima i njihovi RFC se smatraju najšire prihvaćenim.

PKI je od svojih početaka rješenje koje obećava. Nažalost još uvijek broj izgrađenih PKI sistema nije ni blizu onome što se očekivalo prije nekih 10

godina kada su se početi prodavati prve komercijalne izvedbe PKI. OASIS PKI tehnički komitet je istraživao razloge relativno sporog rasta broja implementiranih PKI i glavne smetnje. Njihovi zaključci ukazuju da su glavne smetnje: nedostatak aplikacija koje podržavaju i koriste mogućnosti PKI, veliki troškovi uvođenja PKI i velika kompleksnost PKI rješenja [4].

Primjedba na mali broj aplikacija se odnosi na aplikacije posebne namjene iz različitih oblasti, jer osnovni skup aplikacija opšte namjene, kako je ranije rečeno, postoji. Troškovi uvođenja PKI zaista nisu mali, jer jedno prosječno PKI rješenje košta 750.000 EUR. Rješenje za veće organizacije košta znatno više, po nekoliko miliona EUR. U slučaju angažovanja vanjske firme za izgradnju PKI cijena po korisniku kreće od 50 EUR naviše [5]. Jedna od najvećih firmi koja nudi integrisna PKI rješenja, Verisign, navodi da su troškovi njihovog integrisanog rješenja od 33 USD po korisniku godišnje za velike organizacije od 10.000 korisnika do 80 USD i više za organizacija sa manje od 1000 korisnika [39]. PKI sistemi mogu biti vrlo kompleksni za uvođenje i održavanje. Administrativne procedure registracije i izdavanja certifikata zahtjevaju potvrđivanje identiteta svakog subjekta. Procedure upravljanja sa certifikatima i ključevima, a pogotovo provjeravanje statusa certifikata preko lista opozvanih certifikata mogu biti komplikovane i predstavljati veliko opterećenje na računarsku infrastrukturu. U slučajevima kada postoji međucertificiranje sa CA iz drugih domena utvrđivanje lanca povjerenja do CA kojoj korisnik vjeruje i lociranje listi opozvanih certifikata može postati komplikovano do neizvodivosti. Na ovu vrstu problema ukazuje sa u raznoj literaturi ali najbolji i najreferenciraniji pregled dao je Gutmann [40]. Pored ovih organizacionih problema postoji i problem korisnika. Zapravo to je problem na koji su prvo ukazali Whitten i Tygar [41], a tiče se upotrebljivosti sigurnosnih sistema. Savremene aplikacije koje omogućavaju šifriranje, digitalno potpisivanje, upravljanje ključevima i druge kriptografske operacije vrlo često nisu dovoljno jednostavne za rad da bi ih i obični korisnici računara, bez problema i sa jasnom predstavom šta rade, koristili.

Od PKI se očekivalo da riješi sve probleme sigurnih elektronskih komunikacija i ostvari sve namjene kriptografije na globalnom nivou. Ova su očekivanja bila nerealna te se danas ide u pravcu jednostavnijeg PKI ograničene namjene. PKI se pokazao kao vrlo koristan i nekomplikovan za održavanje u zatvorenim sistemima. PKI posebne namjene, kao što je SPKI [42] [43] za autorizaciju ili PGP za elektronsku poštu, su također primjeri uspješne primjene PKI. O pomenutim problemima i rješenjim za konkretan PKI će se govoriti u slijedećem poglavlju koje sa bavi izgradnjom konkretnog PKI.

P o g l a v l j e 3

3 PLAN IZGRADNJE INFRASTRUKTURE JAVNIH KLJUČEVA

Kako je u poglavlju o teoretskim osnovama rečeno PKI može omogućiti sigurne komunikacije u sistemu gdje je implementiran. Pod sigurnim komunikacijama se podrazumijevaju one u kojima su ostvarene četiri pobrojane namjene kriptografije: privatnost, integritet podataka, autentikacija i neporicanje. U teoretskim osnovama su objašnjeni prinicipi na kojima se zasniva PKI. No, prilikom izgradnje konkretnog PKI postoji niz praktičnih pitanja na koja treba odgovoriti. Na kraju prethodnog poglavlja navedeni su glavni problemi koji se javljaju prilikom uvođenja i eksploatacije PKI. U nastavku rada biće razmotrena, i na njih će biti odgovoreno, glavna pitanja vezana za izgradnju PKI na visokoškolskoj ustanovi. Prilikom određenih razmatarnja, gdje je potrebna dodatna preciznost u definisanju potreba i uslova rada, pretpostaviće se da se radi o fakultetu u Bosni i Hercegovini. Ovo ne bi trebalo uticati na univerzalnost i širu primjenjivost predloženih rješenja.

Prije nego što se pređe na detalje izrade plana navešće se argumenti koji idu prilog izgradnji ovakvog sistema i pricipijelni pristup rješavanju navedenih problema sa praktičnom izgradnjom PKI. Dosadašnja praksa je pokazala da je PKI dobro i izvodljivo rješenje za zatvorene sisteme. Ovdje se pod zatvorenim sistemom podrazumjeva jedna organizacija čiji su svi članovi na neki način, nezavisno od PKI, evidentirani u administrativnim službama organizacije i čiji se broj mijenja na predividiv način. Kako je visokoškoska ustanova tipičan primjer ovakvog sistema, uvođenje PKI bi trebalo biti dobro i izvodljivo rješenje za takvu ustanovu. Takođe je pokazano da uvođenje jednostavnijeg PKI ograničene namjene ima veće šanse za uspjeh. Iz ovog je razloga potrebno jasno definisati razumne ciljeve izgradnje PKI. Pod razumnim se ovdje podrazumjeva minimalan skup ciljeva koji zadovoljavaju

neposredne potrebe visokoškolske institucije za sigurnom elektronskom komunikacijom. Stoga će prvo biti obrađeno definisanje potreba. Ovdje će biti utvrđene aplikacije i subjekti certificiranja. Na osnovu utvrđenih potreba biće definisana potrebna konfiguracija certifikacijske ustanove, što uključuje i moguću registracijsku ustanovu Nakon definisanja konfiguracije CA biće definisana odgovarajuća konfiguracija digitalnih certifikata. Posljednji korak u definisanju elemenata infrastrukture javnih ključeva biće definisanje plana upravljanja certifikatima gdje će pored administrativnih procedura biti razmotrena i spremišta certifikata i liste opozvanih certifikata. Na ovaj način će biti definisani svi elementi PKI sa međusobnim interakcijama.

3.1 Definisanje potreba za digitalnim certifikatima

Prvi korak u izgradnji infrastrukture javnih ključeva, kao i kod svakog drugog projekta, je utvrđivanje potreba koje se žele zadovoljiti. Potrebe su osnova projekta koji definiše okvir unutar koga će se odvijati sve buduće aktivnosti. Utvrđivanje potreba možemo posmatrati kao bilo koji drugi proces donošenja odluka. Sa jedne strane imamo želju da napravimo sistem koji svojim korisnicima pruža sve usluge koje tehnologija omogućava. Sa druge strane imamo praktična ograničenja resursa kao što su novčana, vremenska, materijalna ograničenja, koja postavljaju granicu na ono što stvarno možemo napraviti. Za donošenje ispravne odluke, izbor dobrog rješenja, potrebno je precizno definisati problemsku situaciju koju rješavamo. Ovo znači da moramo utvrditi veličine na koje možemo uticati, takozvane upravljačke varijable. Moramo ustanoviti kako promjene ovih veličina utiču na naš cilj i time definišuću funkciju cilja. Nadalje, potrebno je pronaći uticaj promjene ovih veličina na potrebne resurse kao i raspoložive količine resursa čime se definiše model ograničenja. Ovim postupcima dolazimo do modela našeg sistema koji koristimo u daljem rješavanju problema. Za dobar model je od presudnog značaja da smo izdvojili minimalni skup veličina važnih za opis posmatranih karakteristika sistema. Navedeni pristup rješavanju problema je

standardni metod vrlo detaljno opisan u literaturi koja se bavi problematikom donošenja odluka [44], [45]. U literaturi koja se bavi implementacijom infrastrukture javnih ključeva, međutim, ovo nije uobičajen pristup. Problem modeliranja ove infrastrukture je kompleksan zadatak čiju je uspješnost teško provjeriti. Predmet ovog rada i nije kreiranje determinističkog matematičkog modela infrastrukture javnih ključeva, već projekat izgradnje ovakve infrastrukture. Međutim, navedeni postupak identifikacije upravljačkih varijabli te njihovog uticaja na željeni cilj i njihove povezanosti sa ograničenjima na resurse omogućava sistemski pristup rješavanju bilo kog problema donošenja odluka, pa i ovog kojim se rad bavi.

Definisanje potreba je zapravo utvrđivanje usluga koje želimo da naš sistem pruži svojim korisnicima. Usluge informacionog sistema pružaju se korisnicima putem računarskih aplikacija, te je definisanje usluga zapravo definisanje aplikacija koje će pružati te usluge. Svaka aplikacija utiče na korisnost sistema u pozitivnom smislu, ali takođe zahtjeva resurse za njeno kreiranje i korištenje. Ako se pretpostavi da je mjerilo uspješnosti infrastrukture njena korisnost onda je to i funkcija cilja. U tom slučaju skup izabranih aplikacija predstavlja, na ovom nivou apstrakcije, upravljačke varijable.

U objašnjenju šta predstavlja definisanje potreba, pored usluga navodi se i drugi važan pojam – korisnici. Svaki korisnik sistema zahtjeva određene resurse, ali veći broj korisnika povećava korisnost sistema. Korisnici ne moraju biti svi jednaki po svojim pravima, odnosno ne moraju svi korisnici imati pristup svim uslugama sistema. Korisnike je moguće svrstati u grupe sa istim nivoom potreba. Na osnovu rečenog može se zaključiti da grupe korisnika sa brojevima svojih članova predstavljaju drugi skup upravljačkih varijabli. Znači potrebno je utvrditi koje će aplikacije sistem nuditi kojim korisnicima. U ovom postupku potrebno je utvrditi i uticaj odluka o aplikacijama i korisnicima na potrebne resurse. Neophodno je definisati

potrebni nivo korisnosti sitema te raspoložive resurse. Navedene veličine nije moguće brojčano izraziti, ali se mogu utvrditi okviri unutar kojih se mogu kretati, poštujući principe definisane u uvodu rada. Težina projektantske odluke se sastoji upravo u donošenju odluke u uslovima nedovoljne definisanosti problema. Naredna dva razmatranja će da predlože i obrazlože odgovor na postavljena pitanja. Nakon toga se na osnovu donesenih odluka opisuje dokumentovanje korištenja sistema, koje postaje projektni zadatak i pravni temelj budućeg korištenja infrastrukture javnih ključeva.

3.1.1 Definisanje aplikacija koje koriste certifikate

Kako je u uvodu ovog poglavlja rečeno, prvi korak u izgradnji infrastrukture javnih ključeva je utvrđivanje sigurnosnih usluga koje će sistem da pruža korisnicima. Ove usluge su uslovljene definisanim potrebama. Usluge se pružaju putem aplikacija, tako da je zapravo potrebno definisati aplikacije koje će koristiti digitalne certifikate koje obezbjeđuje PKI. Ove aplikacije se mogu podijeliti u dvije osnovne grupe.

Prvu grupu bi predstavljale standardne aplikacije koje dolaze kao dio operativnog sistema ili softverskih paketa koji se standardno instaliraju na korisničke računare. Tipični predstavnici ovih aplikacija su *Web browser* i e-mail klijent. Drugu grupu predstavljaju aplikacije posebne namjene, bilo da su one nabavljene od specijalizovanih proizvođača softvera ili da su razvijane unutar same organizacije u kojoj se gradi PKI. Razloga za ovakvu podjelu je podrška za PKI koja može biti ugrađena u aplikaciju ili ne. Sve savremene verzije aplikacija iz prve grupe imaju ugrađenu podršku za rad sa certifikatima. To znači da se ove aplikacije u svom postojećem obliku mogu koristiti za pružanje njima predviđenih sigurnih usluga uz korištenje certifikata. Ovdje će detaljnije biti navedene samo aplikacije i usluge za koje se utvrdi da su potrebne za zadovoljavanje planiranih potreba sistema. Aplikacije iz druge grupe, mogu imati ugrađenu podršku za PKI, ali moguće je i da je takvu

podršku potrebno ugraditi, ako je moguće, ili čak ponekad u potpunosti iznova napraviti aplikaciju.

Premda je spomenuto da se usluge pružaju kroz aplikacije, ovo nije potpuno preslikavanje jedan na jedan, već je moguće da neka aplikacija pruža više usluga ili obratno. Osnovne usluge su već opisane u dijelu sa teorijskim opisom PKI, a u njih spadaju šifiranje i dešifriranje podataka u transportu i pri pohranjivanju, digitalni potpisi i autentikacija. Različite aplikacije, zbog različite namjene nude ove sigurnosne usluge u različitim oblicima. Sigurna elektronska pošta podrazumjeva mogućnost šifriranja/dešifiriranja poruka i/ili njihovo digitalno potpisivanje. Sigurni *Web* transfer omogućava autentikaciju obje strane u komunikaciji i šifriranje podataka koje one razmjenjuju. Potpisivanje koda programa omogućava, kao i svako drugo digitalno potpisivanje, autorima zaštitu rada, a korisnicima potvrdu izvora programa.

Poštujući usvojeni princip izgradnje jednostavnog PKI ograničene namjene, a uzimajući u obzir trenutne potrebe visokoškolske institucije za sigurnom elektronskom komunikacijom, predlaže se sljedeći skup usluga koje PKI treba da podržava:

- Nastavno osoblje treba da ima ima mogućnost objavljivanja zvaničnih potpisanih rezultata provjera znanja na visokošolskom intranetu i/ili Internetu.
- Studenti treba da imaju mogućnost prijavljivanja ispita preko *Web*-a.
- Dekan i rukovodstvo trebaju imati mogućnost objavljivanja zvaničnih potpisanih dokumenta visokoškolske institucije na lokalnom intranetu.
- Administracija treba da ima mogućnost objavljivanja dokumenata koji su u njihovoj nadležnosti.
- Svim korisnicima sistema je potreban siguran pristup dokumentima kojima su ovlašteni da pristupe.
- E-mail komunikacija treba da bude šifrirana i potpisana.

Ovdje se govori samo o omogućavanju sigurnog objavljivanja i pristupa dokumentima što je uloga PKI. Pitanje koji su to dokumenti koji će biti objavljeni i kojima će biti omogućen pristup nije predmet ovog rada već interne politike visokoškolske ustanove.

Kao ciljevi izgradnje konkretnog PKI navedeni su, ukratko rečeno, sigurna e-mail komunikacija, sigurna Web autentikacija i objavljivanje digitalno potpisanih podataka preko Web-a. Iz ovoga slijedi da su potrebne aplikacije savremeni e-mail klijent programi i W*eb browser*, te minimalno *Web* programiranje. Savremeni e-mail klijent programi (Outlook, Outlook Express, Lotus Notes) imaju ugrađenu podršku za S/MIME. S/MIME kako je u dijelu sa teoretskim osnovama objašnjeno omogućava šifriranje i digitalno potpisivanje poruka uz korištenje digitalnih certifikata. Savremeni Web *browser*-i (Internet Explorer, Netscape) imaju ugrađenu podršku za SSL i TLS. Oba ova protokola, kako je ranije objašnjeno, omogućavaju šifriranje podataka koje W*eb* server i klijent razmjenjuju, kao i uzajamnu autentikaciju uz pomoć certifikata. Znači korištenjem dvije aplikacije, koje su standardni dio svakog poslovnog računarskog okruženja, izgrađena PKI bi bila funkcionalana i zadovoljila definisane potrebe. To je i jedna od ideja ovog rada: da se iskoristi što više dostupnih komponenata omogućavajući izgradnju operativne PKI uz minimalne zahtjeve za materijalnim i ljudskim resursima. Važno je reći da ova odluka ni na koji način ne ograničava dodavanje novih aplikacija koje podržavaju PKI u sistem, jer će infrastruktura biti izgrađena poštujući standarde koji će omogućiti interoperabilnost sa budućim aplikacijama.

3.1.2 Definisanje korisnika koji dobijaju certifikate

Nakon što su utvrđene aplikacije potrebne za zadovoljavanje definisanih potreba neophodno je odrediti kategorije korisnika ovih usluga. Pod korisnicima se podrazumjevaju ljudi, računari i računarski programi. Korisnici će se aplikacijama predstavljati putem certifikata i na osnovu tipa certifikata će

im biti dodijeljena odgovarajuća prava i odgovornosti. Prvi korak je određivanje grupa korisnika sa identičnim potrebama i pravima. Svi korisnici koji su članovi neke grupe imaće isti tip certifikata. Grupe bi trebale odgovarati organizacionim jedinicama i funkcijama unutar sistema u kom se uvodi PKI. Nakon što su utvrđene grupe potrebno je za svaku grupu utvrditi [46]:

- Tip potrebnog certifikata
- Broj korisnika u grupi
- Fizička lokacija korisnika
- Potrebni nivo sigurnosti
- Potrebni broj certifikata po korisniku
- Uslove za dobivanje certifikata

Za konkretnu organizaciju kao što je visokoškolska ustanova može se napraviti slijedeće grupiranje korisnika:

- Nastavno osoblje
- Studenti
- Službe
- Rukovodstvo
- Administratori računarske mreže i PKI

Na osnovu definisanih usluga koje će sistem pružati i utvrđenih grupa korisnika definišu se potrebni parametri certifikata za sve grupe korisnika. U tabeli 1 je dat prijedlog maksimalnog očekivanog broja korisnika u svakoj od grupa za tipičnu visokoškolsku instituciju u BiH, namjena certifikata na osnovu definisanih potreba i potrebni nivo sigurnosti. Svi korisnici sistema su interni sa po jednim certifikatom, a uslov za dobivanje certifikata je povezanost sa visokoškolskom ustanovom, odnosno pripadnost jednoj od grupa korisnika.

POTREBE KORISNIKA ZA CERTIFIKATIMA			
Grupa	**Broj**	**Namjena**	**Sigurnost**
Nastavno osoblje	200	E-mail, *Web* autentikacija, digitalni potpis	Srednja
Studenti	5000	E-mail, *Web* autentikacija, digitalni potpis	Srednja
Službe	50	E-mail, *Web* autentikacija, digitalni potpis	Srednja
Rukovodstvo	10	E-mail, *Web* autentikacija, digitalni potpis, autentikacija pametnim karticama	Visoka
Računarski administratori	10	E-mail, *Web* autentikacija, digitalni potpis, autentikacija pametnim karticama	Visoka

Tabela 1

3.1.3 Definisanje i dokumentovanje politike korištenja certifikata

Nakon što su definisane potrebe koje buduća infrastruktura javnih ključeva treba da ispunjava neophodno je definisati namjenu, te prava i obaveze koje proističu iz korištenja infrastrukture. U literaturi se često izdavanje certifikata poredi sa izdavanjem pasoša ili drugih ličnih dokumenata [47]. Lični dokumenti se izdaju sa ciljem dokazivanja identiteta. Većina ovih dokumenata, u suštini, povezuje ime sa slikom. Uz sliku i podatke o imenu upisuju se dodatni lični podaci koji preciznije definišu osobu, jer samo ime ne mora biti jedinstveno, te podaci koji identificiraju dokument. Lične dokumente izdaje ovlaštena institucija. Ovlaštena institucija garantuje trećim licima ispravnost podataka na dokumentu. Treća lica treba da imaju jednostavan način da provjere autentičnost dokumenata. Da bi sve ovo funkcionisalo potrebno je povjerenje među svim učesnicima. Povjerenje je

zasnovano na jasno definisanim, odobrenim i objavljenim politici i procedurama izdavanja i korištenja ličnih dokumena. Politika izdavanja definiše uslove dobivanja ovih dokumenata, uslove korištenja te prava i obaveze nosioca dokumenta, institucije koja ga je izdala, te trećih lica koja koriste dokument za provjeru identiteta. Procedure precizno opisuje sve korake u procesu izdavanja ličnih dokumenata, potrebnu prateću dokumentaciju te postupke za sve situacije, kao što su promjena podataka, gubitak dokumenta i slično. Potrebno je pomenuti razliku između međunarodnih putnih dokumenata, npr. pasoš, i lokalnih dokumenata za identifikaciju, npr. lična karta. Lokalni dokument za identifikaciju se koristi unutar zatvorenog sistema (država, opština, kompanija) i institucija koja ga je izdala je dio tog sistema kome svi unutar sistema vjeruju. Međunarodni putni dokumenti se koriste van sistema čija insitucija ih je izdala, ali se na osnovu međunarodno prihvaćenih politike i procedura izdavanja prihvataju.

Digitalni certifikati imaju funkciju ličnih dokumenata kojima se dokazuje identitet u svijetu elektronskih komunikacija. Cetifikat povezuje neki subjekat (čovjek, računar, aplikacija) sa njegovim javnim ključem. Certifikate izdaje certifikacijska ustanova. Certifikacijska ustanova garantuje trećim subjektima ispravnost podataka na certifikatu. Treći subjekti na osnovu digitalnog potpisa certifikacijske ustanove provjeravaju autentičnost certifikata. Kao i kod ličnih dokumenata, funkcionisanje infrastrukture javnih ključeva zasniva se na povjerenju. I ovdje je povjerenje zasnovano na jasno definisanim, odobrenim i objavljenim politici i procedurama izdavanja cerifikata. Skup uslova kreiranja, izdavanja i korištenja digitalnih certifikata naziva se, u PKI literaturi, Politika certificiranja (*Certificate Policy*). Internet Engineering Task Force (IETF) je objavio dokument "Certificate Policy and Certification Practices Framework" [48] koji daje okvir onog što bi trebalo biti definisano u politici certificiranja. Ovaj dokument definiše politiku certificiranja kao "imenovani skup pravila koji ukazuje na primjenljivost certifikata u određenoj zajednici i/ili klasi aplikacija sa zajedničkim sigurnosnim zahtjevima". Skup procedura kojima se

provodi politika certificiranja, u PKI literaturi, naziva se Izjava o praksi certificiranja (*Certification Practice Statement*). IETF *Framework* definiše ovaj dokument kao "izjavu o procedurama koje certifikacijska ustanova provodi pri izdavanju certifikata". Politika certificiranja i Izjava o praksi certificiranja su obavezujući dokumenti za certifikacijsku ustanovu. Na osnovu ovih dokumenata treći subjekti mogu ocjeniti koliko povjerenja mogu imati u certifikate izdate od strane certifikacijske ustanove. Treći subjekti mogu biti iz sigurnosnog domena certifikacijske ustanove ili iz sasvim drugog sigurnosnog domena.

Konkretna Politika certificiranja direktno zavisi od namjene infrastrukture javnih ključeva za koju se definiše ova politika. Jednostavno rečeno, Politika certificiranje se može posmatrati kao dokumentovanje onoga što se želi uraditi [47]. Ovaj dokument može biti veoma obiman za velike međunarodne certifikacijske ustanove kao što je neprofitabilna organizacija EuroPKI [49]. Za internu upotrebu u zatvorenom sistemu moguće je napraviti kraći i manje detaljan dokument, ali koji opet mora imati sve bitne elemente. Ovi neophodni elementi Politike certificiranja su odgovori na pitanja [50]:

- Ko je odgovoran za rad Certifikacijske ustanove?
- Koju zajednicu Certifikacijska ustanova opslužuje?
- Koja su pravila identifikacije subjekata certificiranja?
- Šta je sadržaj certifikata?
- Kakva ograničenja su postavljena na rad Certifikacijske ustanove?
- Šta se mora uraditi u slučaju bilo kakve neregularnosti?

Na osnovu definisane Politike certificiranja kreira se Iskaz o praksi certficiranja. Jednostavno rečeno, Iskaz o praksi certificiranja se može posmatrati kao dokumentovanje onoga kako je potrebno uraditi ono što je definisano u Politici certificiranja [47]. Kako je ovaj dokumenat posljedica Politike certificiranja njegov sadržaj i obim zavise od te politike. Izjava o praksi certificiranja za VeriSign, jednu od najvećih certifikacijskih ustanova na

svijetu je vrlo detaljan i obiman dokument [51]. Sažetija Politika certificiranja za rezultat imaće i sažetiji Iskaz o praksi certificiranja.

Prijedlog izgleda Politike certificiranja na visokoškolskim institucijama objavljen je od strane Internet2, radne grupe za PKI u visokom obrazovanju [52]. Međutim i ovaj dokument je veoma obiman i nepraktičan za implementaciju. Ovoga su bili svjesni i u radnoj grupi, te su pokrenuli ideju PKI *Lite*, za inicijalno lakše uspostavljanje infrastrukture javnih ključeva na visokoškolskim ustanovama [53]. Ideje iza ovog projekta bliske su idejama ovog rada. Iz ovog razloga primjer Politike certificiranja i Izjave o praksi certificiranja koji je predložen u sklopu PKI *Lite* inicijative [54] može biti uzet kao početni model za ova dva dokumenta. Za izgradnju infrastrukture javnih ključeva na visokoškolskoj ustanovi, kakva se obrađuje u ovom radu, certifikacijska politika je rezultat definisanih ciljeva izgradnje infrastrukture. Jasni i kratki odgovori na na neka od navednih pitanja se mogu dati već sada:

- Ko je odgovoran za rad Certifikacijske ustanove?
    - Visokoškolska ustanova (fakultet ili univerzitet).
- Koju zajednicu Certifikacijska ustanova opslužuje?
    - Visokoškolsku ustanovu (fakultet ili univerzitet) sa svim njenim subjektima.

Do odgovora na druga pitanja

- Koja su pravila identifikacije subjekata certificiranja?
- Šta je sadržaj certifikata?
- Kakva ograničenja su postavljena na rad Certifikacijske ustanove?
- Šta se mora uraditi u slučaju bilo kakve neregularnosti?

će se doći u nastavku rada. Na osnovu ovih odgovora može se definisati Politika certificiranja, a potom i Iskaz o praksi certificiranja.

3.1.4 Rezime

U ovoj glavi koja se bavi definisanjem potreba za digitalnim certifikatima utvrđen je skup usluga koje PKI treba da pruža. Ove usluge su *Web* autentikaciija, digitalno potpisivanje i sigurna e-mail komunikacija. Na osnovu ovog skupa usluga definisane su potrebne aplikacije koje ih pružaju. Potrebne aplikacije su *Web* browser i e-mail klijent, koji su standardni dio svakog poslovnog računarskog okruženja, te minimalna količina *Web* baziranih programa. Utvrđene su grupe korisnika ovih usluga te definisane njihove potrebe za certifikatima koji će im omogućiti navedene usluge. Otvoreno je pitanje dokumentovanja PKI kroz dva dokumenta: Politiku certificiranja i Izjavu o praksi certificiranja. Politika certificiranje se može posmatrati kao dokumentovanje namjene PKI. Izjava o praksi certificiranja se može posmatrati kao dokumentovanje onoga kako je potrebno uraditi ono što je definisano u Politici certificiranja. U nastavku rada će biti odgovoreno na otvorena pitanja vezana za sadržaj ovih dokumenata.

3.2 Definisanje konfiguracije CA

U prethodnoj glavi utvrđene su potrebe za certifikatima. Definisane su aplikacije koje je potrebno podržavati. Utvrđene su grupe korisnika buduće infrastrukture javnih ključeva. Razmotrena je politika i praksa certificiranja na osnovu donesenih odluka. Sa ovim podacima moguće je pristupiti definisanju infrastrukture potrebne za podršku utvrđenim ciljevima. Osnova PKI je Certifikacijska ustanova (CA). Šta je CA i koja je njena funkcija objašnjeno je u uvodnom teoretskom dijelu definisanja osnovnih pojmova u PKI. CA o kojoj će se u daljem tekstu govoriti je zapravo program koji obavlja funkciju certifikacijske ustanove. Pošto je CA osnova PKI prvi korak u izgradnji PKI nakon definisanih potreba je utvrđivanje kakva CA je potrebna da bi se zadovoljile definisane potrebe. Potrebno je razmotriti sve aspekte uspostavljanja CA.

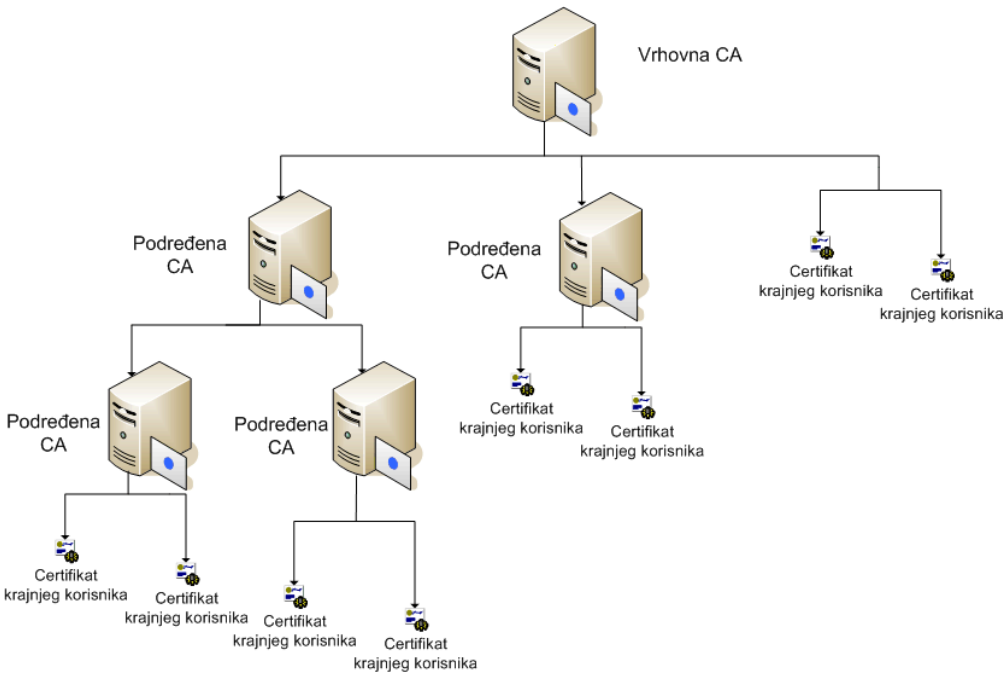
3.2.1 Izbor modela povjerenja (*Trust model*)

Prije utvrđivanja konkretnih parametara CA potrebno je izbrati model povjerenje u kom će CA djelovati. Povjerenje je osnova sigurnih komunikacija. Zapravo svaka vrsta identifikacije, koja je prvi princip sigurnih komunikacija, je zasnovana na povjerenju. Ljude i predmete koje neposredno poznajemo identificiramo direktno. Ljude i predmete koje ne poznajemo direktno identificiramo preko nekog drugog. Dijete pojmove upoznaje preko roditeljima kojima nerazmišljajući vjeruje da za njega ispravno identificiraju sve oko njega. Odrasli upoznaju nove prijatelje preko starih prijatelja kojim vjeruju. Potpune strance u službenim kontaktima identificiramo preko identifikacijskih dokumenata. Ovim dokumentima vjerujemo jer ih je izdala ustanova kojoj vjerujemo jer je izdala i naše identifikacijske dokumente. Mi vjerujemo i identifikacijskim dokumentima koje je izdala neka druga ustanova, a ne naša na osnovu toga što je naša ustanova kojoj vjerujemo rekla da vjeruje toj drugoj ustanovi. Pobrojani primjer zapravo predstavljaju modele povjerenja.

Postoji više formalnih podjela modela povjerenja u svijetu digitalnih certifikata [48] [32], ali bi se osnovna podjela mogla napraviti na direktno i indirektno povjerenje. Kao i u realnom svijetu direktno povjerenje znači da certifikatu vjerujemo jer znamo čiji je, odnosno sami smo se, na neki način, mogli uvjeriti da certifikat pripada svom navedenom vlasniku. Ovaj model u svijetu savremenih elektronskih komunikacija nema veliku praktičnu primjenu osim za uski krug ljudi koji se međusobno poznaju i žele da koriste certifikate za međusobno komuniciranje. Međutim kompletna ideja asimetrične kriptografije bila je da omogući ljudima koji se ne poznaju da elektronski komuniciraju sigurno i sa povjerenjem. Ovo implicira model indirektnog povjerenja. Indirektno povjerenje opet ima dvije glavne grupe koje zapravo predstavljaju modele povjerenja koje ljudi koriste u privatnim i poslovnim kontaktima.

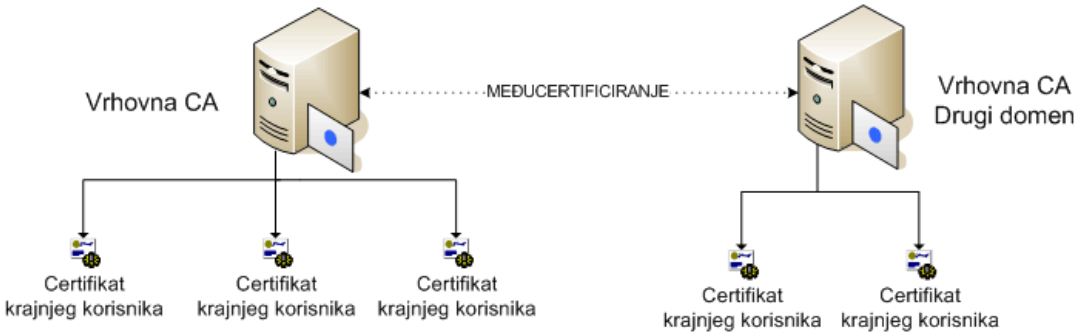
U privatnim kontaktima ljudi se oslanjaju na preporuke drugih ljudi koje poznaju. Ovaj model se u PKI terminologiji naziva mreža povjerenja (*Web of Trust*). Mreža povjerenja je kombinacija direktnog i hijerarhijskog povjerenja gdje certifikate ne potpisuje CA već se korisnici uzajamno certificiraju. Neki certifikat može potpisati svaki od korisnika koji mu vjeruje i označiti jedan od unaprijed definisanih stepena povjerenja. Veći broj potpisa višeg nivoa povjerenja bi trebao da pozitivno utiče na vjerodostojnost certifikata. Konačnu odluku o vrijednosti certifikata, ipak, donosi korisnik, kome je certifikat pokazan kao identifikacijski dokument, na osnovu njegovog povjerenja u sve potpisnike certifikata [32]. Premda ovo zvuči malo komplikovano u praksi vrlo dobro funkcioniše jer je zasnovano na modelu povjerenja koji ljudi koristime u svakodnevnom životu. IETF PKIX radna grupa ima model povjerenja koji je sličan ovome. Oni ga nazivaju model korisničke perspektive. Pod korisnikom se ovdje podrazumijeva onaj koji prihvata certifikat, procijenjuje njegovu vrijednost i na osnovu toga pruža neke usluge ili daje prava. Naziv modela je i njegov opis jer odluka o validnosti certifikata je na korisniku i njegovoj procjeni.

U poslovnim kontaktima ljudi se više oslanjaju na identificiranje poslovnih saradnika od strane neke organizacije kojoj oni pripadaju. Zapravo vjeruju da se neko unutar organizacije pobrinuo za pozitivnu identifikaciju i jamči za identite svog člana. Ovo u suštini predstavlja hijerahijski model povjerenja. Standardni hijerahijski model povjerenja je zasnovan na jednoj vrhovnoj certifikacijskoj ustanovi od koje potiču svi certifikati unutar njenog domena. Vrhovna certifikacijska ustanova izdaje certifikate drugim, podređenim, certifikacijskim ustanovama i/ili krajnjim korisnicima. Podređene certifikacijske ustanove opet mogu izdavati certifikate drugim certfikacijskim ustanovama i/ili krajnjim korisnicima. Na ovaj način se svaki certifikat izdat unutar domena može povezati sa vrhovnim certifikatom i povjerenje u certifikate se zasniva na povjerenju u vrhovnu certifikacijsku ustanovu i kompletan lanac certifikacije do korisničkih certifikata. Dobre strane ovog modela su mogućnost centraliziranog upravljanjanja infrastrukturom javnih ključeva. Vrhovna CA može kroz formu certifikata nametnuti dogovorenu politiku za sve certifikate u domenu. Česta upotreba ove politike je za provođenje potitike imenovanja CA i krajnjih korisnika. Ovaj model odgovara čvrsto ustrojenim organizacijama gdje hijerarhija CA oslikava hijerarhiju organizacije. Uspostavljanje povjerenja sa certifikatima van domena ostvaruje se uzajamnim certificiranjem (*cross-certification*) vrhovnih certifikacijskih ustanova iz dva domena. [30]. Prikaz hijerarhijskog modela povjerenja dat je na slici 3.



Slika 3

Pored standardnog hijererhijskog modela povjerenja postoje još dva modela hijerarhijskog tipa. Hijerarhijski model može postati veoma glomazan tako da se lanac certificiranja između korisničkog certifikata i vrhovne certifikacijske ustanove može biti veoma dugačak. Dva korisnika unutar istog domena koji trebaju sigurno komunicirati moraju vjerovati nekoj udaljenoj certifikacijskoj ustanovi. Lokalni model povjerenja eliminiše duge lance certificiranja. Korisnici vjeruju certifikatima koje je potpisala certifikacijska ustanova koje je izdala i njihov certifikat. Ideja je da lokalna certifikacijska ustanova najbolje poznaje potrebe svojih direktnih korisnika i da oni u nju imaju najviše povjerenja. Za komunikaciju sa korisnicima iz drugih lokalnih domena lokalne certifikacijske ustanove se uzajamno certificiraju. Glavna prednost ovog modela je njegova fleksibilnost. Lokalni model popvjerenja je prikazan na slici 4.

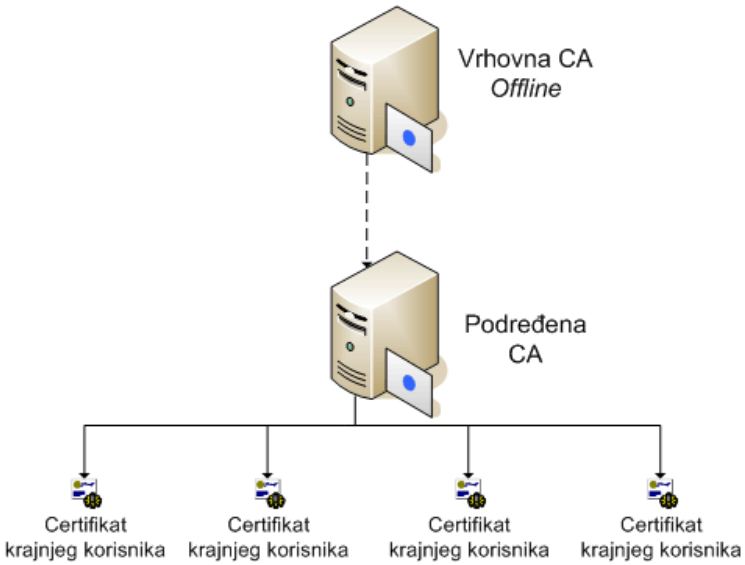


Slika 4

Model povjerenja koji se u praksi najviše koristi je model pohranjenih vrhovnih certifikacijskih ustanova. Ovaj model se najviše koristi jer je ugrađen u sve savremene W*eb browser*-e. Prilikom pristupa sigurnim web lokacijama, HTTPS protokol, identifikacija servera kom se pristupa te šifriranje buduće komunikacije obavlja se na osnovu certifikata koji *Web* server prezentira *browser*-u. Prezentirani certifikat mora biti povezan lancem certificiranja sa jednom od vrhovnih certifikacijskih ustanova predefinisanih u samom *browser*-u. Ovo je hijerarhijski model sa više vrhovnih certifikacijskih ustanova koje nisu uzajamno certificirane već im se svima ravnopravno vjeruje. Povjerenje u ovom modelu je zasnovano na povjerenju u proizvođača W*eb browser*-a koji garantuje vjerodostojnost certifikata ugrađenih vrhovnih certifikacijskih ustanova. Korisnici W*eb browser*-a mogu i dodavati vrhovne certifikacijske kojima oni izaberu da vjeruju. (Autor smatra da ovaj model ima sigurnosnih nedostataka. Pohranjivanje skupa vrhovnih certifikacijskih ustanova lokalno na računaru uz mogućnost dodavanja drugih certifikacijskih ustanova otvara mogućnost, ne baš jednostavnu, ali mogućnost, nedobronamjerne manipulacije skupom certifikacijskih ustanova kojima se vjeruje. Teoretski je moguće i bez znanja korisnika dodati vrhovnu certifikacijsku ustanovu u skup te uspostaviti povjerenje koje ne dolazi od proizvođača *browser*-a niti od samog korisnika.)

Konkretan model koji bi odgovarao planiranoj infrastrukturi javnih ključeva na visokoškolskoj instituciji bi mogao biti kombinacija standardnog

hijererhijskog i lokalnog modela povjerenja, koristeći i pohranjivanje certifikacijskih ustanova od povjerenja. Cilj je da se iskoriste dobre strane svakog od modela. Sve certifikate, za određenu grupu korisnika bi izdavala jedna certifikacijska ustanova što odgovara lokalnom modelu povjerenja. Grupa korisnika može obuhvatati i sve korisnike certifikata. Ovaj model je pogodan za relativno zatvoren krug korisnika kakav je na visokoškolskoj ustanovi. Certifikat korisničke certifikacijske ustanove bi bio izdat od strane vrhovne certifikacijske ustanove što odgovara standardnom hijererhijskom modelu povjerenja. Razlog za kreiranje hijerarhije sa posebnom vrhovnom certifikacijskom ustanovom je povećana sigurnost što će kasnije biti detaljnjije obrazloženo. Pošto planirane aplikacije imaju ugrađenu podršku za model pohranjenih vrhovnih certifikacijskih ustanova, lokane certifikacijske ustanove visokoškolske institucije bi bile dodate u ovaj skup certifikacijskih ustanova od povjerenja. Ovo dodavanje bi bilo obavljeno od strane administratora. Onemogućavanje dodavanja drugih certifikacijskih ustanova u ovaj skup od strane krajnjih korisnbika treba biti ozbiljno razmotreno. Namjera je da se iskoriste pogodnosti ovog modela koje olakšavaju uvođenje certifikata u upotrebu. Prikaz predloženog modela povjerenja je na slici 5.



Slika 5

3.2.2 Interna-eksterna CA

Prva odluka koju je potrebno donijeti pri definisanju potrebne CA je da li će ona biti interna ili eksterna CA. Interna CA se uspostavlja unutar zajednice u kojoj se gradi PKI i održava se unutrašnjim resursima. Eksterna CA podrazumjeva korištenje CA koja je uspostavljena i održavana od strane nekog van organizacije. Obje varijante imaju svoje prednosti i mane. Ova dva rješenja ne isključuju jedno drugo i moguća je njihova kombinacija.

Interna CA se smatra dobrim izborom za organizacije čiji će se certifikati uglavnom koristiti unutar same organizacije. Glavne prednosti su [46]:

- Omogućava da organizacija ima direktnu kontrolu nad svojom sigurnosnom politikom
- Omogućava usklađivanje politike certificiranja sa ukupnom sigurnosnom politikom
- Može biti integrisana sa postojećom informatičkom infrastrukturom
- Može se proširivati funkcionalnost i broj korisnika uz relativno male dodatne izdatke

Neki od nedostataka interne CA su [46]:

- Organizacija mora sama upravljati svojim certifikatima
- Vrijeme potrebno za stavljanje u funkciju obično je duže nego kod eksterne CA
- Organizacija mora preuzeti odgovornost za probleme sa PKI

Eksterna CA je dobro rješenje za organizacije koje veliki broj poslova za koje su potrebni certifikati obavljaju sa subjektima izvan organizacije. Prednosti ovog izbora su:

- Spoljni partneri mogu imati veće povjerenje u certifikate treće, profesionalne, strane
- Omogućava korištenje sigurnosnih tehnologija zasnovanih na certifikatima pri izgradnji internog PKI

- Koristi se tehnološko znanje institucije koja se specijalizovala za CA
- Koristi se poznavanje tehničkih, pravnih i poslovnih aspekata korištenja certifikata koje kompanija koja prodaje CA posjeduje

Nedostaci ovog rješenja su:

- Obično visoka cijena po certifikatu
- Smanjena fleksibilnost pri konfigurisanju i upravljanju certifikatima
- Neophodno je imati stalnu vezu sa vanjskom CA
- Ograničena integracija sa internom informatičkom infrastrukturom

Moguće je kombinovati ova dva rješenja sa ciljem korištenja dobrih strana svakog od njih. Upotreba vanjske CA za vrhovnu CA koja samo certificira interne CA koji obavljaju ostale poslove sa certifikatima je jedno od rješenja koje pruža povjerenje spoljnjim partnerima, a većinu kontrole zadržava unutar organizacije.

Za izgradnju PKI na visokoškolskoj instituciji kako je ovdje definisana očigledan izbor je interna certifikacijska ustanova. Planirana upotreba certifikata je interna, a visoka cijena vanjskog rješenja je neprihvatljiva. Neophodno je napomenuti da se ovim ne isključuje mogućnost uvezivanja se drugim institucijama, visokoškolskim ili drugim, na bazi vanjskog CA kome bi uvezane strane vjerovale. Ovo se može postići pomenutim uzajamnim certificiranjem.

3.2.3 Potrebni broj CA i njihove funkcije

Kada je poznata namjena certifikata, izabran model povjerenja i odlučeno da se koristi interna CA potrebno je utvrditi potrebni broj CA koje će izdavati certifikate i upravljati njima. Prvi korak u određivanju broja CA je utvrđivanje potrebnih tipova CA po namjeni. U suštini CA može biti:

- Vrhovna CA – Sama potpisuje svoj certifikat i povjerenje svih korisnika unutar domene je zasnovano na povjerenju u ovu certifikacijsku ustanovu.
- Podređena CA – Njen certifikat je potpisan od strane druge CA.

Unutar jednog domena u standardnom hijerarhijskom modelu povjerenja nalazi se samo jedna vrhovna CA. Broj podređenih CA zavisi od izvedbe PKI. Moguće su izvedbe i bez podređenih CA, gdje je vrhovna CA istovremeno i jedina i ona koja izdaje certifikate krajnjim korisnicima. Takođe je moguće postojanje velikog broja podređenih CA raspoređenih u više hijererhijskih nivoa. Pošto je osnovna zadaća CA izdavanje certifikata uobičajena je podjela na osnovu toga kome CA izdaje certifikate:

- CA koja izdaje certifikate drugim CA
- CA koja izdaje certifikate krajnjim korisnicima – Izdavačke CA

Moguće je da jedna certifikacijska ustanova izdaje certifikate i drugim certifikacijskim ustanovama i krajnjim korisnicima, ali je vrlo neuobičajeno i ne smatra se dobrom praksom.

Kako je u sklopu izbora modela povjerenja već razmatrano pitanje o potrebi za više od jedne CA ovdje će biti samo ponovljena odluka da se izabere model sa vrhovnom CA koja će izdavati samo certifikate drugim CA. Kao razlog za izbor ovog modela navedena je povećana sigurnost uz obećanje o detaljnijem objašnjenju koje se ovdje daje. Povjerenje unutar cijelog sigurnosnog domena zasnovano je na povjerenju u vrhovnu CA. Ako dođe do kompromitacije vrhovne CA ruši se osnova povjerenja i kompletan sistem sigurnog komuniciranja unutar domena više nije siguran. Sigurnost vrhovne CA može se povećati ako ona izda samo potrebne certifikate podređenim CA i drži se odvojena od računarske mreže. Odvojenost od drugih računara može se postići fizičkim gašenjem računara, gašenjem softverske aplikacije koja obavlja funkciju CA, ali najbolji metod je fizičko odvajanje od računarske mreže držeći računar upaljenim i aplikaciju CA aktivnom. Na ovaj način se smanjuje

izloženost vrhovne CA, ali se zadržava mogućnost evidentiranja svih događaja na računaru, putem sistemskih servisa evidentiranja događaja, na kom se softverska aplikacija CA izvršava. Uobičajen termin za ovakvu nepovezanu CA je *offline* CA. [46]. Ovako nešto ne bi bilo moguće ako bi vrhovna CA izdavala i certifikate krajnjim korisnicima jer bi onda morala biti stalno, ili dovoljno često, uvezana u sistem i spremna da opsluži zahtjeva za novim certifikatima. Nepovezanost vrhovne CA ni na koji način ne utiče na verifikaciju certifikata.

Pored ovih mjera neophodno je smjestiti računar sa vrhovnom CA na fizički sigurnu lokaciju sa ograničenim i kontrolisanim pristupom samo minimalnom neophodnom broju lica. Dodatna mjera sigurnosti koju je preporučljivo uvesti je mogućnost prijavljivanja na računar sa CA samo uz pomoć pametne kartice sa certifikatom. Poželjno bi bilo provesti i druge mjere zaštite za slučaj fizičke kompromitacije prostorije u kojoj se računar nalazi koje bi neovlaštenom licu otežale kompromitaciju vrhovne CA. Ovdje se misli na onemogućavanje pokretanja operativnog sistema sa vanjskih medija (floppy disk, CD/DVD, USB *flash* memorija, ...), te zaštitu BIOS-a putem lozinke, pa čak i fizičko onemogućavanje otvaranja kućišta računara. Sva ove mjere ne mogu zamijeniti fizičku sigurnost jer se smatra da je sposobnom *hacker*-u dovoljno pola sata fizičkog pristupa računaru za njegovu potpunu kompromitaciju. Neophodno je osigurati redovno sigurnosno pohranjivanje podataka, ali o tome će biti riječi pri utvrđivanju potrebnog hardvera za računar na kom će se izvršavati aplikacija CA.

Pošto je donesen odluka o postojanju jedne vrhovne CA koja izdaje certifikate samo podređenim CA potrebno je utvrditi potreban broj podređenih CA. Stvari koje treba razmotriti pri donošenju ove odluke su [dijelom 46]:

- Broj krajnjih korisnika – certifikata; - Veći broj korisnika može zahtijevati veći broj CA da bi se mogao izdavati i održavati potreban broj certifikata.
- Organizaciona podijeljenost organizacije – Ako je organizacija u kojoj se izdaju certifikati organizaciono podijeljena tako da su potrebe korisnika za certifikatima različite može biti potrebno imati CA za svaku od organizacionih jedinica koja će izdavati odgovarajuće certifikate.
- Geografska distribuiranost organizacije – Ako je organizacija u kojoj se izdaju certifikati geografski razuđena moze biti potrebno imati CA na svakoj od lokacija da bi smanjio mrežni promet između udaljenih lokacija i obezbijedilo dovoljno brzo izdavanje certifikata.
- Povećanje pouzdanosti – Redundantne CA mogu osigurati besprekidan rad infrastrukture javnih ključeva i u slučaju ispada neke od CA.
- Namjena certifikata – Potrebe za različitim tipovima certifikata mogu nametnuti potrebu za više CA od kojih će svaka izdavati određeni tip certifikata.

Podređene CA, kao je već rečeno, mogu biti:

- CA koja izdaje certifikate drugim CA, u kom slučaju one obavljaju funkciju posredničke CA između njima nadređenih i podređenih CA. Ovakve certfikacijske ustanove se često koriste za provođenje politike certificiranja i nazivaju *policy* CA
- CA koja izdaje certifikate krajnjim korisnicima – Izdavačke CA

Za manje organizacije sa nevelikim brojem korisnika i ograničenom namjenom certifikata čak i jedna CA može zadovoljiti potrebe. Jedna CA je lakša za administraciju i održavanje.

Za PKI koja se razmatra ovdje broj korisnika je relativno mali za mogućnosti savremenih implementacija CA. Takođe pojedinačne visokoškolske ustanove,

ovdje se misli na određeni fakultet, a ne na neki univerzitet u cijelini, uobičajeno nisu prostorno distribuirane i predstavljaju jednu organizacionu jedinicu. Po ovim elementima jedna CA bi mogla biti sasvim dovoljna. S obzirom na postojanje registracijskog procesa, nezavisnog od PKI, na visokoškolskim ustanovama nema potrebe za posebnom registracijskom ustanovom već samo za dodavanjem procedure registracija PKI korisnika kod CA prilikom uobičajene registracije korisnika (upis, izbor u zvanje, zapošljavanje). Ova procedura će biti detaljnije razmatrana kada se budu razmatrale sve administrativne procedure. Povećanje pouzdanosti je uvijek preporučljivo, ali planirana namjena PKI ne opravdava postizanje veće pouzdanosti uvođenjem redundantnih CA. Planirano je postojanje više grupa korisnika sa nešto različitim potrebama, ali su aplikacije koje će koristiti infrastrukturu identične te se sve ove potrebe mogu zadovoljiti sa samo jednom CA. Sve navedene odluke su zasnovane na usvojenom principu jednostavnosti izvedbe koja će omogućiti realnu izgradnju upotrebljive PKI na visokoškolskoj ustanovi. Ovim se ne isključuje mogućnost dodavanja CA u skladu sa novim potrebama ili materijalnim mogućnostima, jer usvojena struktura CA to omogućava.

3.2.4 Potrebni hardver

Kada je poznata namjena certifikata i njihov broj potrebno je utvrditi potrebne računarske resurse za izdavanje i upravljanje ovim certifikatima. Za ovo je pored broja certifikata potrebno utvrditi i njihove karakteristike od kojih je dužina ključa od najveće važnosti, jer najviše utiče na resurse potrebne za kriptografske operacije koje su dio rada sa certifikatima. Vrlo važan je i podataka o intenzitetu izdavanja certifikata, odnosno broju certifikata koji je neophodno izdati u određenom vremenskom periodu. Geografska raspoređenost organizacije i kvalitet veza u računarskoj mreži jako utiču na performanse, odnosno potrebne resurse. Planirani resursi pored tekućih potreba trebaju imati prostora za buduća proširenja.

Pošto je CA računarski program koji se izvršava na računarskom hardveru, uglavnom serverske konfiguracije, potrebno je razmotiriti uticaj pojedinih komponenata na performanse.

1. Procesor – Kriptografske operacije zahtjevaju mnogo računanja sa velikim brojevima. Ovdje dužina izabranog ključa ima presudnu ulogu. Ovo znači da je CA aplikacija koja intenzivno koristi procesorske resurse, te je procesor kritični resurs za CA. Poboljšanje procesora i/ili povećavanje njihovog broja ima direktan pozitivan efekat na efikasnost CA.
2. Diskovni podsistem – Potrebni kapacite najviše zavisi od broja certifikata, jer veličina certifikata ne zavisi od dužine ključa. Prostor potreban za pohranjivanje jednog certifikata je oko 30 KB [46]. Veća brzina diska omogućava brže izdavanje certifikata, ali potrebno je napomenuti da veće dužine ključeva traže dužu obradu u procesoru i rezultiraju u rjeđem pisanju na disk čime se smanjuje potrebna brzina rada diskovnog podsistema. Korištenje RAID tehnologije ima vrlo pozitivan uticaj na performanse.
3. Memorija – CA nije memorijski zahtjevna aplikacija takao da su količina i tip memorije koji su odgovarajući za instalirani operativni sistem sasvim dovoljni.

Pored hardverskih komponenata servera, važan faktor koji utiče na performanse CA je broj drugih aplikacija koje se izvršavaju na serveru. Zbog negativnog uticaja drugih aplikacija na performanse, a još više iz sigurnosnih razloga preporučuje se izvršavanje CA na sopstvenom serveru.

U konkretnom slučaju je na osnovu prethodno utvrđenog prostora na disku potrebnog za pohranjivanje certifikata, 30 KB, i procjene ukupnog broja certificiranih korisnika na visokoškolskoj ustanovi, 5.000, moguće utvrditi potrebni prostor na disku jednostavnim množenjem

$$5.000 * 30 \text{ KB} = 150\,000 \text{ KB} = 150 \text{ MB}$$

što je mnogo manje od kapaciteta bilo kog diska koji je danas moguće nabaviti. Znači da će bilo koji savremeni hard disk zadovoljiti potrebe za prostorom. Izdavanje i obnavljanje certifikata na visokoškolskoj ustanovi biće vezano za vrijeme upisa kad će svi studentski certifikati morati biti obrađeni. Ovo znači da je intenzitet izdavanja certifikata veliki u jednom kraćem vremenskom periodu. Međutim, za savremene CA aplikacije ovaj intenzitet ne predstavlja nikakav problem. Windows Server 2003 na serveru sa dualnim procesorom i 512 MB RAM-a može izdati 2 miliona certifikata sa standardnom dužinom (512) ključa dnvevno. Čak i sa neuobičajeno velikim CA ključem (> 2048) moguće je izdati više od 750.000 certifikata dnevno [46]. Planirani rad sa certifikatima će se odvijati unutar jedne visokoškolske institucije gdje bi 100 Mbitna računarska mreža bila sasvim dovoljno za očekivani mrežni saobraćaj uzrokovan radom certifikacijske ustanove.

Na osnovu navedenog može se zaključiti da bilo koja savremena serverska konfiguracija može zadovoljiti definisane potrebe za kapacitetom, performasnama i skalabilnošću. Radi funkcije koju bi ovaj server obavljao potrebno je staviti naglasak na pouzdanost. Sa jedne strane potrebno je obezbijediti pouzdanost komponenata nabavkom od pouzdanog proizvođača, a sa druge strane potrebno je koristiti tehnologiju sa povećanom pouzdanošću kao što je RAID, te komponente koje omogućavaju pravljenje sigurnosnih kopija podataka (*backup*). Prema raranije utvrđenom potrebnom broju CA može se zaključiti da nema potrebe za većim brojem hardverskih servera nego što je potreban broj softverskih CA aplikacija.

3.2.5 Rezime

U ovoj glavi utvrđena je potrebna configuracija CA koje će zadovoljiti prethodno definisane potrebe. Izabran je model povjerenja koji se sastoji od vrhovne CA, koja se drži odvojenom od računarske mreže (*offline* CA), i podređene izdavačke CA, koja izdaje certifikate krajnjim korisnicima i čiji certifikat je potpisala vrhovna CA. Utvrđeno je da će sve CA biti interne

odnosno uspostavljene i održavane od strane visokoškolske institucije u kojoj se uvodi PKI. Ustanovljeno je da jedna izdavačka CA može zadovoljiti potrebe korisnika kako su prethodno definisane. Funkciju registracijske ustanove će obavljati CA. Potrebni hardvare za svaku od CA, vrhovnu i izdavačku, je standardna savremena serverska konfiguracija koja uključuje RAID diskove i uređaje za sigurnosno pohranjivanje podataka.

3.3 Definisanje konfiguracije certifikata

Pošto je utvrđena potrebna organizacija certifikacijskih ustanova koje će izdavati certifikate neophodno je konfigurisati i same certifikate. Pojam digitalnog certifikata i formati certifikata koji se koriste su opisani u poglavlju sa teoretskim osnovama infrastrukture javnih ključeva. Ovdje će biti detaljno razmotren format certifikata koji bi odgovarao njihovoj planiranoj namjeni. Pored formata certifikata sigurnosne opcije certifikata će biti razmotrene. Biće predloženi kriptografski algoritimi, dužine ključeva i period valjanosti certifikata i odgovarajućih ključeva.

3.3.1 Format certifikata

Dva preovladavajuća formata digitalnih certifikata su X.509 i PGP. Format X.509 je definisan od strane ITU-T, kao i ISO i aktuelna je verzija 3 [31]. PGP certifikati, koji se često nazivaju i PGP ključevi, nisu standardizovani od strane zvaničnih standardizacijskih institucija ali ih koristi veoma rašireni softverski proizvod za sigurnu komunikaciju kompanije PGP tako da ih je neophodno spomenuti i razmotriti u diskusiji o formatima certifikata. PGP certfikati su detaljno opisani u korisničkoj literaturi PGP korporacije [32]. Oba formata certifikata u suštini povezuju javni ključ sa vlasnikom certifikata potvrđujući to digitalnim potpisom. Osnovna razlika je u tome što X.509 certifikati izvorno imaju jedan digitalni potpis, dok PGP certifikati mogu, i najčešće imaju više potpisa koji potvrđuju vezanost javnog kluča sa vlasnikom. Ova razlika je zapravo posljedica modela povjerenja koji PGP koristi. Ovaj model se u PKI terminologiji naziva mreža povjerenja (*Web of Trust*) i detaljnije je opisan u dijelu rada koji se bavio izborom modela povjerenja za budući PKI. U tom dijelu rada izabran je modificirani hijerarhijski model povjerenja koji PGP certifikati ne podržavaju tako da ne mogu biti izabrani za izgradnju planirane PKI i neće dalje biti razmatrani. Ovdje treba napomenuti da PGP program, iako izvorno radi sa PGP certifikatima, ima mogućnost rada i sa X.509

certifikatima, te je, zbog dobrih osobina ovog programa, potrebno razmotriti i mogućnost njegovog korištenja.

Izabrani X.509 certifikati postoje u tri verzije, v1, v2 i v3. Sve verzije su standardizovane i kompatibilne unazad, odnosno novije verzije, sa većim brojem, imaju sva polja kao i ranije verzije, te još neka dodatna. ITU-T X.509 ili ISO/IEC 9594-8 definiše standardni format certifikata i kao dio X.500 preporuka za Direktorije objavljen je 1988. Ovo se naziva verzijom 1. U verziji 2 su 1993 dodata još dva polja. Kroz praktična iskustva u upotrebi certifikata pojavila se potreba za dodatnim poljima. Na osnovu ove potrebe ISO/IEC, ITU-T and ANSI X9 su 1996 definisali novi format v3. Ovaj format omogućava dodavanje novih polja, ali ne zahtijeva njihovo postojanje. Pomenute organizacije su utvrdile skup standardnih ekstenzija za dodatna polja, ali nisu striktno definisale način njihove upotrebe odnosno tumačenja značenja [30]. Da bi se olakšala upotreba certifikata za Internet aplikacije IETF radna grupa za mreže, podgrupa za PKIX, je 2002. godine objavila RFC3280, koji specificira format X.509 certifikata i lista opozvanih certifikata za Internet X.509 PKI. Ovaj dokument potvrđuje namjenu osnovnih polja certifikata verzije 2, te utvrđuje namjenu ekstenzija za dodatna polja iz verzije 3. Striktno poštovanje prijedloga iz ovog dokumenta bi trebalo omogućiti interoperabilnost različitih aplikacija koje izdaju i provjeravaju digitalne certifikate. Treba imati u vidu da je ovo oblast koja je još u razvoju te se tumačenja nekih dokumenata razlikuju od proizvođača do proizvođača.

Posebnu kategoriju certifikata predstavljaju kvalifikovani elektronski certifikati. Ovo je termin koji se koristi u Direktivi Evropskog parlamenta i savjeta o pravnim okvirima za elektronski potpis [55]. Ovaj dokument je uputa članicama Evropske unije za kreiranje pravnih okvira koji podržavaju elektronski potpis. Definicija kvalifikovanog elektronskog certifikata u BiH pravnom dokumentu koji reguliše ovu problematiku [9] je identična onoj iz EU Direktive. IETF PKIX radna grupa je posvetila RFC3739 [56] definisanju

profila kvalifikovanih certifikata. Važnost kvalifikovanog certifikata je u tome što je jedan od uslova za pravnu jednakost digitalnog potpisa sa svojeručnim da je digitalni potpis napravljen koristeći kvalifikovani certifikat. Jedan od ciljeva ovog projekta implementacije PKI je i da navede i pokaže kako je moguće ispuniti sve uslove potrebne za kvalifikovano certifikaciono tijelo ovlašteno da izdaje kvalifikovane certifikate. Potrebno je napomenuti da se u EU Direktivi i BIH Odluci o elektronskom potpisu nigdje ne spominju tehnički detalji implemenatacije, kao što je format certifikata X.509, već samo uslovi koje certifikat mora ispunjavati. Pošto se definicija kvalifikovanog certifikata dobrim dijelom poklapa sa izabranim formatom X.509v3, ovdje će posebno biti istaknute samo razlike kada se bude govorilo o konkretnim poljima certifikata. One se u suštini svode na to da u kvalifikovanom certifikatu mora biti naznačeno da je to kvalifikovani certifikat te da je potrebno jasno naznačiti namjenu za koju je certifikat izdan.

Nezavisno od aplikacije koja će biti korištena kao CA potrebno je utvrditi princip koga će se držati prilikom kreiranja certifikata. Drugim riječima potrebno je dati lokalno značenje svakom od polja u certifikatu. Neke od odluka su pitanje usvojene politike imenovanja subjekata, dok su neke vrlo tehničke prirode. Princip dodjeljivanja vrijednosti poljima koja nemaju tehničko značenje biće samo naveden. X.509 v3 certifikat je u suštini digitalno potpisan skup podataka, tako da sam certifikat ima polja sa podacima, polje sa vrijednošću digitalnog potpisa CA nad poljima sa podacima, te polje koje informiše o tome koji je od mogućih algoritama korišten za digitalno potpisivanje. Mogući algoritmi za digitalno potpisivanje i druge kriptografske operacije sa X.509 certifikatima su definisani u RFC3279[57]. Izbor algoritma i njegovih parametara će biti kasnije detaljnije razmatran u ovom poglavlju. Polja sa podacima se sastoje od osnovnih polja i ekstenzija.

Osnovovna polja sa predloženim sadržajem su:

1. Verzija – Moguće vrijednosti su v1, v2, v3. Predložena vrijednost je v3.
2. Serijski broj – Pozitivan cijeli broj jedinstven unutar CA. Aplikacija koja implementira CA brine se o zadovoljavanju potrebnih uslova.
3. Potpis – Identifikacija algoritma koji je korišten pri potpisivanju certifikata od strane CA. Vrijednost ovog polja mora biti identična vrijednosti ranije pomenutog polja koje ide uz vrijednost digitalnog potpisa. CA aplikacije automatski generišu identičnu vrijednost u ova dva polja, a izbor algoritma će, kako je već rečeno, bit kasnije detaljnije obrađen.
4. Izdavač – Ovo polje, kao i polje "Subjekat" imaju posebne zahtjeve za kvalifikovane certifikate u odnosu standardne definisane u RFC3280. Ti zahtjevi su da se identificira organizacija odgovorna za izdavanje certifikata. Ime organizacije koje se ovdje upiše mora biti zvanično registrovano ime organizacije. U sklopu ovog imena se minimalno mora nalaziti i ime države izdavanja. Dozvoljeni su i drugi elementi koji pobliže definišu organizaciju ali oni moraju biti definisani u Politici certificiranja ili Izjavi o praksi certificiranja. Predložena vrijednost ovog polja je zvanični registrovani naziv visokoškolske ustanove, te BA kao kod države Bosne i Hercegovine.
5. Subjekat – Ovo polje identificira entitet asociran sa javnim ključem koji se nalazi u polju "javni ključ subjekta". Za kvalifikovani certifikat ovo polje mora imati vrijednost prepoznatljivog (*distinguished*) imena subjekta. U sklopu imena se mora nalaziti odgovarajući podskup atributa koji jedinstveno određuju subjekat. Prvi od atributa mora biti ime i/ili prezime ili pesudonim subjekta. Pošto se jedinstvenost subjekta garantuje unutar domena u kom je izdat certifikat uobičajeno je uključiti podatke o organizaciji na način na koji su one predstavljene u polju sa podacima o izdavaču certifikata. Moguće je uključiti i titulu, što može biti korisno na visokoškolskoj instituciji. Ako je potrebno upisuje se i serijski broj koji omogućava razlikovanje dva subjekta ako

su sva ostala polja subjekta iste vrijednosti. Predloženi atributi za ovo polje su ime i prezime onoga kome je izdat certifikat, titula i serijski broj, kao i podaci o visokoškolskoj ustanovi koji su dati i u polju izdavač.

6. Validnost – U ovom polju se definiše period validnosti certifikata. Ovaj period je definisan sa dva datuma: datum početka važenja certifikata i datum prestanka važenja certifikata. Predložena vrijednost datuma početka važenja certifikata je datum izdavanja certifikata, a datum prestanka važenja certifikata će biti izračunat na osnovu definisanog vremena valjanosti certifikata. Utvrđivanje trajanja valjanosti certifikata će biti detaljnije razmatrano kasnije u ovom poglavlju. Važno je da se ovo trajanje može globalno definisati na nivou CA aplikacije i tipa certifikata, a aplikacija će se pobrinuti za unošenje gore predloženih vrijednosti u certifikate koje izdaje.
7. Informacija o javnom ključu subjekta – Ovo polje sadržava javni ključ subjekta i podatke o korištenom kriptografskom algoritmu. Izbor algoritma će, kako je već rečeno, biti razmatran kasnije u ovom poglavlju. Aplikacije koje implementiraju CA brinu se za pravilno popunjavanje ovog polja.
8. Jedinstveni ID izdavača – Ovo polje je opcionalno i RFC3280 preporučuje njegovo ne korištenje.
9. Jedinstveni ID subjekta – Ovo polje je opcionalno i RFC3280 preporučuje njegovo ne korištenje.

Ekstenzije se pojavljuju počevši od verzije 3, a pošto je to predložena verzija potrebno je utvrditi neophodna polja i njihove vrijednosti. Pošto tumačenje ovih polja u praksi nije uvijek jedinstveno, potrebno je koristiti samo neophodna polja sa jasno definisanom namjenom. Kako je planirano izdavanje kvalifikovanih certifikata moraju se koristiti bar ekstenzije neophodne da bi certifikat učinile kvalifikovanim. Neophodne ekstenzije će biti definisane i njihova vrijednost predložena na osnovu EU Direktive [55] i

BIH Odluke [9] o elektronskom potpisu, a u skladu sa RFC3739 [56] o formatu kvalifikovanih certifikata.

Potrebne ekstenzije sa predloženim vrijednostima su:

1. Izjava o kvalifikovanom certifikatu – Ovo polje je neophodno da bi certifikat bio kvalifikovan [55] [9]. Sadržaj ovog polja je zapravo izjava izdavača da je certifikat izdat kao kvalifikovani certifikat u skladu sa važećim zakonom u odgovarajućem pravnom sistemu. Ovakva izjava i više detalja se obično daju u Politici certificiranja i Izjavi o praksi certificiranja na koje se u sklopu certifikata upućuje posebnom ekstenzijom koja će biti navedena kasnije. Predložena vrijednost za ovo polje je izjava visokoškolske ustanove da je certifikat izdat kao kvalifikovani certifikat u pravnom sistemu Bosne i Hercegovine.
2. Namjena ključa – Ovo polje je potrebno imati za kvalifikovane PKIX certifikate [56] i preporučeno je njegovo postojanje u EU kvalifikovanim certifikatima [55] [9]. Sadržaj polja definiše kriptografsku namjenu ključa koji je dat u certifikatu. PKIX definiše devet mogućih namjena, odnosno vrijednosti ovog atributa, koje se mogu kombinovati. Ove namjene su: digitalno potpisivanje, neporicanje, šifriranje ključa, šifriranje podataka, razmjena ključeva, verifikacija certifikata, potpisivanje CRL, samo šifriranje i samo dešifriranje. Stvarno moguće vrijednosti su ograničene izabranim kriptografskim algoritmom. Kako je namjena kvalifikovanih certifikata da omoguće digitalne potpise koji imaju osobine i vrijednost svojeručnih potpisa, odgovarajuće namjene bi bile: digitalno potpisivanje i neporicanje. Tumačenje značenja odabranih atributa namjene mora biti dato u Politici certificiranja i/ili Izjavi o praksi certificiranja u skladu sa važećim pravnim propisima. Prilikom izbora kriptografskog algoritma potrebno je voditi računa da se izabere onaj koji omogućava planiranu namjenu certifikata.

3. Identifikator politike certificiranja – Ovo polje je alternativni način potvrđivanja da je certifikat izdat kao kvalifikovani certifikat. Njegova vrijednost pokazuje na lokaciju gdje se može naći Iskaz o praksi certificiranja. Predložena vrijednost je URL adresa ovog iskaza.
4. Atributi subjekta iz imenika – Ovo polje sadrži dodatne atribute subjekta koji dopunjuju informacije iz osnovnog polja subjekat. Atributi koji se pohranjuju u ovo polje su oni koji nisu dio prepoznatljivog imena subjekta, ali se mogu biti od koristi za različite namjene, ako što je autorizacija [56]. Skup standardno prepoznatih atributa čine:
   - Datum rođenja
   - Mjesto rođenja
   - Pol
   - Zemlja državljanstva
   - Zemlja boravka

   Predloženi sadržaj ovog polja su odgovarajuće vrijednosti ovih atributa.
5. Identifikator ključa ustanove – Ovo polje omogućava identificiranje javnog ključa koji odgovara privatnom ključu kojim je certifikat potpisan. Namjena ovog polja je da omogući utvrđivanje putanje certificiranja [30]. RFC3280 preporučuje korištenje ove ekstenzije. U skladu sa ovom preporukom predloženo je i korištenje ovog polja.

Namjena ovog razmatranja formata certifikata je bila da se jasno utvrdi potrebni format, X.509v3, sa svim potrebnim poljima i njihovim predloženim vrijednostima. Konkretan način zadavanja ovog formata i željenih vrijednosti zavisiće od izabrane softverske aplikacije za certifikacijsku ustanovu. Većina aplikacija ima mogućnost predefinisanja formata certifikata i sadržaja polja za sve tipove certifikata koje CA aplikacija izdaje. U svakom slučaju, utvrđivanje potrebnih polja i njihovih vrijednosti zahtjeva jasno utvrđivanje potreba i njima odgovarajuće namjene certifikata.

3.3.2 Sigurnosne opcije certifikata

U sklopu definisanja certifikata potrebno je izabrati i neke sigurnosne parametre certifikata. Ovi parametri, kako je već napomenuto, tiču se izbora algoritma za kriptografske operacije sa certifikatima i dužine ključa. Uz ove parametre potrebno je utvrditi i vremensko trajanje važenja certifikata i njihovih ključeva. Vezano za ova vremena neophodno je utvrditi i strategiju obnavljanja certifikata. Sve ove odluke direktno utiču na sigurnost certifikata i cijele infrastrukture javnih ključeva. Ono što komplikuje izbor je suprotnost zahtjeva. Promjene vrijednosti parametara u pravcu povećanja sigurnosti utiču i na povećavanje kompleksnosti i sporosti infrastrukture. Potrebno je naći ravnotežu između dovoljno sigurnosti i prihvatljive kompleksnosti. Nema jedinstvenog odgovora šta je dovoljna sigurnost već se za svaku situaciju traži odgovor. Opšti princip zaštite, ne samo računarske, je da vrijednost resursa potrebnih protivniku za uklanjanje zaštite treba biti bar približna vrijednosti resursa koji se štite. Ako je za nedozvoljeno otvaranje nekog sefa potrebno uložiti 1000 KM, a provalnik pretpostavlja da se u sefu nalazi 1000 KM, nije za očekivati da će se provalnik odlučiti za nasilno otvaranje sefa. Sa druge strane, vrijednost resursa za uspostavljanje zaštite mora biti dovoljno manja od vrijednosti resursa koji se štite. Ako se za čuvanje 1000 KM kupi sef koji košta 1000 KM onda je na zaštitu potrošena ista vrijednost sredstava kao i vrijednost koja se štiti što se ne čini opravdanim. Iz ovoga se nameće i jedan logički zaključak da vrijednost resursa za uspostavljanje zaštite mora biti dovoljno manja od vrijednosti resursa potrebnih za njeno neovlašteno uklanjanje. Kriptografska zaštita koja se koristi u PKI u svakom slučaju zadovoljava ovaj posljednji uslov. U traženju ove ravnoteže između sigurnosti i kompleksnosti usvaja se princip da je neophodno ostvariti potrebnu sigurnost makar i na račun kompleksnosti. Gradi se sistem za sigurnosno komuniciranje koji mora prije svega biti siguran, a ono što je potrebno odlučiti je koliko je sigurnosti potrebno.

Certifikacijska ustanova izdaje certifikate koji su svi istog formata, ali nisu svi iste namjene. Prema namjeni certifikata potrebno je utvrditi njegove sigurnosne opcije. Prva podjela je na certifikate za:

- Certifikacijske ustanove
- Krajnje korisnike

Certifikati za CA očigledno trebaju imati veću sigurnost od certifikata krajnjih korisnika jer je i njihova vrijednost veća. Kompromitacijom certifikata CA kompromitovani su i svi certifikati izdani od te CA. Prema prethodno utvrđenom potrebnom broju CA i modelu povjerenja, planirana infrastruktura predviđa dva nivoa CA:

- Vrhovna CA – Izdaje certifikate samo drugim CA unutar sistema
- Izdavačka CA – Certificirana od strane vrhovne CA i izdaje certifikate krajnjim korisnicima.

Između ove dvije CA jasno je da su zahtjevi za sigurnost certifikata vrhovne certifikacijske ustanove veći.

Certifikati za krajnje korisnike se sa sigurnosnog aspekta mogu podijeliti u dvije, u ranijem poglavlju utvrđene, grupe:

- Certifikati za računare
- Certifikati za ljude

Broj certifikata za računare će biti manji od broja certifikata za ljude, jer će računarski certifikati biti izdavani samo računarskim serverima, dok će sva ljudska bića korisnici sistema dobiti kvalifikovane certifikate.

Certifikati za ljude će se opet međusobno razlikovati za različite ranije definisane grupe korisnika:

- Računarski i PKI administratori
- Rukovodstvo fakulteta
- Nastavno osoblje
- Službe

- Studenti

Za sve pobrojane tipove certifikata će sada biti predložene i obrazložene sigurnosne opcije.

3.3.2.1 Kriptografski algoritmi

Može zvučati čudno ako se kaže da izbor kriptografskog algoritma i nije toliko bitan za sveukupnu sigurnost sistema, ali to je zaista tako. Savremeni kriptografski algoritmi, standardizovani i vremenom provjereni, su toliko sigurni da su vrlo vjerovatno najsigurniji dio svake PKI. Većina savremenih računarskih sigurnosnih sistema pada na implementacijama i ljudskom faktoru, a nikad na samim kriptografskim algoritmima. [20]. Da bi sve ovo stajalo potrebno je izabrati pouzdan algoritam. Takođe je potrebno izabrati algoritam koji je standardno podržan radi buduće komunikacije i razmjene certifikata sa subjektima van organizacije. Oba ova uslova se zadovoljavaju izborom algoritama predloženih u RFC3279, IETF PKIX dokumentu koji se definiše algoritme i njihove identifikatore za X.509 PKI [57]. RFC3279 specifikacija definiše sadržaj polja signatureAlgorithm, signatureValue, signature, and subjectPublicKeyInfo u Internet X.509 certifikatima i listama opozvanih certifikata (CRL). Specificirani su argumenti za jednosmjerne *hash* funkcije, digitalno potpisivanje i javni ključ.

Od tri navedena algoritma za jednosmjerne *hash* funkcije: MD2, MD5 i SHA-1; SHA-1 je preferirani algoritam za Interenet X.509 PKI. Pošto je SHA-1 sugerisan kao najbolji izbor razumno je koristiti ga i radi buduće interoperabilnosti sa drugim PKI.

Algoritimi definisani za digitalno potpisivanje su RSA, DSA (D*igital Signature Algorithm*) i ECDSA (*Elliptic Curve Digital Signature Algorithm*). Nijedan od algoritama nije posebno istaknut. Prilikom definisanja formata certifikata utvrđene su namjene certifikata i rečeno je da je potrebno da izabrani kriptografski algoritam podržava planirane namjene. U ovom slučaju

konzervativno opredijeljenje za najstariji i još uvijek najrašireniji od algoritama, RSA, pruža najveću vjerovatnoću podržanosti od aplikacije koja će biti izabrana za implementaciju certifikacijske ustanove. RSA je također dobar izbor i za kompatibilnost sa drugim CA jer sve vrhovne CA koje su ugrađene u savremene W*eb browser*-e koriste RSA algoritam. RSA podržava planirane namjene certifikata: digitalno potpisivanje i neporicanje. Ovaj algoritam za digitalne potpise mora biti kombinovan sa nekim od algoritama za jednosmjerno hashiranje. Pošto je za tu namjenu izabran SHA-1, onda će izabrani algoritam za digitalno potpisivanje biti RSA sa SHA-1.

Broj algoritama predloženih za javne ključeve je najveći. Predloženi algoritmi su: RSA, DSA, Diffie-Hellman razmjena ključeva, KEA (*key exchange algorithm*) i eliptičke krive sa DSA i sa Diffie-Hellman. Pošto je RSA izabran za digitalno potpisivanje sasvim je logično i da se za javne ključeve izabere RSA.

3.3.2.2 Dužine ključeva

Nakon što su izabrani kriptografski algoritmi potrebno je utvrditi potrebne dužine javnih ključeva za sve tipove certifikata koji će se izdavati. Izabrana dužina ključa direktno utiče na sigurnost koja se postiže primjenom algoritma. Izbor odgovarajućih dužina ključeva je od kritičnog značaja za implementaciju odgovarajuće sigurnosti. Veća dužina ključa znači i veću sigurnost, ali i duže vrijeme potrebno za kriptografske operacije. Sigurnost izabranog RSA algoritma leži u, pretpostavljenoj, težini rastavljanja velikog broja na proste faktore. Napretkom u algoritmima i tehnologiji smanjuje se vrijeme potrebno za ove operacije, odnosno sve veći brojevi se mogu rastaviti na proste faktore u sve kraćem vremenu. Trenutno najveći broj rastavljen na proste faktore je 576 bitni broj (174 decimalne cifre) [58]. Ovo je u decembru 2003 postigla grupa naučnika sa nekoliko njemačkih univerziteta [59]. Korišteni algoritam bio je *general number field sieve*.

Računarsko vrijeme, mjereno u MIPS (milion instrukcija u sekundi) godinama potrebno za rastavljanje brojeva različite dužine na proste faktore, po ovom algortimu, prema posljednjoj dostupnoj procjeni [20], dato je u tabeli 2:

Broj bita	**Potreban broj MIPS godina za rastavljanje**
512	30.000
768	$2*10^{8}$
1024	$3*10^{11}$
1280	$1*10^{14}$
1536	$3*10^{16}$
2048	$3*10^{20}$

Tabela 2

Savremeni Pentium 4 procesori obavljaju oko 2000 miliona instrukcija u sekundi [60][61]. Ovo otprilike znači da bi 15 računara sa ovakvim procesorima radeći neprekidno godinu dana uspjeli rastaviti broj dužine 512 bita na proste faktore. Ili bi isti broj mogao biti rastavljen u roku od 6 dana sa oko 1000 ovakvih računara. Na ovaj način bi se iz javnog RSA ključa moglo doći do privatnog ključa i u potpunosti eliminisati sve elemente sigurnosti sistema. Prema tome se može reći da već danas 512 bitni ključ nije dovoljno siguran. Ključevi od 768 i 1024 bita izgledaju prilično bezbjedni u sadašnjem trenutku.

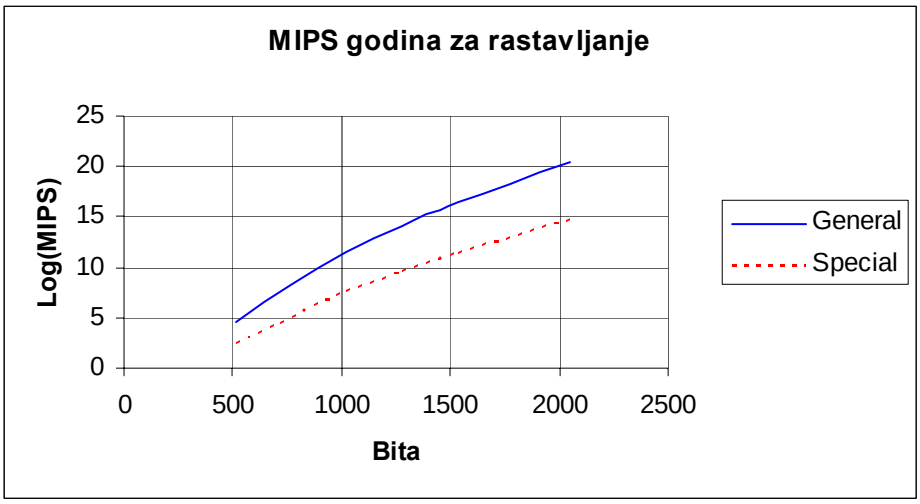
Međutim PKI, odnosno izabrane veličine ključeva, treba da nude sigurnost i na duži vremenski rok. Vrlo je nezahvalno praviti dugoročne prognoze u ovoj oblasti jer su se tu opekla i velika imena poput Ronald Rivesta, jednog od autora RSA algoritma. On je naime 1977 godine pretpostavio da će za rastavljanje 125 cifrenog broja na proste faktore biti potrebno $40*10^{15}$ godina [62]. Ipak je neophodno donijeti odluku o dužini ključeva zasnovanu na nekim prognozama. Kada se prognozira napredak računara uglavnom se citira takozvani Moore zakon. Ovo zapravo nije nikakav zakon već predviđanje jednog od direktora Intela koje je on iznio još 1965 godine i koje se do sada pokazalo ispravnim. Ono otprilike kaže da će broj tranzistora po integralnom

kolu rasti eksponencijalno sa vremenom, odnosno da će se moć računara udvostručavati otprilike svakih 18 mjeseci [63]. Znači da će računari za desetak godina biti oko 100 puta moćniji, odnosno 10000 puta moćniji za dvadesetak godina. Pretpostavka je da će doći i do napretka u metodama rastavljanja na proste faktore. Jedna od mogućnosti je da će algoritam *special number field sieve*, sada primjenjiv samo na specijalne brojeve biti opšteprimjenjiv. Ovaj algoritam je mnogo brži što pokazuje i tabela 3 [20]:

Broj bita	**Potreban broj MIPS godina za rastavljanje**
512	<200
768	100,000
1024	$3*10^7$
1280	$3*10^9$
1536	$2*10^{11}$
2048	$4*10^{14}$

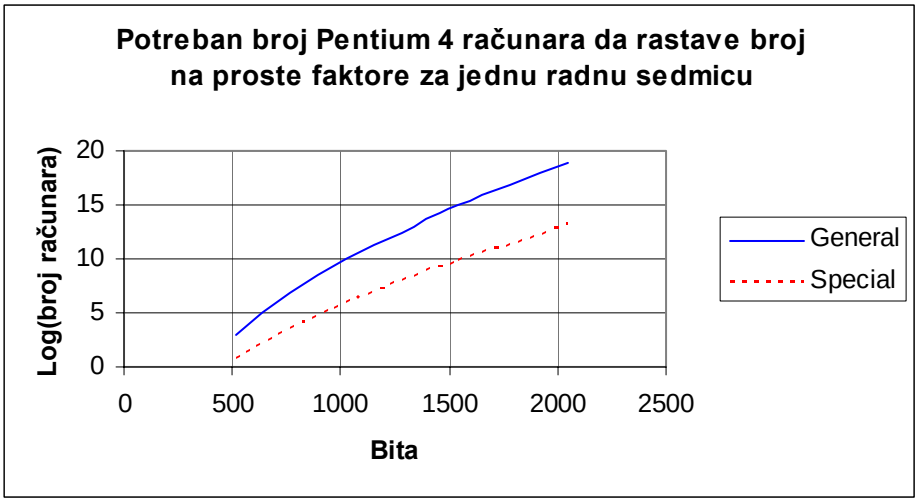
Tabela 3

Graf na slici 6 prikazuje, u logaritamskoj razmjeri, potreban broj MIPS godina za rastavljanje broja na proste faktore u zavisnosti od dužine broja u bitima za *General* i *Special Number Field Sieve* algoritme.



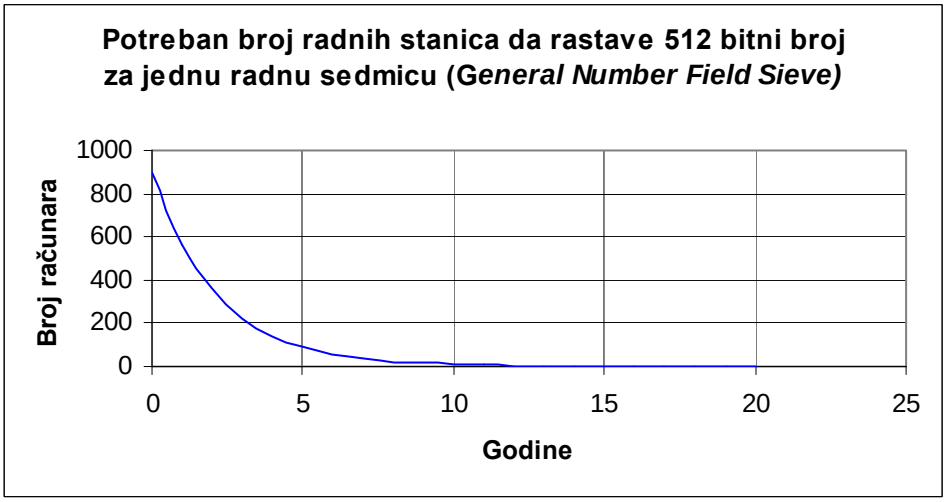
Slika 6

Graf na slici 7 prikazuje, u logaritamskoj razmjeri, potreban broj Pentium 4 računara za rastavljanje broja na proste faktore za jednu radnu sedmicu (6 dana) u zavisnosti od dužine broja u bitima za *General* i *Special Number Field Sieve* algoritme.



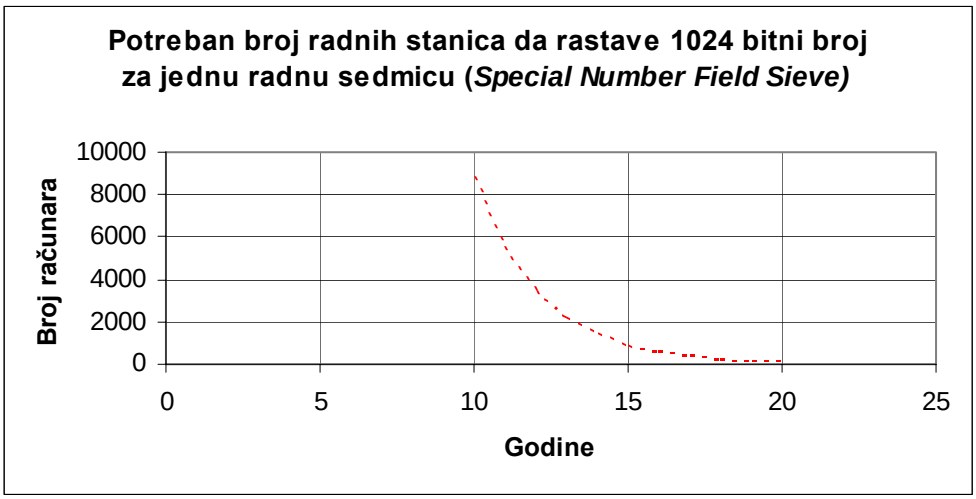
Slika 7

Graf na slici 8 prikazuje očekivanu promjenu potrebnog broja računara za rastavljanje 512 bitnog broja na proste faktore za jednu radnu sedmicu (6 dana) koristeći *General Number Field Sievealgoritam* u naredih 20 godina.



Slika 8

Graf na slici 9 prikazuje očekivanu promjenu potrebnog broja računara za rastavljanje 1024 bitnog broja na proste faktore za jednu radnu sedmicu (6 dana) koristeći *Special Number Field Sievealgoritam* u naredih 20 godina.



Slika 9

Iz ovoga slijedi da bi 1024 bitni ključ mogao za 15-ak godina biti jednako (ne)siguran kao što je danas 512 bitni. Također slijedi da će 2048 bitni i veći ključevi, ako ne bude znatnih odstupanja od navedenih razmatranja, i dalje biti vrlo sigurni za deset, a možda i više godina.

Do sada se samo govorilo o mogućnosti rekonstrukcije privatnog ključa iz javnog, ali se nisu uzimali u obzir troškovi takvog proračuna. Ovo je vrlo važan elemenat sigurnosti, jer kako je ranije rečeno vrijednost resursa potrebnih protivniku za uklanjanje zaštite treba biti bar približna vrijednosti resursa koji se štite. Odnosno, ako je vrijednost podataka koji su zaštićeni ključem manja od troškova rekonstrukcije ključa, ključ se može smatrati praktično sigurnim. Jedna od posljedica "Moore-ovog zakona" je da su se istorijski svakih pet godina troškovi za isti broj MIPS smanjivali deset puta. Znači da bi za deset godina svi proračuni trebali biti 100 puta jeftiniji. Opet se dolazi do istog zaključka da bi praktična sigurnost 1024 bitnog ključa za 15-ak godina mogla biti jednaka današnjoj praktičnoj sigurnosti 512 bitnog ključa.

Prema tome podaci zaštićeni 1024 bitnim ključem bi u narednih 15 godina trebali vrijediti manje od troškova organizovanja i rada 1000 savremenih računara jednu radnu sedmicu. Većina korisničkih podataka sa vremenom brzo gubi na vrijednosti tako da se izbor 1024 bitnog ključa za certifikate krajnjih korisnika čini kao siguran izbor. Takođe je i uobičajeno vrijeme trajanja valjanosti certifikata i ključa krajnjih korisnika kraće od 10 godina. O ovome će se voditi računa i detaljnije će biti razmotreno u narednom poglavlju.

Prije konačne odluke o potrebnoj dužini ključeva potrebno je razmotriti i negativnu stranu dužih ključeva. Kriptografske operacije kod asimetrične kriptografije su računski intenzivne. Najduža od ovih operacija je generisanje novog para ključeva koje se odvija prilikom kreiranja certifikata i dodjeljivanja javnog ključa subjektu. Kreiranje para ključeva kod izabranog RSA algoritma uključuje pronalaženje pogodnog para prostih brojeva, te izračunavanje javnog i privatnog ključa na osnovu ovih brojeva, kako je u teoretskim osnovama objašnjeno. Ovo nisu trivijalne operacije i njihovo trajanje eksponencijalno raste sa rastom dužine ključa. Vremena potrebna za generisanje parova ključeva različitih dužina na savremenom 2,8 GHz pentium 4 procesoru su data u tabeli 4 [64]:

Dužina ključa (bita)	**Vrijeme (sekundi)**
512	0.040
768	0.094
1024	0.176
1536	0.415
2048	1.348

Tabela 4

O ovim veličinama treba povesti računa prilikom izbora dužine ključa za sve tipove certifikata.

Očigledno da je najvrijedniji certifikat i javni ključ vrhovne CA jer se njegovom kompromitacijom kompromituju i svi njemu podređeni certifikati.

Prema planiranom modelu povjerenja i broju CA vrhovna CA će izdavati samo certifikate izdavačkim CA i samoj sebi. Inicijalno je planirana samo jedna izdavačka CA tako da će vrhovna CA izdati samo dva certifikata. Ovo znači da nema prepreka da se izabere vrlo dugačak ključ. Međutim nema potrebe da se pretjeruje tako da je preložena vrijednost 4096 bita.

Izdavačka CA će izdavati sve certifikate što znači da će njen ključ biti najkorišteniji u sistemu, te treba povesti računa da bude upravo dovoljne dužine. Većina certifikata koji će se izdavati biće izdavani studentima u vrijeme upisa, što znači da se može očekivati veliki intenzitet izdavanja certifikata. Međutim kako je u poglavlju u kom je razmatran hardver potreban za rad certifikacijske utvrđeno da na savremenoj serverskoj platformi kakva je planirana broj dnevno izdanih certifikata i sa neuobičajeno velikim CA ključem (> 2048) može biti više stotina hiljada, a ukupan broj planiranih certifikata ne prelazi nekoliko hiljada, nema nikakvih problema da se za korisničku certifikacijsku ustanovu izabere vrlo sigurna dužina ključa od 2048 bita.

Korisnički certifikati takođe imaju različite sigurnosne zahtjeve. Certifikati rukovodstva fakulteta će se koristiti za potpisivanje dokumenata koji treba da važe duži vremenski period i čija je vrijednost veća od dokumenata koje će potpisivati drugi korisnici. Vrijednost certifikata računarskih i PKI administratorima je u pravima koja im certifikati omogućavaju te je potrebno da i ovi certifikati imaju vrlo sigurne ključeve. Na drugoj strani su studentski certifikati koji imaju najmanju vrijednost i po tipu dokumenata koje će potpisivati i po pravima pristupa koja će imati. Ipak, ranije usvojena minimalna dužina ključa od 1024 bita bi, za sada, trebala zadovoljiti sigurnost svih certifikata krajnjih korisnika. Dodatna sigurnost za certifikate rukovodstva i računarske i PKI administracije se može postići korištenjem pametnih kartica za pohranjivanje certifikata.

Prema gore navedenom predložene dužine ključeva po tipovima certifikata su slijedeće:

- Vrhovna (root) CA – 4096
- Izdavačka (issuing) CA – 2048
- Certifikati za računare - 1024
- Računarski i PKI administratori - 1024
- Rukovodstvo fakulteta - 1024
- Nastavno osoblje - 1024
- Službe - 1024
- Studenti – 1024

3.3.2.3 Period valjanosti certifikata i pripadajućih ključeva

Kako je u prethodnom poglavlju već raspravljano, sigurnost certifikata, odnosno privatnog ključa, ne zavisi samo od dužine ključa već i vremenskog perioda u kom se koristi. Jedan od razloga je prethodno spomenuti napredak u algoritmima za rastavljanje na proste faktore i napredak računarske tehnologije. Drugi, do sada ne spomenuti razlog, je izloženost ključa napadima. Što je duže ključ valjan, duži je i period u kom je javni ključ javno dostupan i može biti testiran na slabosti. Iz ovih razloga odluka o dužini vremena valjanosti certifikata i pripadajućih ključeva zavisi od dužine ključa i namjene certifikata. Certifikati koji se više koriste su više izloženi opasnosti. Kraći životni vijek certifikata povećava njihovu sigurnost, ali povećava i administrativne zadatke oko njihovog obnavljanja ili ponovnog izdavanja. U sklopu hijerarhijske infrastrukture javnih ključeva potrebno je također voditi računa o međusobnoj zavisnosti certifikata. Kada certifikat CA, koja je izdala druge certifikate istekne, automatski ističu i svi njeni certifikati. Znači da certifikati viši u hijerehiji povjerenja moraju imati duži vijek trajanja, a da se ovaj vijek smanjuje kako se spušta niz hijerahiju do krajnjih korisnika. Certifikati krajnjih korisnika označavaju povezanost krajnjeg korisnika sa institucijom koja je izdala certifikat. Vrijeme valjanosti certifikata krajnjih

korisnika, odnosno period na koje se izdaju treba da odražava najkraći planirani period pripadanja krajnjeg korisnika instituciji.

Visokoška ustanova, za kakvu se planira PKI, ima vrlo jasno definisane cikluse u kojima se odvija većina procesa. Najveći broj budućih krajnjih korisnika certifikata su studenti koji se godišnje upisuju ili obnavljaju upis u visokoškolsku ustanovu. Nastavni ansambl se planira za svaku školsku godinu. Iz ovoga slijedi logičan zaključak da bi se certifikati za studente i nastavno osoblje trebali obnavljati godišnje. Certifikati bi se mogli obnavljati do pet puta sa istim ključem. Pet godina je relativno siguran period za planiranu dužinu ključa, a uobičajena vezanost studenata za visokoškolsku ustanovu je oko pet godina. U istom periodu je uobičajeno i da članovi nastavnog ansambla promijene svoj status, odnosno napreduju u zvanju. Količina dokumenata koji su mogli biti potpisani certifikatom može biti jako velika, ali njihova vrijednost brzo opada sa vremenom. Prijave ispita i ispitni rezultati uglavnom su vrlo male vrijednosti ili bezvrijedni u roku od godinu dana. Rukovodstvo, službe i računarska administracija uglavnom nisu na ovom godišnjem planu promjena, ali je njihov broj dovoljno mali da godišnje obnavljanje njihovih certifikata ne bi trebalo predstavljati problem.

Certifikat izdavačke CA mora imati period važenja duži od jedne godine da bi se osiguralo da certifikati koje izdaje važe cijelu godinu nakon izdavanja. Ovaj certifikat će biti najkorišteniji u cijelom sistemu i prema tome najizloženiji. Planirana dužina ključa od 2048 bita bi trebalo osigurati bezbijednost certifikata za bar pet godina što bi trebao biti i period važenja certifikata. Zbog velike upotrebe ovih certifikata potrebno je planirati reviziju sigurnosnih uslova svake dvije godine te obnavljanje certifikata sa istim ključem nakon dvije godine, ako se sigurnosni uslovi nisu promijenili.

Certifikat vrhovne CA treba imati najduže vrijeme valjanosti u sistemu. Po do sada planiranom to mora biti duže od pet godina. Vrhovna certifikacijska ustanova će izdavati vrlo mali broj certifikata, samo korisničkim certifikacijski

ustanovama, i biće držana odvojena od računarske mreže (*offline*) na fizički sigurnoj lokaciji što je čini prilično neizloženom i vrlo sigurnom. Prema ranijoj diskusiji o dužini ključeva, planirani ključ od 4096 bita bi trebao garantovati sigurnost i za narednih dvadeset godina. Međutim ovo je ogroman period za oblast računarske sigurnosti, a i očekivati je i neke administrativne promjene u ovom periodu. Period važenja od deset godina sa obnavljanjem nakon pet godina bi trebao biti dovoljno siguran, ali i dovoljno dug da se ne poremeti vrijeme valjanosti svih podcertifikata.

Prema gore navedenom predloženi periodi valjanosti po tipovima certifikata su slijedeći:

- Vrhovna CA – 10 godina, obnavljanje nakon 5 godina
- Izdavačka CA – 5 godina, obnavljanje nakon 2 godine
- Krajnji korisnici – 1 godina, do pet obnavljanja sa istim ključem

3.3.3 Rezime

Razmatrana je konfiguracija certifikata koja može zadovoljiti definisane potrebe visokoškolske ustanove. Predložen je X.509 v3 format certifikata. Unutar ovog formata navedena su potrebna polja sa njihovim vrijednostima. Pri ovome se vodilo računa da se pored tehničkih standarda zadovolje i pravni zahtjevi koje certifikati moraju zadovoljiti da bi bili smatrani kvalifikovanim certifikatima. Predloženi su kriptografski algoritmi za certifikate: SHA-1 za *hash* funkciju, RSA za javne ključeve i kombinacija RSA sa SHA-1 za digitalno potpisivanje. Za RSA algoritam razmatrane su potrebne dužine ključeva koje će obezbjediti potrebnu sigurnost vodeći računa da trajanje kriptografskih operacija ne bude duže nego što je neophodno. Predložene dužine ključeva su 1024 bita za krajnje korisnike, 2048 bita za izdavačku CA i 4096 bita za vrhovnu CA. Na kraju su predloženi periodi valjanosti različitih tipova certifikata: jedna godina za krajnje korisnike, pet godina za izdavačku CA i 10 godina za vrhovnu CA. Prolaskom kroz ovaj proces donesene su sve važne

odluke vezane za konfiguraciju certifikata. Ovim bi posao konfigurisanja CA aplikacije trebao biti vrlo pojednostavljen i sveden na relativno jednostavnu interaktivnu instalaciju izabrane softverske aplikacije za implementaciju CA. Ostalo je još da se odgovori na pitanja vezana za upravljanje ovako definisanim certifikatima što će biti predmet razmatranja u nastavku rada.

3.4 Definisanje plana upravljanja certifikatima

Nakon što su, na osnovu utvrđenih potreba, definisani potrebna konfiguracija CA i digitalnih certifikata preostalo je još da se razmotri upravljanje certifikatima i predloži odgovarajući plan. Na ovaj način bi se definisali svi elementi PKI sa međusobnim interakcijama.

Svi detalji upravljanja neće biti razmatrani jer su neki čisto administrativni i rješeni su ili unutar sam aplikacije koja se koristi za CA ili su usko povezani sa drugim administrativnim procedurama na visokoškolskoj ustanovi. Detaljno će biti razmotreni oni aspekti upravljanja certifikatima koji obično predstavljaju najveću smetnju kod uvođenja PKI. Kako je u pregledu postojećeg stanja u oblasti PKI rečeno, velika kompleksnost PKI rješenja je jedan od glavnih razloga za teže odlučivanje organizacija za izgradnju PKI ili čak za neuspjeh takve izgradnje. Dobar dio pomenute kompleksnosti potiče od procedura i elemenata upravljanja certifikatima. Kako je cilj rada da predstavi izvodljiv PKI, težiće se jednostavnosti rješenja. Razmotriće se metode dobijanja i obnavljanja certifikata i mogućnost njihove integracije sa postojećom administrativnom infrastrukturom na visokoškolskim ustanovama. Sigurnost privatnih ključeva, kao osnova sigurnosti PKI, će biti detaljno izložena i biće predloženo odgovarajuće rješenje. Na kraju će biti izložena problematika spremišta certifikata i opozivanja certifikata, koja je bolna tačka PKI. Biće predloženo sigurno i praktički izvodivo rješenje.

3.4.1 Metode dobijanja i obnavljanja certifikata

Procedure inicijalnog izdavanja certifikata obično su jedan od najveći uzroka adminstrativne komplikovanosti izgradnje infrastrukture javnih ključeva. Razlog za ovo leži u činjenici da je za kvalitetan certifikat nepohodno da krajnji korisnik, subjekat certifikata, bude pozitivno identikovan. Pozitivna identifikacija u ovom kontekstu znači utvrđivanje nedvojbene pouzdanosti podataka o subjektu koji će se nalaziti u certifikatu. Certifikat povezuje

podatke o subjektu sa njegovim javnim ključem. Certifikacijska ustanova svojim potpisom garantuje ispravnost podataka u certifikatu. Na primjer, ako u certifikatu stoji samo e-mail adresa subjekta, CA mora utvrditi da ta e-mail adresa zaista "pripada" imaocu privatnog ključa kome odgovara. Pripadnost e-mail adrese je zapravo teško utvrditi, ono što CA zapravo potvrđuje je da subjekt ima pristup adresi, odnosna da na nju može primati i sa nje slati poruke. Provjera ovog pristupa je prilično jednostavna i ne zahtjeva više od razmjene e-mail poruka između subjekta i certifikacijske ili registracijske ustanove. Ovo je primjer vrlo jednostavnog certifikata vrlo ograničene upotrebljivosti. U principu što su precizniji podaci o subjektu, to je certifikat veće upotrebne vrijednosti, ali zahtijeva od certifikacijske ustanove više truda u provjeravanju ovih podataka. Potrebna preciznost podataka o subjektu koji se nalaze na certifikatu zavisi od namjene certifikata. Velike firme koje se bave prodajom PKI usluga, kao Verisign, imaju više različitih tipova certifikata u zavisnosti od nivoa povjerenja u identitet subjekta certificiranja [65]. Kvalifikovani certifikati koji se izdaju ljudima moraju sadržavati prepoznatljivo (*distinguished*) ime subjekta [55]. Za ovo je neophodno da je subjekt certificiranja poznat certifikacijskoj ustanovi. Poznat ovdje znači da se osoba sa pomenutim imenom identificirala certifikacijskoj ustanovi.

Najsigurniji način da se ova identifikacija obavi je lično pojavljivanje osobe sa zvaničnim identifikacijskim dokumentima u certifikacijskoj ustanovi ili nekoj od registracijskih ustanova, ako ih ima, koje obavljaju poslove identifikacije za CA. Iako je lično pojavljivanje najsigurniji način identifikacije, to nije i najjednostavniji. U slučaju da CA ima veliki broj subjekata koje treba certificirati ili je prostorno raširena po širem regionu ili čak cijelom svijetu potrebno je imati organizovanu mrežu registracijskih ustanova od povjerenja koje će obavljati ovu identifikaciju. Povjerenje je ovdje od presudnog značaja, jer kako je već rečeno povjerenje u CA je ključ za buduće povjerenje u certifikate. Organizovanje ovakve mreže je veliki administrativni i logistički zadatak. To je jedan od razloga što se postojanje jedne vrhovne svjetske

certifikacijske ustanove koja bi potvrđivala digitalne certifikate svih stanovnika zemlje i kojoj bi svi stanovnici vjerovali teško može realizovati.

Poseban slučaj prestavljaju zatvoreni sistemi u kojima su članovi sistema već poznati administrativnim strukturama. Ovakve sisteme čine sve vrste organizacija koje svojim članovima izdaju identifikacijske dokumente na osnovu pripadnosti organizaciji. Primjeri ovakvih organizacija su sve vrste poslovnih sistema, od malih do velikih kompanija, i obrazovne institucije. Postojeća infrastruktura identifikacije unutar ovih sistema čini ih vrlo pogodnim za nadogradnju i infrastrukture javnih ključeva.

Prije prelaska na prijedlog konkretne metode izdavanja certifikata na visokoškolskoj ustanovi potrebno je razmotriti još jedan aspekt ovog procesa. To je pitanja generisanja para ključeva, privatnog i javnog. Ovaj par ključeva može generisati sam subjekt, certifikacijska ili registracijska ustanova. Sam proces generacije ključeva nezavisno od toga ko ga obavlja može biti izveden u softveru ili hardveru. U slučaju da par ključeva ne generiše subjekat potrebno je obezbijediti siguran način njegovog dostavljanja subjektu. To se može učiniti fizičkim predavanjem ključa na nekom elektronskom mediju, slanjem sigurnog uređaja za pohranjivanje ključeva, kao što je pametna kartica, ili elektronskom isporukom koristeći SSL. U slučaju kada subjekt generiše par ključeva potrebno je obezbijediti bezbjedno dostavljanje javnog ključa certifikacijskoj ustanovi. Uobičajen način je elektronski transfer koristeći SSL ili elektronskom porukom koju je potpisala registracijska ustanova. [48]

Prednost generisanja para ključeva od strane krajnjeg korisnika - subjekta certifikata je što u tom slučaju privatni ključ nikada nije dostupan nikome osim samom subjektu. Ovim je subjekat u potpunosti odgovoran za privatni ključ i njegovu upotrebu. Takođe nema rizika koji transfer privatnog ključa od CA do subjekta nosi. Sa druge strane, organizacija može zahtijevati generisanje svih parova ključeva na jednom centralnom mjestu. Na taj način se omogućava sigurnosno pohranjivanje kopija korisničkih privatnih ključeva.

Ovo može biti važno ako se ključevi koriste za šifriranje podataka koji se pohranjuju na neki medij, jer u slučaju gubitka privatnog ključa kojim su šifrirani, bez sigurnosne kopije privatnog ključa bilo bi ih nemoguće dešifrovati. Drugi razlog za centralno generisanje parova ključeva može biti odluka organizacije da koristi specijalizovan hardver za generisanje kvalitetnijih ključeva. Naravno u ovom slučaju ostaje pitanje sigurnog dostavljanja privatnog ključa korisniku. Takođe je važno osigurati da privatni ključevi korisnika ne budu dostupni nikome osim ovlaštenoj osobi i to samo u slučaju gubitka privatnog ključa od strane krajnjeg korisnika. [36]

Predloženo riješenje za proceduru inicijalne registracije krajnjih korisnika i izdavanje certifikata na visokoškolskoj ustanovi oslanja se na pogodnost da se radi o zatvorenom sistemu. Svi budući korisnici moraju proći kroz već postojeću administrativnu proceduru priključivanja sistemu, koja je nezavisna od buduće PKI. Studenti se priključuju sistemu prilikom upisa na visokoškolsku ustanovu, a uposlenici prilikom zasnivanja radnog odnosa. Postojeća infrastruktura i procedure priključivanja organizaciji trebaju biti iskorištene i proširene koracima neophodnim za izdavanje certifikata. Podaci kojima se identificira subjekat certifikata se prikupljaju u sklopu postojećih procedura i krajnji korisnici se lično pojavljuju u odgovarajućim administrativnim službama.

Ovim je prvo pitanje izdavanja certifikata, identifikacija, u potpunosti riješeno. Preostalo je da se utvrdi procedura generisanja para ključeva i uručivanja certifikata. S obzirom da je namjena certifikata obezbjeđenje sigurne Web i e-mail komunikacije, a ne šifriranje podataka koji se čuvaju, nema potrebe za čuvanjem sigurnosnih kopija privatnih ključeva krajnjih korisnika. Poseban slučaj čine privatni ključevi rukovodstva i računarskih i PKI administratora, te računarskih servera, koje je potrebno sigurnosno pohraniti zbog njihove posebne važnosti i vezanosti za funkciju koju obavljaju, a ne za ličnost koja ih koristi. Ostali krajnji korisnici mogu koristiti svoje privatne ključeva za

šifriranje podataka koje pohranjuju na diskove i ostale trajne medije za svoje lične potrebe, ali se o kreiranju sigurnosne kopije privatnih ključeva moraju pobrinuti sami. Ako je utvrđeno da se sigurnosne kopije privatnih ključeva standardnih krajnjih korisnika ne trebaju koristiti otpada jedan od razloga za centralo generisanje parova ključeva. Drugi razlog bi mogao biti utvrđena potreba za specijalnim hardverom za generisanje kvalitetnijih ključeva. S obzirom na planiranu namjenu infrastrukture javnih ključeva, te finansijske resurse koje bi specijalizovani hardver zahtijevao njegova nabavka i korištenje nisu opravdani. Prema tome parove ključeva će generisati sami krajnji korisnici. Teoretski, krajnji korisnici mogu ključeve generisati u hardveru ili softveru, ali praktično ne postoji potreba niti resursi za posebnim hardverskim modulima kod krajnjih korisnika. Kvalitet i sigurnost softverski generisanih ključeva je dovoljna za planiranu namjenu.

Pitanje dostavljanja javnog ključa certifikacijskoj ustanovi, te povrata potpisanog certifikata krajnjim korisnicima treba biti riješeno na najjednostavniji siguran način. Za studente se predlaže slijedeća procedura:

Prilikom upisa na visokoškolsku ustanovu studenti popunjavaju veliki broj dokumenata. Ti dokumenti su uglavnom u štampanoj formi, ali se može očekivati njihovo postepeno pomjeranje *on-line*, i ovaj projekat treba biti poticaj u tom pravcu. Nezavisno od oblika ostalih upisnih dokumenata potrebno je dodati korake za digitalno certificiranje studenata. Prije nego što se studenti lično pojave u studentskoj službi sa svim dokumentima biće potrebno da putem *Web*-a popune zahtijev za izdavanje digitalnog certifikata od strane visokoškolske ustanove. Sve savremene aplikacije koje implementiraju funkciju certifikacijske ustanove imaju ovu mogućnost. Studenti bi putem HTTPS protokola pristupili određenoj stranici na visokoškolskoj Web lokaciji. Nakon popunjavanja potrebnih podataka, kojih bi trebalo bit minimalni skup, jer već postoje u drugim dokumentima, njihov *browser* bi generisao par ključeva i predao serveru javni ključ za certificiranje.

Pošto se koristi HTTPS osigurana je privatnost, a prije svega integritet javnog ključa koji se šalje od korisnika do servera. Privatni ključ nikad ne napušta računar na kom je generisan čime je osigurana njegova privatnost i potpuna kontrola od strane krajnjeg korisnika ključa. Posebno pitanje predstavlja sigurnost privatnog ključa na računaru, ali će taj aspekt sigurnosti biti obrađen kasnije. Po završetku ovog procesa korisnik dobiva jedinstveni identifikacijski niz karaktera ili broj koji je neophodno predočiti u studentskoj službi prilikom zahtjeva za izdavanje certifikata. Ovim brojem se osigurava da je student, koji se pojavi u studentskoj službi, gdje će biti pozitivno identificiran, zaista onaj koji je generisao par ključeva i zatražio izdavanje digitalnog certifikata.

U sklopu procedure upisa službenici studentske službe će, kada upis bude zvaničan, pokrenuti proceduru na aplikaciji CA koja će odobriti izdavanje certifikata. Izdati certifikat CA aplikacija smješta u spremište certifikata. Student ponovo pristupa, putem HTTPS-a sa istog računara sa kog je uputio zahtjev i na kom se nalazi privatni ključ, W*eb* stranici visokoškolske ustanove na kojoj će moći pokupiti svoj odbreni certifikat. Ovim je omogućen siguran prenos izdatog certifikata do krajnjeg korisnika kom se certifikat izadje. Nakon toga se za identifikaciju i osiguravanje sigurnosti komunikacija koriste isključivo certifikati. Ovom procedurom su ispunjeni svi zahtjevi za sigurno izdavanje digitalnih certifikata. Slična procedura koja bi se oslanjala na iste module može se provesti i za certificiranje uposlenika. Ovdje bi učesnici u procesu bili budući uposlenici i kadrovska služba.

Kako se certifikati izdaju na određeni rok potrebno ih je obnavljati. Obnavljanje certifikata bi se obavljalo prilikom produženja pripadnosti visokoškolskoj ustanovi. Prilikom daljih upisa na naredne godine studija studentski certifikati bi bili obnavljani. Slična procedura bila bi i sa uposlenim prilikom obnavljanja ugovora ili reizbora u zvanja.

3.4.2 Sigurnost privatnog ključa

Sigurnost dobrog kriptografskog sistema zasnovana je na dužini i sigurnosti ključa, a ne na navodnoj tajnosti algoritma. Sigurnost kriptografije sa javnim ključem zasnovana je na dužini i sigurnosti privatnog ključa. Potrebna dužina ključa za konkretan sistem je utvrđena u ranijem razmatranju. Ostalo je da se razmotri sigurnost privatnog ključa. Privatni ključ u PKI predstavlja subjekat certifikata. Posjedovanje privatnog ključa omogućava digitalno potpisivanje poruka i dešifriranje poruka šifriranih odgovarajućim javnim ključem. Ovo znači da se posjednik privatnog ključa može, u elektronskim komunikacijama koje se oslanjaju na certifikat sa odgovarajućim javnim ključem, predstavljati kao subjekat certifikata bio on to ili ne. Isto tako ako subjekat izgubi privatni ključ on se više ne može elektronskim putem identificirati kao subjekat certifikata. Postoji veliki broj teoretskih razmatranja sa ciljem da se opovrgnu dvije prethodne rečenice i onemogući lažno predstavljanje sa tuđim privatnim ključem, te omogući elektronsko dokazivanje identita u slučaju gubitka privatnog ključa. Međutim, u praksi uglavnom kompromitacija ili gubitak privatnog ključa znače kompromitaciju ili gubitak digitalnog identiteta. Za ovakve slučajeve PKI predviđa opozivanje certifikata koje će biti kasnije obrađeno i koje ima svojih problema. Bez obzira na opozivanje, koje može i da savršeno funkcioniše, postoji administrativni problem dobivanja novog certifikata i njegove distribucije te pristupa starim dokumentima šifirarnim starim javnim ključem. Postoji sigurnosni problem u periodu od kada je privatni ključ kompromitovan do trenutka kada je to otkriveno, što ne mora biti, a i uglavnom nije istovremeno. Moguće su i pravni problemi vezani za odgovornost u zavisnosti od namjene certifikata i njegove upotrebe u ovom periodu. Nijedan od ovih problema nije nerješiv, ali ih je mnogo bolje izbjeći što se postiže povećavanjem sigurnosti privatnog ključa.

Privatni ključ je digitalni podatak, niz bita koji se čuva ne nekom elektronskom mediju. Digitalni podaci su vrlo pogodni za razmjenu i kopiranje što ih čini vrlo teškim za zaštitu. U svom standardnom obliku, kao

datoteka na disku, digitalne podatke je moguće iskopirati, a da je to vrlo teško ili nemoguće otkriti. Znači, moguće je da privatni ključ bude kompromitovan, a da njegov vlasnik i ne bude svjestan toga sve dok se ne otkriju negativne posljedice. Čak i dobro zaštićen digitalni podatak na disku se prililikom korištenja učitava u radnu memoriju računara, što znači da je moguće da se ovaj podatak na savremenom računaru koji obično izvršava više programa istovremeno u nekom trenutku privremeno zapiše na dio diska koji se koristi za proširivanje radne memorije (*page* ili *swap file*). Iskusan i uporan zlonamjernik može doći do ovog podataka zapisanog u ovaj privremeni prostor na disku [20]. Ovo su razlozi protiv pohranjivanja privatnih ključeva na računarima i takozvanog softverskog šifriranja.

Alternativa su hardverski uređaji za pohranjivanje privatnih ključeva i obavljanje kriptografskih operacija nad njima. Glavni predstavnik ovakvih uređaja su pametne kartice (*smart card*). Ovo su plastične kartice veličine i oblika kreditne kartice sa ugrađenim računarskim čipom. Postoji više vrsta ovih čipova koji se ugrađuju u pametne kartice, ali onaj koji je interesantan je takozvani kriptografski. Ovaj čip omogućava, između ostalog, pohranjivanje privatnog ključa na pametnoj kartici i lokalno, tj. u čipu, obavljanje kriptografskih operacija sa ovim ključem. Na ovaj način se obezbjeđuje da privatni ključ nikad ne napušta karticu. Pored ove očigledne veće sigurnosti, pametne kartice imaju prednost što su fizička stvar poput pravog ključa prema kojoj se ljudi obično odnose kao nečemu što ima vrijednost, što treba čuvati i za koju je lako otkriti da je otuđena. Za pristup pametnim karticama u pravilu je neophodno unijeti PIN kod. Na ovaj način se pametnim karticama postiže dvostepena autentikacija korisnika koji dakle mora nešto imati - pametnu karticu i nešto znati - PIN. Ovo je vrlo sigurno rješenje, ali ima svoje praktične nedostake. Za pristup kartici potreban je čitač kartica koji se mora hardverski povezati sa računarom kao i softverski instalirati. Ovo uglavnom postavlja prevelike zahtjeve na resurse dostupne za implementaciju PKI tako

da praktična upotreba pametnih kartica u PKI još nigdje nije široko primjenjena [66].

Iz ovih razloga su predlagana i neka međurješenja. Dva glavna PKI pristupa su virtualni soft tokeni i virtualne pametne kartice. Kod PKI koji koristi virtualne soft tokene privatni ključ je šifriran lozinkom i ovako šifriran pohranjen na serveru. Korisnik se svojom lozinkom autenticira serveru što mu omogućava da preko sigurne konekcije privremeno dođe do ključa koji se onda do kraja sesije koristi lokalno za kriptografske operacije [67]. Kod PKI koji koristi virtualne pametne kartice privatni ključ korisnika je podijeljen na dva dijela, čovjeku razumljivu lozinku i tajnu komponentu. Lozinku zna samo korisnik, a tajna komponenta je pohranjena na serveru. Korisnik se autenticira serveru putem svoje lozinke i uspostavlja se sigurna konekcija. Putem ove konekcije korisnik prosljeđuje serveru podatak koji treba šifrirati. Koristeći tajnu komponetu server obavlja dio šifriranja, a ostatak se obavlja kod korisnika uz pomoć njegove lozinke [68]. Na ovaj način se kompletan privatni ključ nikada ne rekonstruiše ni na strani servera ni na strani korisnika.

Prijedlog rješenja sigurnosti privatnog ključa u PKI na visokoškolskoj ustanovi treba da bude u skladu sa potrebama i mogućnostima ustanove. Iako najsigurnije, rješenje sa pametnim karticama je vjerovatno van domašaja visokoškolske ustanove. Zapravo planirana namjena PKI ne opravdava ulaganja potrebna za upotrebu pametnih kartica za sve korisnike PKI. Kada su razmatrane sigurnosne opcije certifikata predloženo je da se pametne kartice koriste za najvrijednije korisničke privatne ključeve, rukovodstva i PKI administratora. Ovo nije teško napraviti jer se radi o vrlo ograničenom broju pametnih kartica, odnosno potrebnih čitača i instalacija. Dobra strana ovog rješenja je što su to privatni ključevi vezani za funkciju, a ne pojedinu osobu. Promjenom osobe koja obavlja neku od navedenih funkcija na fakultetu samo bi se promijenio PIN pametne kartice sa privatnim ključem i ona bi bila predata novoj osobi. Na taj način bi digitalni potpis, recimo dekana, uvijek bio

isti nezavisno od toga ko obavlja ovu funkciju. Za preostale korisnike potrebno je drugo rješenje. Virtualni smart tokeni i virtualne pametne kartice eliminišu potrebu za karticama i čitačima, ali su administrativne procedure potrebne za održavanje servera i infrastrukture koja bi podržava ova rješenja vjerovatno preteške za visokoškolske ustanove koje ili imaju jako malu IT ekipu ili je čak uopšte nemaju. Prostaje čuvanje privatnih ključeva na računaru korisnika koje i pored navedenih nedostataka može biti učinjeno prihvatljivo sigurnim.

Savremeni operativni sistemi razumiju značaj privatnog ključa i omogućavaju njegov poseban tretman. Aplikacije koje implementiraju CA omogućavaju konfiguraciju certifikata sa posebnim opcijama koje poboljšavaju sigurnost privatnog ključa. Privatni ključ se može i treba proglasiti neeksportabilnim, što znači da će operativni sistem poduzeti sve korake da spriječi ispis privatnog ključa na bilo kakav elektronski mediji. Na ovaj način se omogućava da privatni ključ nikad ne napušta računar korisnika. Teoretski je moguće da zlonamjerna osoba sa pristupom računaru kompromituje sve što postoji na računaru, ali resursi potrebni za ovo su vjerovatno veći od vrijednosti privatnih ključeva korisnika. Slučajevi praktičnih napada ove vrste još nisu objavljeni. Drugi korak koji se može i treba poduzeti je da se privatni ključ proglasi zaštićenim visokom sigurnošću. Na ovaj način prilikom svakog pristupa privatnom ključu operativni sistem informiše korisnika i zahtjeva njegovu saglasnost koja se izražava unošenjem lozinke. Kako planirana namjena PKI podrazumjeva umjeren broj digitalnih potpisivanja koja korisnik obavlja, ne više od nekoliko na dan u posebnim okolnostima, potreba da se prođe kroz proces unošenja lozinke prilikom potpisivanja ne bi trebao predstavljati smetnju. Na ovaj način je i proces digitalnog potpisivanja u potpunosti pod kontrolom korisnika-potpisnika, a ne računara, odnosno neke aplikacije. Potpisivanje dokumenta mora biti svjestan čin što se na ovaj način postiže. Proglašavajući privatni ključ neeksportabilnim i ograničavajući pristup ka njemu sa lozinkom, postiže se dvostepena autentikacija. Korisnik mora da

nešto ima, računar na kom se nalazi privatni ključ, i da nešto zna, lozinku za pristup privatnom ključu.

3.4.3 Spremišta certifikata i liste opozvanih certifikata

Objavljivanje certifikata, odnosno njihovo stavljanje javnosti na raspolaganje, a pogotovo njihovo opozivanje su bolne tačke PKI. Pitanje objavljivanja certifikata, odnosno njihovog smještanja u neko javno dostupno spremište se još i može riješiti i na drugi način. Pitanje opozivanja certifikata još uvijek nije riješeno na univerzalan način. Problem je lakše sagledati ako se vrati na inicijalnu ideju iza certifikata te njihovu namjenu. Certifikati su nastali kao dodatak na kriptografiju sa javnim ključem. Oni su trebali da uliju povjerenje trećim licima - korisnicima javnih ključeva - u informaciju o vlasniku ključa. Ovo povjerenje poticalo je od povjerenja u potpisnika certifikata, certifikacijsku ustanovu. Nakon ove ideje uvidjelo se da bi bilo vrlo pogodno napraviti neku vrstu imenika certifikata koja bi olakšala pronalaženje certifikata i javnog ključa neke osobe. Ovi imenici, odnosno spremišta certifikata, postala su dio infrastrukture javnih ključeva, koja kako joj ime kaže osigurava infrastrukturu za rad kriptografije sa javnim ključevima.

Problem je nastao kada je bilo potrebno napraviti jedno takvo upotrebljivo i javno dostupno spremište certifikata. Javno dostupno znači dostupno svim potencijalnim korisnicima certifikata za čitanje i pretraživanje. Ovakvo spremište je trebalo biti i jednostavno njegovim administratorima za ažuriranje. Krug potencijalnih korisnika certifikata može biti jako veliki, odnosno neograničen. Naći odgovarajući format i način pristupa za sve ove korisnike nije jednostavno. X.509 format certifikata je nastao kao dio specifikacije X.500 direktorija i trebao je da riješi problem kontrole pristupa ovakvim direktorijima. X.500 direktoriji su trebali da budu korak ka univerzalnim spremištima svih vrsta podataka pa i certifikata. Međutim, stroga hijerarhijska struktura X.500 modela, nije u potpunosti podobna za savremenu praktičnu upotrebu koja uglavnom uključuje alate i metode kao

što su relacione baze podataka i nehijerarhijske organizacije [69]. Ipak dva najveća problema spremišta certifikata su bila kako pronaći spremište, direktoriji, u kom se nalazi certifikat osobe čiji javni ključ tražimo, te kako, kada je pronađeno spremište, pronaći certifikat te osobe čije ime (i prezime) ne mora biti jedinstveno u tom spremištu [40].

Praktična rješenja ovog problema polaze od osnovnih namjena kriptografije javnih ključeva. Kada se certifikat koristi za identifikaciju, odnosno autentikaciju, na osnovu koje se vrši autorizacija ili provjera digitalnog potpisa, uobičajeno je da entitet koji se autenticira priloži uz svoju elektronsku prijavu i odgovarajući certifikat. Na ovom principu rade dva najkorištenija protokola koja koriste certifikate, S/MIME i SSL. Kada je certifikat, odnosno javni ključ, subjekta potreban da bi mu se poslala šifrirana poruka uobičajena su dva rješenja. Lokalno rješenje podrazumjeva zatvoreni sistem u kom postoji jedinstveno spremište certifikata u kom je provedena neka politika jedinstvenosti imena subjekata. Primjeri ovoga su adresari implementirani u savremenim aplikacijama za saradnju (Microsoft Exchange, IBM Domino) koji omogućavaju uključivanje digitalnih certifikata u podatke o subjektu i jednostavno pretraživanje. Globalnog rješenja nema i teško da ga može biti. Iako postoje neke vrste spremišta certifikata koja su planetarno dostupna, to jest koje imaju geografski široko rasprostranjene subjekte, ipak se jedinstvena identifikacija subjekata može postići samo unutar tih spremišta, odnosno sistema koje pokrivaju, što ih, u suštini, čini lokalnim. Jedno od rješenja koje izalazi iz lokalnih okvira opet podrazumjeva dobivanje certifikata direktno od subjekta kome se želi poslati šifrirana poruka. Ovo podrazumjeva da postoji povjerenje u CA koja je potpisala certifikat koji je subjekt poslao.

Navedena praktična "rješenja" problema distribucije certifikata otvorila su mnogu veći problem, opozivanje certifikata. Već je rečeno da certifikat, odnosno veza subjekta sa javnim ključem, može postati nevažeći prije svog isticanja naznačenog u samom certifikatu. Razlozi za ovo mogu biti gubitak ili

kompromitacija privatnog ključa subjekta, kao i prestanak povezanosti subjekta i CA iz koje je proizilazilo povjerenje CA u identitet subjekta iskazano izdavanjem certifikata. Informaciju o prestanku važenja certifikata, opozivanje, je potrebno učiniti dostupnom svim trećim licima, potencijalnim korisnicima certifikata za identifikaciju subjekta certifikata ili šifriranje komunikacije sa njim.

U početnoj ideji sa globalnim direktorijima predviđene su liste opozvanih certifikata (CRL) koje se objavljuju u istom direktoriju gdje se objavljuju i certifikati. Mogućnost pretraživanja direktorija za certifikatima i njihovo čitanje podrazumjeva i mogućnost pretraživanja direktorija za opozvanim certifikatima. Liste opozvanih certifikata bi trebala da objavljuje CA koja je izdala certifikate ili takozvani ovlašteni, od strane CA, izdavača CRL. Ove liste se izdaju u predefinisanim vremenskim intervalima i imaju period važenja do vremena kada treba da se objavi nova lista. Od korisnika certifikata se očekuje da redovno provjerava najsvježiju listu opozvanih certifikata da bi utvrdio da li je certifikat koji mu je prezentiran opozvan.

Pošto se u praksi uglavnom ne koriste globalni direktoriji za distribuciju certifikata distribucija CRL na ovaj način postaje mnogo teže upotrebljiva. Problem sa provjerom CRL je isti kao i sa pronalaženjem certifikata jer je potrebno pronaći spremište, direktoriji, u kom se nalazi najsvježija lista opozvanih certifikata izdata od iste CA koja je izdala i certifikat u pitanju. Informacija o lokaciji liste opozvanih certifikata je predviđena kao polje u ekstenzijama koje su uvedene u verziji 3 X.509 formata certifikata. Ovo polje nije obavezno što znači da ova informacije ne mora postojati u certifikatu. Opet, ako je ova informacija i dio certifikata moguće je da bi provjera ove liste, koja se može nalaziti na nekom serveru na drugom kraju svijeta, trajala predugo za bilo kakvu "živu" aplikaciju. U slučaju da je moguće pronaći listu opozvanih certifikata i izvršiti provjeru u prihvatljivom vremenu, većina aplikacija pamti vrijeme isticanja liste opozvanih certifikata i ne vrši novu

provjeru do ovog vremena. Ako je u međuvremenu, došlo do opozivanja certifikata i objavljena je nova lista ona neće biti uzeta u obzir.

Da bi se ostvarila stalna ažurnost validnosti podataka svaka upotreba certifikata bi zahtijevala učitavanje najsvježije liste opozvanih certifikata. Liste opozvanih certifikata u svom izvornom obliku uključuju sve opozvane certifikate, a ne samo razlike u odnosu na prethodno opozvanu listu. Ove stalne provjere bi prouzrokovale toliki promet podataka na svakoj računarskoj mreži da bi ona postala praktički neupotrebljiva. Ovaj promet bi predstavljao, nezlonamjerni i neplanirani, DDOS (*distributed denial-of-service*) napad. Lako je zamisliti rezultate planiranog napada zlonamjernog napadača koji bi stalnim upitima za listom opozvanih certifikata onesposobio server na kome se lista nalazi da ispunjava ikakve zahtjeve drugih korisnika Čak i bez stalnih provjera liste opozvanih certifikata javlja se veliki porast u mrežnom prometu i upita ka serveru u periodu kad ističe važenje liste i svi klijenti koji se oslanjaju na ovo vrijeme traže novu listu.

Za problem opozivanja certifikata ne postoji univerzalno rješenje, ali postoje neki pristupi ovom pitanju koji olakšavaju provjeru validnosti certifikata. SPKI [42] [43] rješenje ne koristi opozivanje certifikata. Certifikati se izdaju na kraći period i sa usko definisanom namjenom. SET (*Secure Electronic Transaction*) [70] ne opoziva certifikate već jednostavno uklanja nevažeće certifikate iz centralnog spremišta certifikata. Ovo rješenje podrazumjeva *online* provjeru certifikata i oslanja se na mali broj poznatih spremišta kod velikih finasijskih ustanova. Recimo, najraširenija upotreba nekog oblika PKI, korištenjem modela pohranjenih certifikata vrhovnih CA u *Web browser*-e, u potpunosti ignoriše pitanje opozivanje certifikata pohranjenih CA. Certifikati su dio *browser*-a i ne mijenjaju se bez direktne intervencije korisnika, koje su rijetke i na njih se i ne računa, ili instalacije nove verzije browser-a. Rivest [71] je predložio neke principe rada koji bi eliminisali problem opozivanja certifikata. Ovi principi kažu da bi korisnik certifikata trebao postavljati

zahtjeve na "svježinu" certifikata, a da je obaveza subjekta certificiranja, odnosno onoga prezentira certifikat kao identifikacioni dokument, da obezbjedi sve podatke potrebne da posvjedoče o važenju certifikata, što može uključivati i najnoviju listu opozvanih certifikata. Ovi principi su u skladu sa pomenutim rješenjima.

Rješenje koje se predlaže za konkretan PKI koji se obrađuje u ovom radu koristi pogodnosti organizacije u koju se uvodi PKI i planiranu namjenu PKI. Osnovna pogodnost je činjenica da je visokoškolska ustanova zatvoren sistem što za neke namjene omogućava lokalno rješenje. Planirana namjena PKI, odnosno certifikata, je za digitalno potpisivanje dokumenta i sigurnu e-mail komunikaciju. Na osnovu ove namjene se definiše procedura pronalažnja certifikata i provjere njihove validnosti. Digitalno potpisivanje dokumenta koje treba biti omogućeno za neke namjene, kao što su prijavljivanje ispita i objavljivanje rezultata, bi se radilo koristeći *Web*. Pod ovim se podrazumjeva upotreba *Web browser*-a od strane autora i potpisnika dokumenta za komunikaciju sa *Web* serverom koja se može odvijati u okviru lokalne mreže ili preko Interneta. Radi jednostavnosti i jedinstvenosti rješenja i načina potpisivanja bi bilo pogodno sva ostala planirana digitalna potpisivanja dokumenata napraviti na ovom principu što ne predstavlja veći problem. U cilju pomenute jednostavnosti neophodno je izbjeći komplikovane procedure potpisivanja koje mogu zbuniti korisnike i dovesti do problema opisanih u [41].

Korisnik, potpisnik dokumenta prijavljuje se na *Web* server sa svojim korisničkim imenom i lozinkom koristeći HTTPS protokol kojim se osigurava da je server zaista onaj kom se želi pristupiti, šifriranje i integritet podataka koji se razmjenjuju. U ovom trenutku nema potrebe za korisničkim certifikatom. Potrebni podaci koji će biti potpisani unose se u predefinisanu *Web* formu čiji format odgovara vrsti dokumenta. Po završetku unosa korisnik pritiskom miša na dugme na kome bi trebalo jednostavno pisati "POTPIŠI I

POŠALJI" započinje proceduru digitalnog potpisivanja i slanja podataka serveru. Ovim se korisnički ekran čini maksimalno jednostavnim i šanse za greške korisnika su svedene na minimum. (Greške prilikom unosa podataka nisu predmet ovog razmatranja i njihovo otklanjanje spada u domen u drugoj literaturi dobro obrađene teme *Web* programiranja).

Proces koji se odvija nakon pritiska na dugme je onaj koji je opisan u teoretskom dijelu o digitalnim poptpisima. Skup podataka unesnih na formi uz dodatak informacije o vremenu i datumu se propušta kroz *hash* funkciju, ta zatim šifrira privatnim ključem korisnika. Aplikacija će pokušati pristupiti privatnom ključu korisnika da bi izvršila ovu operaciju. Kako je ranije objašnjeno privatni ključ bi trebao biti pohranjen ili na računaru korisnika ili na pametnoj kartici. Pristup ključu će zahtijevati od korisnika da unese odgovarajući pristupni kod, lozinku za privatni ključ pohranjen na računaru, a PIN-a za onaj na pametnoj kartici. Korisnik će o ovome biti obaviješten putem dijaloga koji bi u uputstvu korisnicima morao biti jasno opisan i koji je u suštini vrlo jednostavan. Unošenje pristupnog koda još jednom potvrđuje namjeru korisnika da potpiše dokument. Nakon ovoga se podaci sa forme zajedno sa potpisom šalju serveru.

Server na osnovu prijave korisnika pretražuje spremište certifikata koje se nalazi na poznatoj lokaciji u lokalnoj mreži. Spremište certifikata uključuje i informaciju o tome da li je certifikata opozvan. Ova informacije se automatski generiše prilikom objavljivanja liste opozvanih certifikata od strane izdavačke CA. Izdavačka CA objavljuje listu opozvanih certifikata jednom dnevno što je dovoljno čest interval za broj dokumenta koji se potpisuju i njihovu vrijednost. Oblik spremišta certifikata se ovdje ne definiše. To može biti bilo koji oblik pohranjivanja podataka koji postoji u organizaciji od običnih datoteka do relacionih baza podataka. Bitno je da su njegova lokacija i format zapisa poznati ovoj aplikaciji koja pruža uslugu digitalnog potpisivanja na *Web* serveru. U koliko se pronađe certifikat i potvrdi da nije opozvan, uz pomoć

javnog ključa iz certifikata se vrši provjera digitalnog potpisa. Ako je potpis potvrđen podaci sa forme se zajedno sa potpisom pohranjuju u bazu za buduće prikazivanje. Na ovaj način je traženje certifikata i provjera njihove validnosti lokalizovana i stavljena u zadatak aplikaciji koje se izvršana na *Web* serveru. Postiže se željena ažurnost uz minimalne troškove resursa. Ova provjera se obavlja samo kod potpisivanja dokumenta, a ne prilikom pristupa serveru. Na ovaj način se smanjuje broj pretraživanja spremišta certifikata i promet na računarskoj mreži. S obzirom na očekivani broj korisnika i broj dokumenata koji će biti potpisivani očekivani promet podataka i broj pretraživanja spremišta certifikata ne bi trebao predstavljati opterećenje bilo kom savremenom serveru i računarskoj mreži koji su opisani u dijelu rada koji se bavi hardverom potrebnim za konkretan PKI.

Prilikom pristupa ovim, digitalno potpisanim, podacima od strane drugih korisnika aplikacija koja pruža ovu uslugu će napraviti provjeru stanja certifikata kojim su podaci potpisani kao i validnost digitalnog potpisa. Na ovaj način će korisnici biti upozoreni ako je došlo do opozivanja certifikata ili promjene podataka od trenutka njihovog podataka. Na ovaj način se takođe otklanja i teoretska opasnost da navodni potpisnik dokumenta nije znao da je njegov privatni ključ bio kompromitovan u trenutko kad su podaci potpisani te da je podatke potpisao neko drugi sa tim kompromitovanim ključem.

Za sigurnu e-mail komunikaciju predlaže se iskorištavanje pogodnosti zatvorenog sistema koji omogućava provedbu politike jedinstvenosti imena subjekata i pomenutu mogućnost dodavanja digitalnih certifikata u adresar aplikacije koja se koristi za e-mail komunikaciju na visokoškolskoj ustanovi. Prilikom izdavanja certifikata oni bi bili dodavani u adresare. U slučaju opozivanja certifikata opozvani certifikati bi bili uklanjani iz adresara.

Što se tiče korisnika van sistema visokoškolske ustanove ovo rješenje se ne bavi njima i ne pruža im nikakve posebne pogodnosti u odnosu na ranije pomenuta rješenja. Ako neko van visokoškolske ustanove želi sigurnu

komunikaciju sa članovima visokoškolske ustanove mora koristiti klasičnu metodu distribucije certifikata i lista opozvanih certifikata. Znači trebaju od korisnika sa kojim žele komunicirati dobiti certifikat i sami provjeravati da li je isti opozvan. Liste opozvanih certifikata će biti u svom standardnom formatu objavljivane na javno dostupnoj lokaciji.

Na ovaj način se problem distribucije certifikata i provjere njihove validnosti automatizuje i u potpunosti sakriva od korisnika. Korisnici samo dobivaju informacije ako postoji neka neregularnost. Dokumente nije moguće potpisati certifikatom koji je opozvan. Dokumenti koji su potpisani certifikatom koji je kasnije opozvan su posebno označeni. Nije moguće poslati šifriranu e-mail poruku nekome čiji je certifikat opozvan.

3.4.4 Rezime

Razmatrano je upravljanje certifikatima sa posebnim osvrtom na one aspekte ovog procesa koji su najteži za implementaciju i podižu kompleksnost PKI. Navedeni su u praksi korišteni pristupi ovim problemima. Preložena su konkretna rješenja za svako od razmatranih pitanja. Inicijalno izdavanje certifikata i njihovo obnavljanje je najbolje integrisati sa postojećim administrativnim procedurama upisa studenta, izbora nastavnog osoblja i zapošljavanja vannastavnog osoblja. Predloženo rješenje podrazumjeva minimalno proširenje zadataka i maksimalnu jednostavnost za one koji inače obavljaju ove procese. Par ključeva, privatni i javni, treba da se generiše na računarima krajnjih korisnika, subjekata certifikata, koristeći *Web* stranicu visokoškolske ustanove. Ovaj proces je jednostavan i ne zahtjeva posebno znanje od subjekata certificiranja. Privatni ključevi se čuvaju na računaru gdje su kreirani kao zaštićeni podatak visoke sigurnosti što se postiže odgovarajućom konfiguracijom certifikata i aplikacije koja ih generiše. Na ovaj način je pristup privatnom ključu omogućen samo onima koji imaju pristup računaru i koji znaju lozinku za pristup ključu, što predstavlja dvostepenu autentikaciju. Digitalni certifikati korisnika bi se čuvali na lokaciji dostupnoj

Web aplikaciji koja omogućava digitalno potpisivanje dokumenata i ova aplikacija bi se brinula za provjeru opozvanosti certifikata. Certifikati bi također bili dodani u e-mail adresar korisnika visokoškolske ustanove. Opozvani certifikati bi se automatski uklanjali iz adresara. Standardna lista opozvanih certifikata bi se izdavala za vanjske korisnike.

4 ZAKLJUČAK

Ovaj rad se bavi izgradnjom infrastrukture javnih ključeva (PKI) na visokoškolskoj ustanovi. PKI je sistem koji omogućava sigurne komunikacije preko nesigurnih medija uz pomoć kriptografije sa javnim ključevima. PKI ideja nije nova, ali praktične implementacije ovakvih sistema su uglavnom komplikovane i zahtijevaju velike materijalne i ljudske resurse. Visokoškolske ustanove imaju specifične zahtjeve i prilično ograničene resurse koje mogu posvetiti izgradnji i održavanju PKI. Vodeći računa o ovim specifičnostima i ograničenim resursima, rad predlaže rješenje koje je prihvatljivo i izvodivo.

Problemi u implementaciji PKI su uglavnom uzrokovani činjenicom da se od PKI očekivalo da riješi sve probleme sigurnih elektronskih komunikacija i ostvari sve namjene kriptografije na globalnom nivou. Ova očekivanja su nerealna te se danas ide u pravcu jednostavnijeg PKI ograničene namjene. Implementacija PKI precizno definisane namjene u zatvorenim sistemima ima mnogo veće šanse za uspjeh. Visokoškolska ustanova je zatvoren sistem u kome se uz dobro definisanu namjenu može implementirati PKI sa dostupnim resursima. Rad koristi pogodnost zatvorenog sistema i polazi od definisanja potreba koje se žele zadovoljiti da bi se definisala namjena PKI.

Na samom početku rada ukratko su objašnjene teoretske osnove na kojim je PKI zasnovan. Ovdje su definisani svi pojmovi, protokoli i procedure koji se koriste u nastavku rada koji se konkretno bavi implementacijom PKI.

U prvom dijelu rada koji se bavi definisanjem potreba za digitalnim certifikatima utvrđen je skup usluga koje PKI treba da pruža. Ove usluge su *Web* autentikaciija, digitalno potpisivanje i sigurna e-mail komunikacija. Na osnovu ovog skupa usluga definisane su potrebne aplikacije koje ih pružaju. Potrebne aplikacije su *Web* browser i e-mail klijent, koji su standardni dio svakog poslovnog računarskog okruženja, te minimalna količina *Web* baziranih programa. Utvrđene su grupe korisnika korisnika ovih usluga te

definisane njihove potrebe za certifikatima koji će im omogućiti navedene usluge. Otvoreno je pitanje dokumentovanja PKI kroz dva dokumenta: Politiku certificiranja i Izjavu o praksi certificiranja. Politika certificiranje se može posmatrati kao dokumentovanje namjene PKI. Izjava o praksi certificiranja se može posmatrati kao dokumentovanje onoga kako je potrebno uraditi ono što je definisano u Politici certificiranja.

Nakon definisanja potreba utvrđena je potrebna configuracija CA koje će ih zadovoljiti. Izabran je model povjerenja koji se sastoji od vrhovne CA, koja se drži odvojenom od računarske mreže (*offline* CA), i podređene izdavačke CA, koja izdaje certifikate krajnjim korisnicima i čiji certifikat je potpisala vrhovna CA. Utvrđeno je da će sve CA biti interne odnosno uspostavljene i održavane od strane visokoškolske institucije u kojoj se uvodi PKI. Ustanovljeno je da jedna izdavačka CA može zadovoljiti potrebe korisnika kako su prethodno definisane. Funkciju registracijske ustanove će obavljati CA. Potrebni hardver za svaku od CA, vrhovnu i izdavačku, je standardna savremena serverska konfiguracija koja uključuje RAID diskove i uređaje za sigurnosno pohranjivanje podataka.

Nakon utvrđene potrebne konfiguracije CA razmatrana je konfiguracija certifikata koja može zadovoljiti definisane potrebe visokoškolske ustanove. Predložen je X.509 v3 format certifikata. Unutar ovog formata navedena su potrebna polja sa njihovim vrijednostima. Pri ovome se vodilo računa da se pored tehničkih standarda zadovolje i pravni zahtjevi koje certifikati moraju zadovoljiti da bi bili smatrani kvalifikovanim certifikatima. Predloženi su kriptografski algoritmi za certifikate: SHA-1 za *hash* funkciju, RSA za javne ključeve i kombinacija RSA sa SHA-1 za digitalno potpisivanje. Za RSA algoritam razmatrane su potrebne dužine ključeva koje će obezbjediti potrebnu sigurnost vodeći računa da trajanje kriptografskih operacija ne bude duže nego što je neophodno. Predložene dužine ključeva su 1024 bita za krajnje korisnike, 2048 bita za izdavačku CA i 4096 bita za vrhovnu CA. Na

kraju su predloženi periodi valjanosti različitih tipova certifikata: jedna godina za krajnje korisnike, pet godina za izdavačku CA i 10 godina za vrhovnu CA. Prolaskom kroz ovaj proces donesene su sve važne odluke vezane za konfiguraciju certifikata. Ovim bi posao konfigurisanja CA aplikacije trebao biti vrlo pojednostavljen i sveden na relativno jednostavnu interaktivnu instalaciju izabrane softverske aplikacije za implementaciju CA.

U završnom poglavlju razmatrano je upravljanje certifikatima sa posebnim osvrtom na one aspekte ovog procesa koji su najteži za implementaciju i podižu kompleksnost PKI. Navedeni su u praksi korišteni pristupi ovim problemima. Preložena su konkretna rješenja za svako od razmatranih pitanja. Inicijalno izdavanje certifikata i njihovo obnavljanje je najbolje integrisati sa postojećim administrativnim procedurama upisa studenta, izbora nastavnog osoblja i zapošljavanja vannastavnog osoblja. Predloženo rješenje podrazumjeva minimalno proširenje zadataka i maksimalnu jednostavnost za one koji inače obavljaju ove procese. Par ključeva, privatni i javni, treba da se generiše na računarima krajnjih korisnika, subjekata, certifikata, koristeći *Web* stranicu visokoškolske ustanove. Ovaj proces je jednostavan i ne traži posebno znanje od subjekata certificiranja. Privatni ključevi se čuvaju na računaru gdje su kreirani kao zaštićeni podatak visoke sigurnosti što se postiže odgovarajućom konfiguracijom certifikata i aplikacije koja ih generiše. Na ovaj način je pristup privatnom ključu omogućen samo onima koji imaju pristup računaru na kome se nalazi privatni ključ i koji znaju lozinku za pristup ključu, što predstavlja dvostepenu autentikaciju. Digitalni certifikati korisnika bi se čuvali na lokaciji dostupnoj *Web* aplikaciji koja omogućava digitalno potpisivanje dokumenata i ova aplikacija bi se brinula za provjeru validnosti certifikata. Certifikati bi takođe bili dodani u e-mail adresar korisnika visokoškolske ustanove. Opozvani certifikati bi se automatski uklanjali iz adresara. Standardna lista opozvanih certifikata bi se izdavala za vanjske korisnike.

Kroz navedena poglavlja dati su odgovori na sva važna kriptografska pitanja na koja je potrebno odgovoriti prije pristupanja implementaciji PKI na visokoškolskoj ustanovi. Pitanja na koja će trebati dalje odgovoriti su iz domena politike visokoškolske ustanove i domena softverskog inženjeringa.

Kako je u radu navedeno, prvi slijedeći korak u implementaciji bi trebao biti definisanje Politike certificiranja kojom visokoškolska ustanova javno definiše namjenu PKI kroz skup uslova kreiranja, izdavanja i korištenja digitalnih certifikata. Ovim dokumentom su definisana prava i obaveze visokoškolske ustanove koja izdaje certifikate, kao i subjekata certificiranja, što spada u domen politike visokoškolske ustanove. Na osnovu ove Politike i rješenja predloženih u radu potrebno je kreirati Izjavu o praksi certificiranja koja jasno definiše na koji se način provodi specificirana politika.

Na osnovu usvojene Politike certificiranja i Izjave o praksi certificiranja pristupa se izgradnji PKI. U radu je definisana potrebna konfiguracije CA bez specifikacije neke posebne aplikacije koja je implementira. U ovoj fazi biće neophodno opredjeliti se za neku od dostupnih aplikacija koja se najbolje uklapa u postojeću informatičku infrastrukturu visokoškolske ustanove. Softverske aplikacije koje implementiraju CA, i na koje se misli u radu, su uglavnom već dostupne visokoškolskim ustanovama u sklopu instaliranih operativnih sistema (Microsoft Windows Server 2000/2003) ili softverskih paketa (IBM Domino), ili su *open source* rješenja dostupna svima (OpenCA). Nijedna od ovih aplikacija ne zahtjeva nabavku novog softvera što ovo rješenje čini finansijski prihvatljivijim za visokoškolske ustanove. Instalacija ovih aplikacija, i certifikata koje one izdaju, na osnovu parametara definisanih u ovom radu je vrlo jednostavna.

Ovaj rad definiše preocedure koja obezbjeđuju siguran rad planiranih PKI aplikacija, a prvenstveno *Web* baziranih formi i njihovog digitalnog potpisivanja. Da bi planirani PKI ostvario punu funkcionalnost neophodno je ove procedure integrisati sa postojećim bazama podataka u kojima se nalaze

podaci o studentima i ispitima. U koliko takve baze ne postoje, trebale bi biti kreirane i implementirane zajedno sa PKI. U prilogu je data jedan prikaz ogledne implemetacije koja pokazuje izvodljivost nevedenih rješenja.U prikazanoj implementaciji su na najjednostavniji način, realizovane osnovne funkcionalnosti Studentske službe neophodne za demonstraciju rješenja.

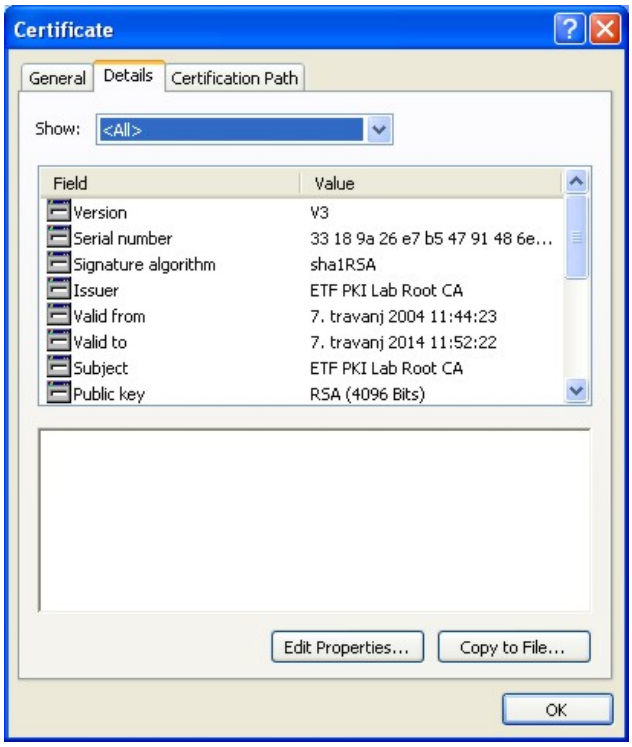
PRILOG A: OGLEDNA IMPLEMENTACIJA

U ovom prilogu je dat prikaz implementacije rješenja predloženog u radu. Implementacija je urađena kao ogledni primjer koji pokazuje izvodljivost nevedenih rješenja. Za punu funkcionalnost rješenja bilo bi ga neophodno integrisati sa sistemom za rad studentske i kadrovske službe na visokoškolskoj instituciji. Ovdje su samo, na najjednostavniji način, realizovane osnovne funkcionalnosti studentske službe neophodne za demonstraciju rješenja. U opisu implementacije će detaljnije biti predstavljeni dijelovi implementacije koji su specifični i nisu opisani na drugim mjestima. Funkcije koje su dijelovi korištenih gotovih softverskih paketa će biti navedene i upućeno na lokaciju na kojoj se mogu naći podrobnije informacija, kao što je dokumentacija proizvođača. Za konkretnu implementaciju je korištena Microsoft platforma operativnih sistema i aplikacija. Ovaj izbor ni na koji način ne favorizuje ovu platformu ili ograničava mogućnost implementacije na drugim platformama ili čak njihovu kombinaciju. Rješenja predložena u radu su na višem nivou apstrakcije i njihova primjenljivost je nezavisna od platforme na koj se implementiraju i alata koji se za to koriste. U ovom prilogu će biti prikazane osnovne procedure ogledne impementacije:

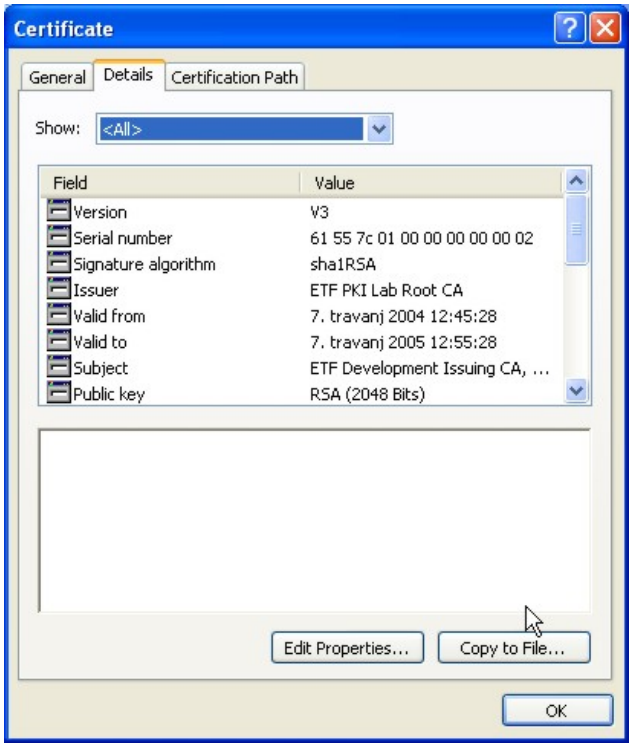
- Uspostavljanje certifikacijskih ustanova
- Izdavanje certifikata
- Prijavljivanje ispita
- Objavljivanje rezultata ispita

A.1 Uspostavljanje Certifikacijskih ustanova

Prvi korak implementacije je uspostavljanje certifikacijskih ustanova (CA). Prema utvrđenoj konfiguraciji CA potrebne su dvije CA, vrhovna i izdavačka. Obje CA su interne. Vrhovna CA se drži odvojena od računarske mreže (*offline* CA). Izdavačke CA izdaje certifikate krajnjim korisnicima i njen certifikat potpisuje vrhovna CA. Funkciju registracijske ustanove obavlja izdavačka CA. Kako je u radu rečeno uspostavljanje CA je zapravo instalacija softverske aplikacije koja obavlja ovu funkciju. U radu je predložen i hardverska konfiguracija potrebna za efikasan i pouzdan rad CA, ali je u ovoj oglednoj implementaciji korišten dostupni hardvare. Obje CA su instalirane na standardne savremene računarske radne stanice. Operativni sistem instaliran na obje CA je Microsoft Windows Server 2003 Standard Edition. Za CA aplikaciju korištena je komponenta Windows Server 2003 Certification Services. Ova komponenta je standardni dio Windows serverskih operativnih sistema od verzije 2000. Instalacija Certification Services je jednostavan proces koji se sastoji od nekoliko korisničkih ekrana na kojima je potrebno unijeti željene vrijednosti parametara CA. Ova procedura je detaljno opisana u korisničkoj dokumentaciji Server 2003 (*Help*), na Microsoft Web stranicama i u [46] i ovdje neće biti posebno izlagana. Vrijednosti parametara su one definisane u radu. Za obje CA izabrana je verzija 3 X.509 certifikata i kriptografski algoritmi: SHA-1 za *hash* funkciju, RSA za javne ključeve i kombinacija RSA sa SHA-1 za digitalno potpisivanje. Dužina ključa za vrhovnu CA je 4096 bita, a period valjanosti 10 godina. Dužina ključa za izdavačku CA je 4096 bita, a predloženi period valjanosti je pet godina, s tim što je u ovoj oglednoj implementaciji izbran period važenja od jedne godine. Prvo je instalirana vrhovna CA koja je sama potpisnik svog certifikata, a zatim izdavačka CA čiji certifikat je potpisala vrhovna CA. Na slikama 10 i 11 su prikazani certifikati vrhovne i izdavačke CA.



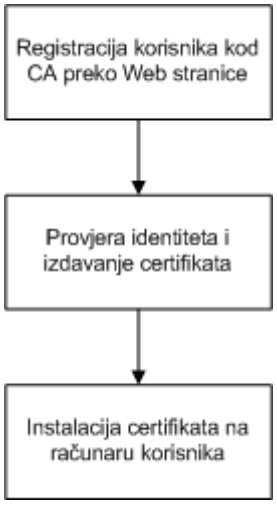
Slika 10



Slika 11

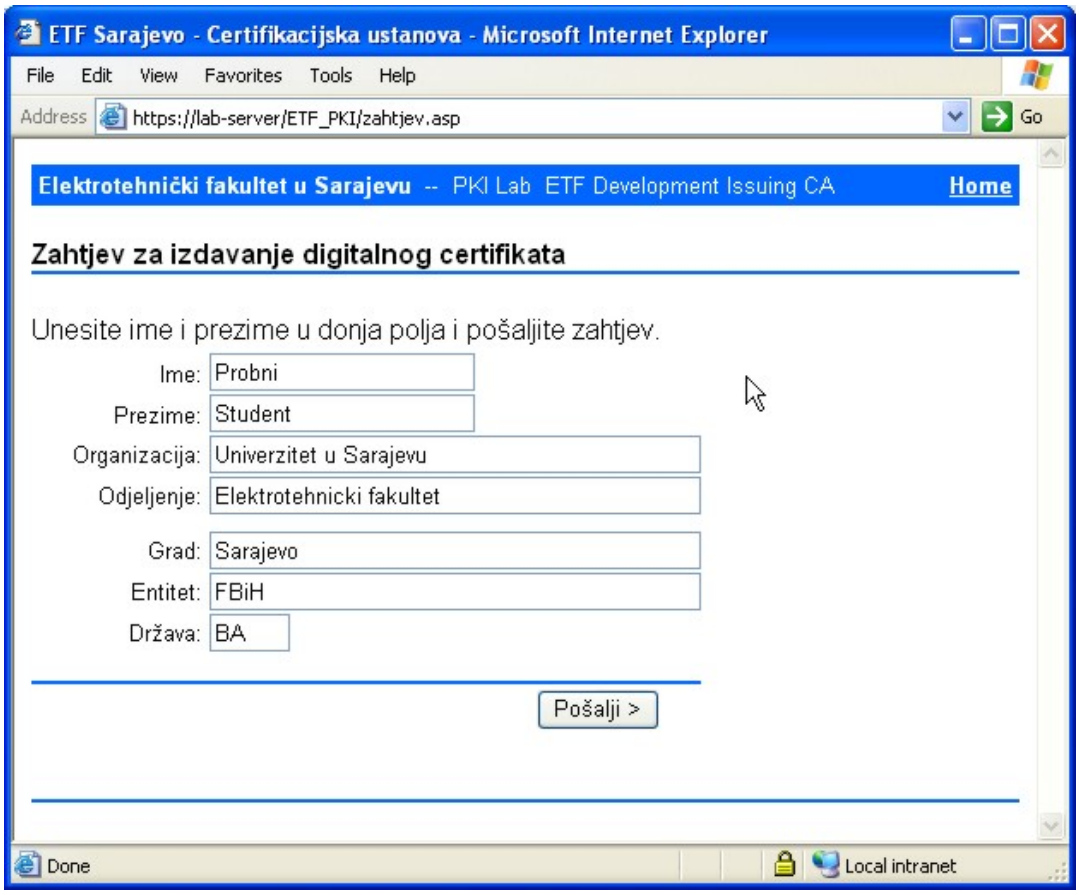
A.2 Procedura izdavanja certifikata

Nakon instalacije i aktiviranja vrhovne i izdavačke CA implementirana je predložena procedura izdavanja certifikata. Izdavanje certifikata se obavlja u tri koraka. U prvom se korisnici registruju kod CA putem W*eb* stranice i tom prilikom se generiše par ključeva, privatni javni, i zahtjev za izdavanje certifikata koji se šalje CA na potpisivanje. U drugom koraku se korisnik pojavljuje lično u studentskoj i kadrovskoj službi gdje se potvrđuje njegov identitet i izdaje mu se traženi certifikat. Treći korak se sastoji od instalacije certifikata na računaru korisnika što se opet radi preko W*eb* stranice. W*eb* stranice koje obavljaju navedene funkcije su napravljene na osnovu Microsoft primjera koji su instalirani prilikom instalacije Certificate Services. Primjeri su prilagođeni predviđenoj namjeni.



A.2.1 Registracija korisnika

Na slici 12 dat je prikaz *Web* stranice na kojoj korisnik popunjava zahtjev za izdavanje certifikata. Stranici se pristupa koristeći HTTPS protokol čime se osigurava privatnost podataka koji se razmjenjuju i identitet *Web* servera. Korisnik popunjava samo polja sa imenom i prezimenom, vrijednosti ostalih polja se automatski popunjavaju.



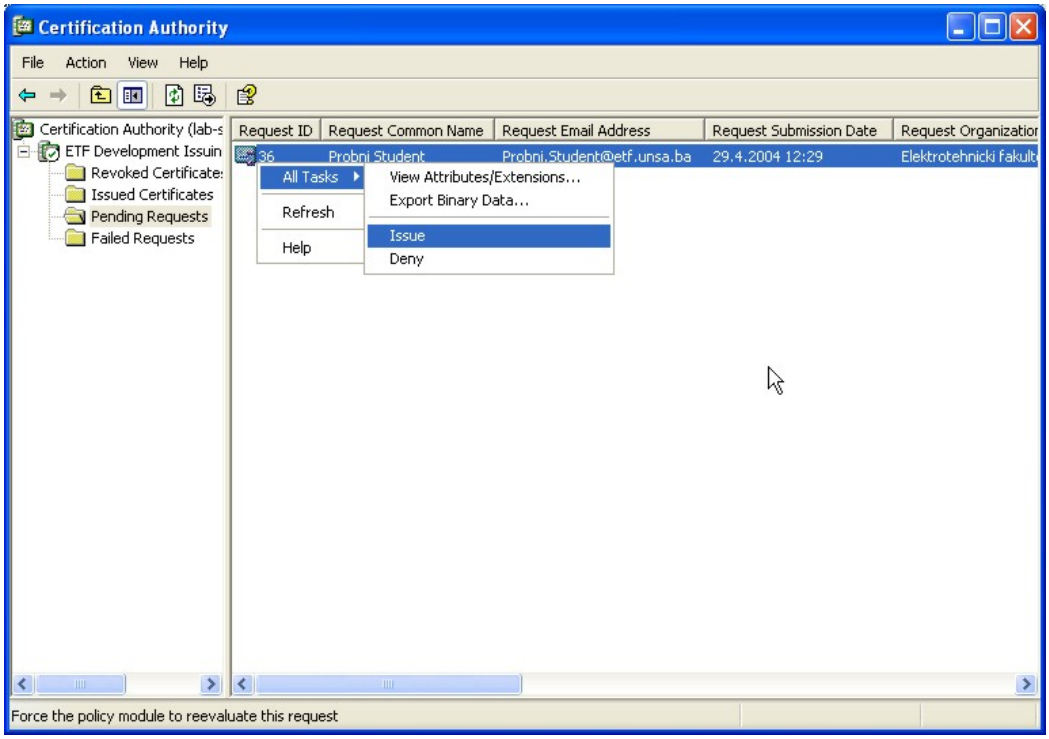
Slika 12

Pritiskom na dugme "Pošalji" generiše se par ključeva predefinisane dužine od 1024 bita. Privatni ključ se kreira kao zaštićeni podatak, prilikom ovog procesa od korisnika se zahtjeva da izabere nivo sigurnosti. Potrebno je da korisnik izabere visoki nivo sigurnosti te unese lozinku kojom se kontroliše svaki pristup privatnom ključu. Korisnik se obavještava da *Web* stranica šalje certifikat u njegovo ime što je neophodno potvrditi. Na kraju procesa korisnik se obavještava o tome da je njegov zahtjev proslijeđen odgovarajućoj službi (studentskoj ili kadrovskoj) i daje mu se identifikacijski broj njegovog zahtjeva. Korisnik se upućuje da se lično pojavi o navednoj službi radi pozitivne identifikacije. Na ovaj način je proces kreiranja zahtjeva maksimalno pojednostavljen za korisnika i smanjena je mogućnost greške. Procedure iza *Web* stranice za predavanje zahtjeva se brinu o tome da zahtjev bude

proslijeđen u odgovarajućem formatu koji će omogućiti izdavanje definisanog formata certifikata sa svim utvrđenim parametrima.

A.2.2 Izdavanje certifikata

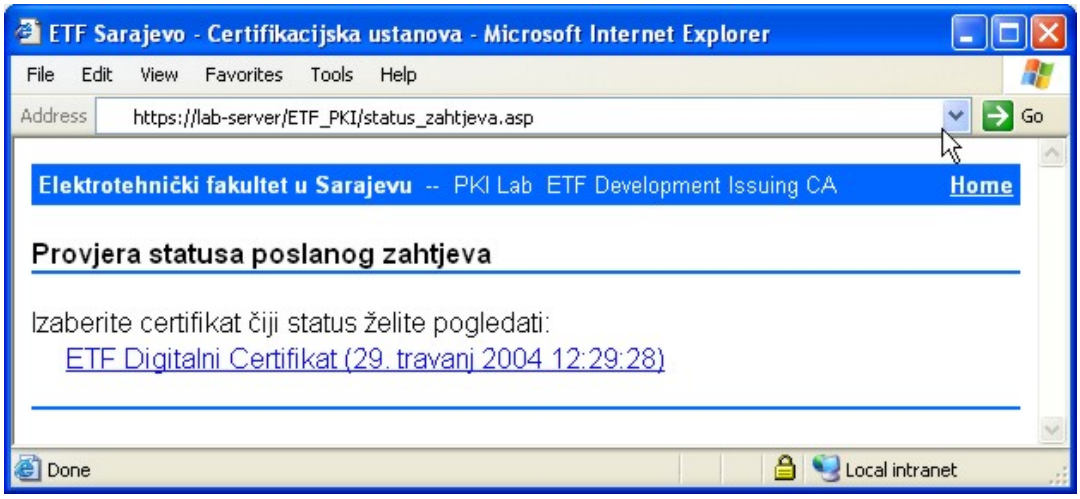
Nakon pojavljivanja korisnika u odgovarajućoj službi i njegove pozitivne identifikacije, ako su zadovoljeni svi ostali uslovi za izdavanje certifikata, certifikat se izdaje korisniku. Ovo se obavlja korištenjem Windows Certification Authority aplikacije koja je instalirana prilikom instalacije Certificate Services. Ova aplikacija omogućava jednostavno izdavanje i opozivanje certifikata. Ovu aplikaciju mogu koristiti korisnici kojima su data odgovarajuća prava. To u zavisnosti od usvojene procedure mogu biti uposlenici službi ili posebni PKI administratori. Na slici je 13 je pokazano izdavanje certifikata koji je tražen u prethodnom koraku.



Slika 13

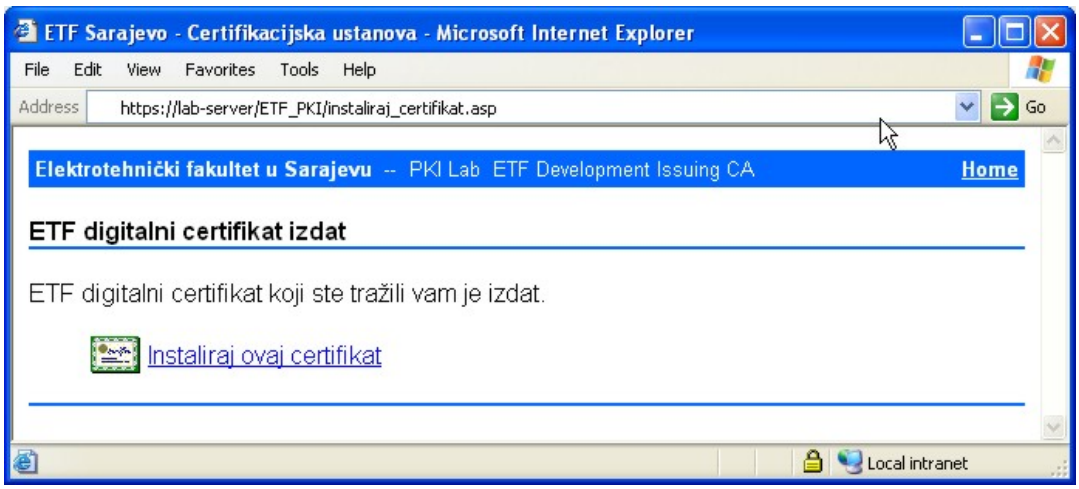
A.2.3 Instalacija certifikata

Kada je certifikat izdat potrebno je da korisnik sa istog računara sa kog je poslao zahtjev i na kom se nalazi privatni ključ ponovo pristupi PKI *Web* stranici sa koje može instalirati certifikat. Slika 14 pokazuje stranicu koja omogućava provjeru statusa zahtjeva.



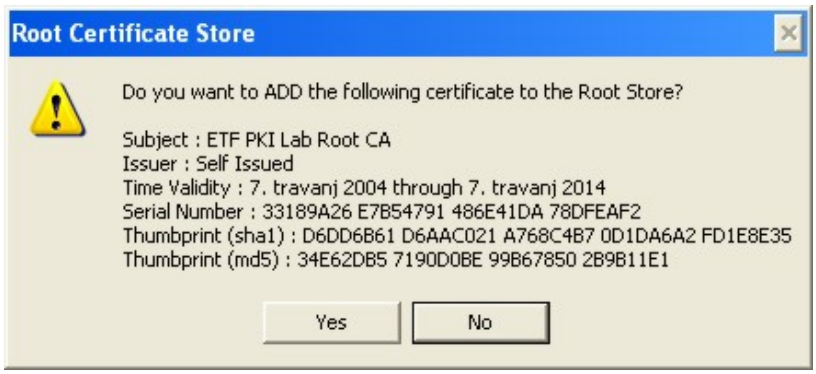
Slika 14

Sa ove stranice se, ako je u prethodnom koraku certifikat izdat, stiže do stranice sa koje se obavlja instalacija certifikata na računar.



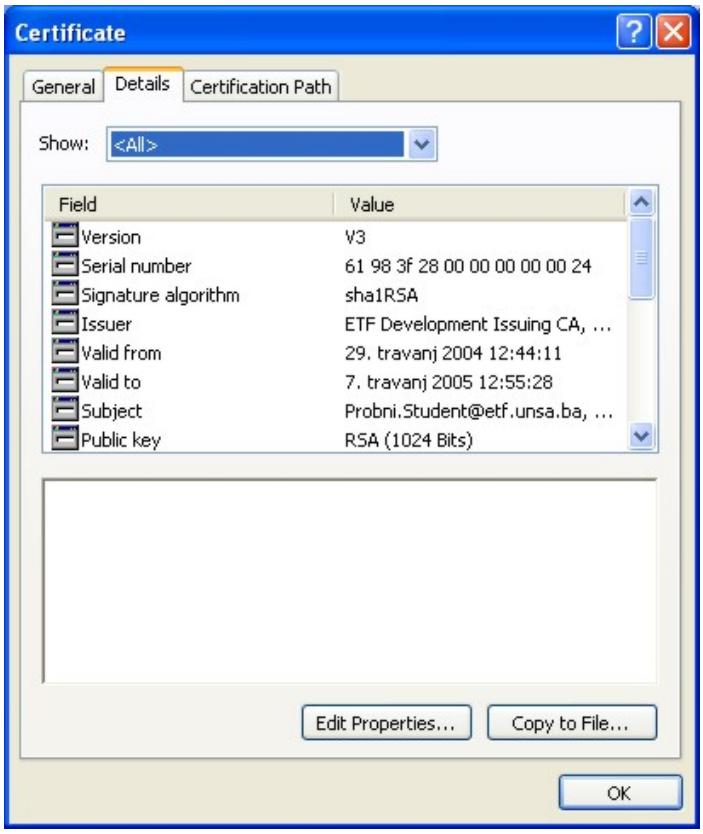
Slika 15

Prilikom instalacije certifikata operativni sistem upozorava korisnika da *Web* stranica instalira certifikat na njegov računar, te traži od njega da to prihvati, kao i da prihvati instalaciju certifikata vrhovne CA koja je izdala certifikat. Instalacija certifikata vrhovne CA visokoškolske ustanove, pored omogućavanja instaliranja korisničkog certifikata, ustanovljava povjerenje u sve certifikate izdate od ove CA i njene izdavačke CA. Na ovaj način se ostvaruje povjerenje u sve certifikate visokoškolske ustanove i olakšava buduće korištenje PKI.



Slika 16

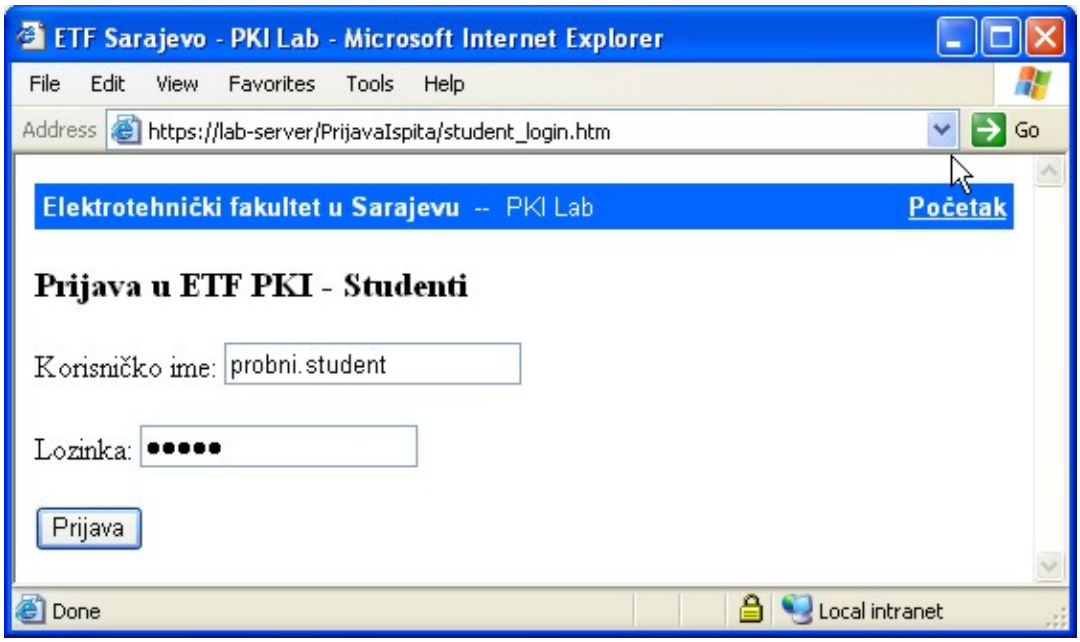
Na ovaj način je završen proces izdavanja i instalacije certifikata koji je sada spreman za korištenje i zaštićen na odgovarajući način. Na slici 17 prikazan je certifikat krajnjeg korisnika.



Slika 17

A.3 Prijavljivanje ispita

Procedura prijavljivanje ispita i objavljivanja njihovih rezultata su relativno slične iz korisničke perspektive mada su namjenjene različitim korisnicima. Korisnik, potpisnik dokumenta prijavljuje se na *Web* server sa svojim korisničkim imenom i lozinkom koristeći HTTPS protokol kojim se osigurava da je server zaista onaj kom se želi pristupiti, šifriranje i integritet podataka koji se razmjenjuju. Na slici18 je data stranica na kojoj se korisnici prijavljuju.

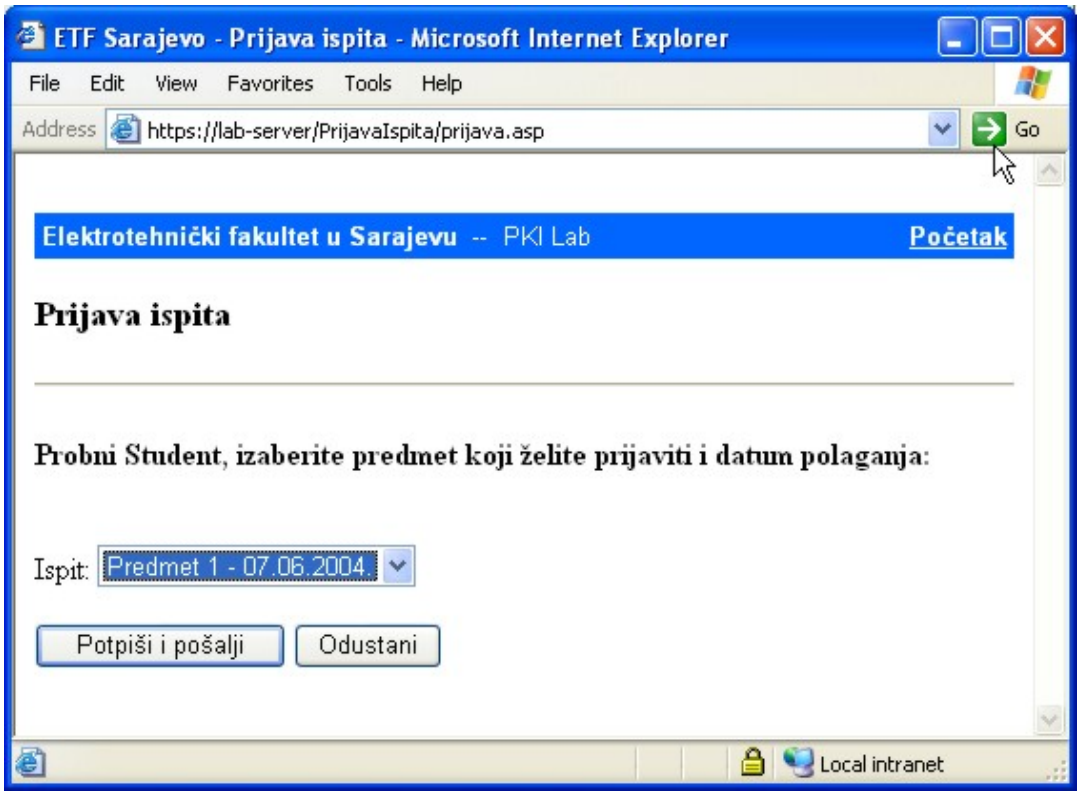


Slika 18

Nakon uspješne prijave na *Web* server student može prijaviti ispit ili pogledati objavljene rezultate ispita. Prilikom prijavljivanja ispita samo je potrebno izabrati predmet i datum ispita iz liste koja je dinamički generisana iz baze podataka o ispitnim rokovima. Svi ostali podaci koji se inače unose u pisane prijave se automatski učitavaju iz baze podataka na osnovu studentske prijave. Stranica putem koje se prijavljuje ispit data je na slici 19.

Nakon izbora predmeta i datuma ispita korisnik potpisuje i šalje svoju prijavu pritiskom na dugme sa odgovarajućim nazivom. Ovim se pokreće procedura digitalnog potpisivanja koja se sastoji od generisanja svih podataka potrebnih za uredno popunjavanje prijave što uključuje i tekući datum i vrijeme koji se zatim *hash*-iraju te šifriraju privatnim ključem korisnika. Kada aplikacija pokuša pristupiti privatnom ključu korisnika javlja se poruka o tome i od korisnika se traži da unese pristupni kod (lozinku) koja će omogućiti digitalno potpisivanje (Slika 20). Podaci, zajedno sa digitalnim poptisom se šalju serveru koji vrši provjeru certifikata, konsultuje listu opozvanih certifikata (CRL) i verificira autentičnost potpisa i integritet podataka. Ako se sve slaže podaci se pohranjuju u bazu podataka i korisnik se obavještava o uspješno prijavljenom

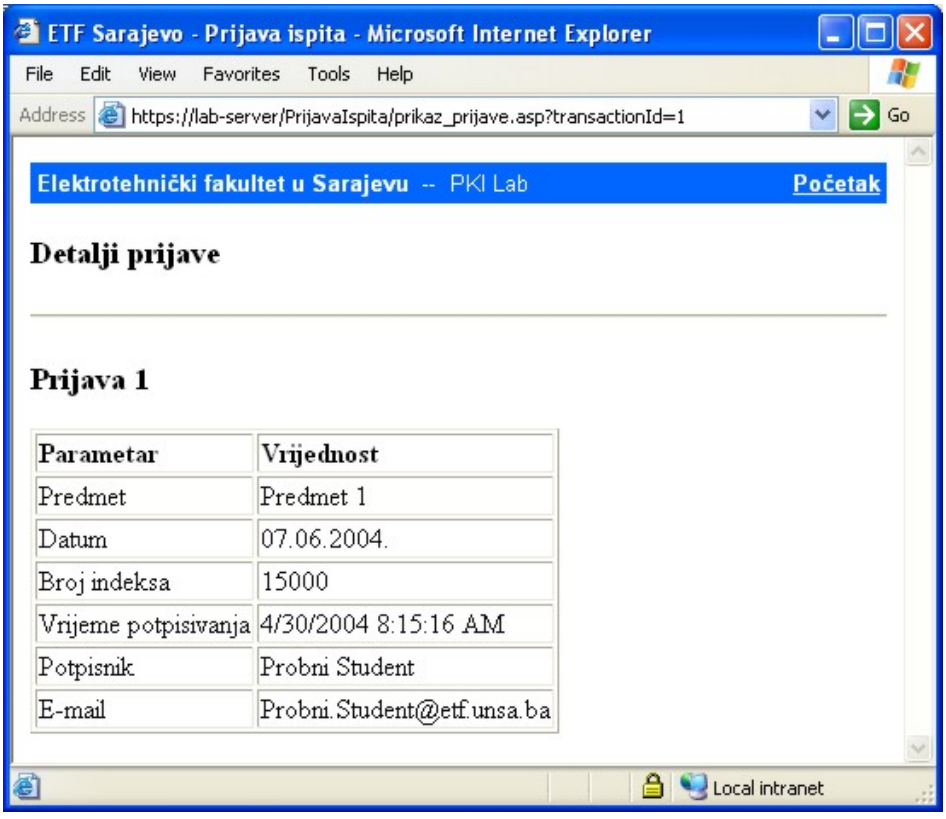
ispitu. U slučaju neslaganja ništa se ne upisuje u bazu i korisnik se obavještava o razlozima neuspjeha prijave.



Slika 19

Na slici 21 dat je jednostavan prikaz osnovnih podataka iz prijave upisanih u bazu. Prilikom pristupa ovim, digitalno potpisanim, podacima od strane drugih korisnika aplikacija koja pruža ovu uslugu će napraviti provjeru stanja certifikata kojim su podaci potpisani. Na ovaj način će korisnici biti upozoreni ako je došlo do opozivanja certifikata od trenutka potpisivanja podataka. Na ovaj način se otklanja i teoretska opasnost da navodni potpisnik dokumenta nije znao da je njegov privatni ključ bio kompromitovan u trenutko kad su podaci potpisani te da je podatke potpisao neko drugi sa tim kompromitovanim ključem. Dostupnost ovih podataka se može podesiti na osnovu politike visokoškolske ustanove o tome ko može vidjeti podatke o prijavama.

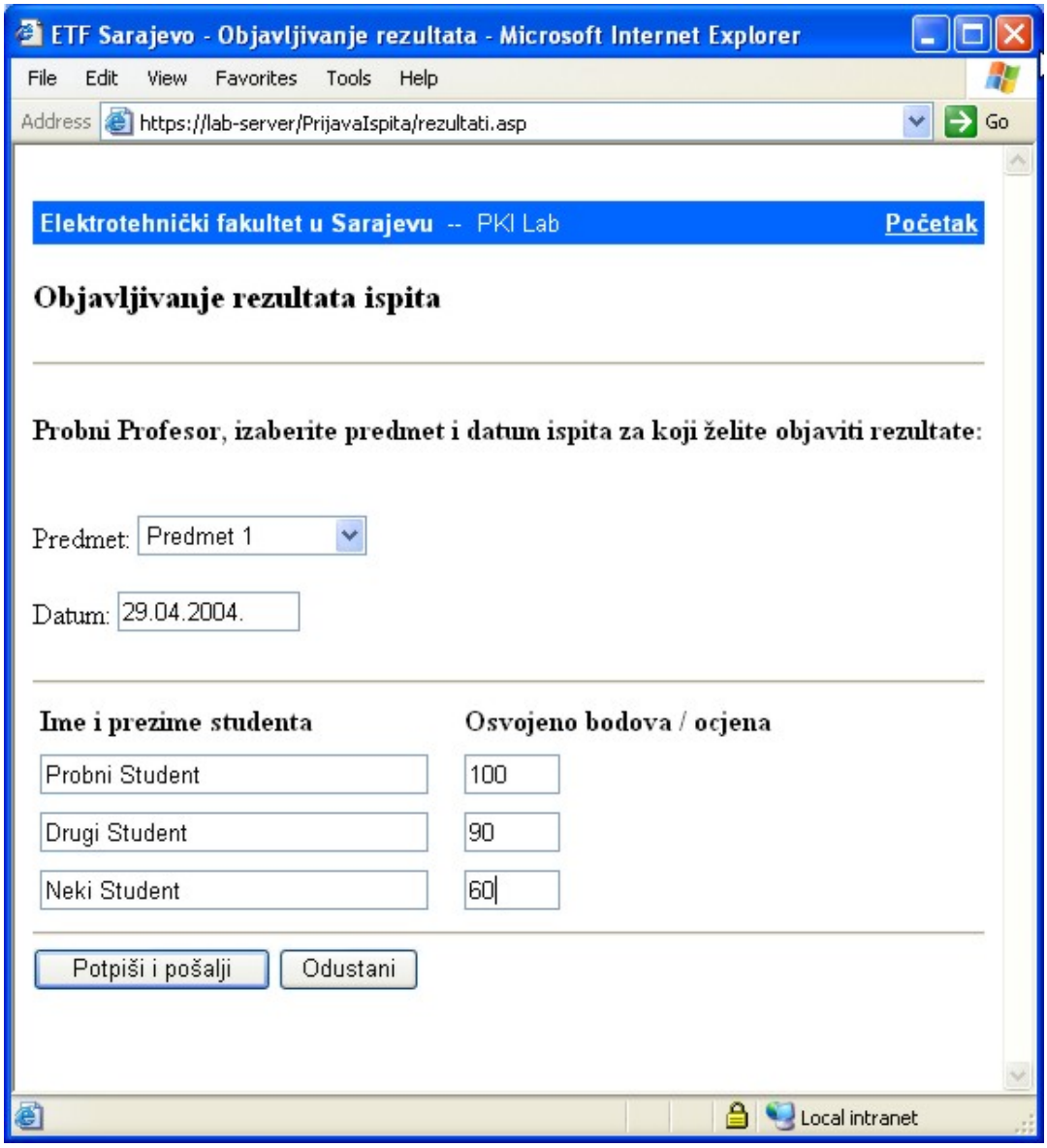
Slika 20



Slika 21

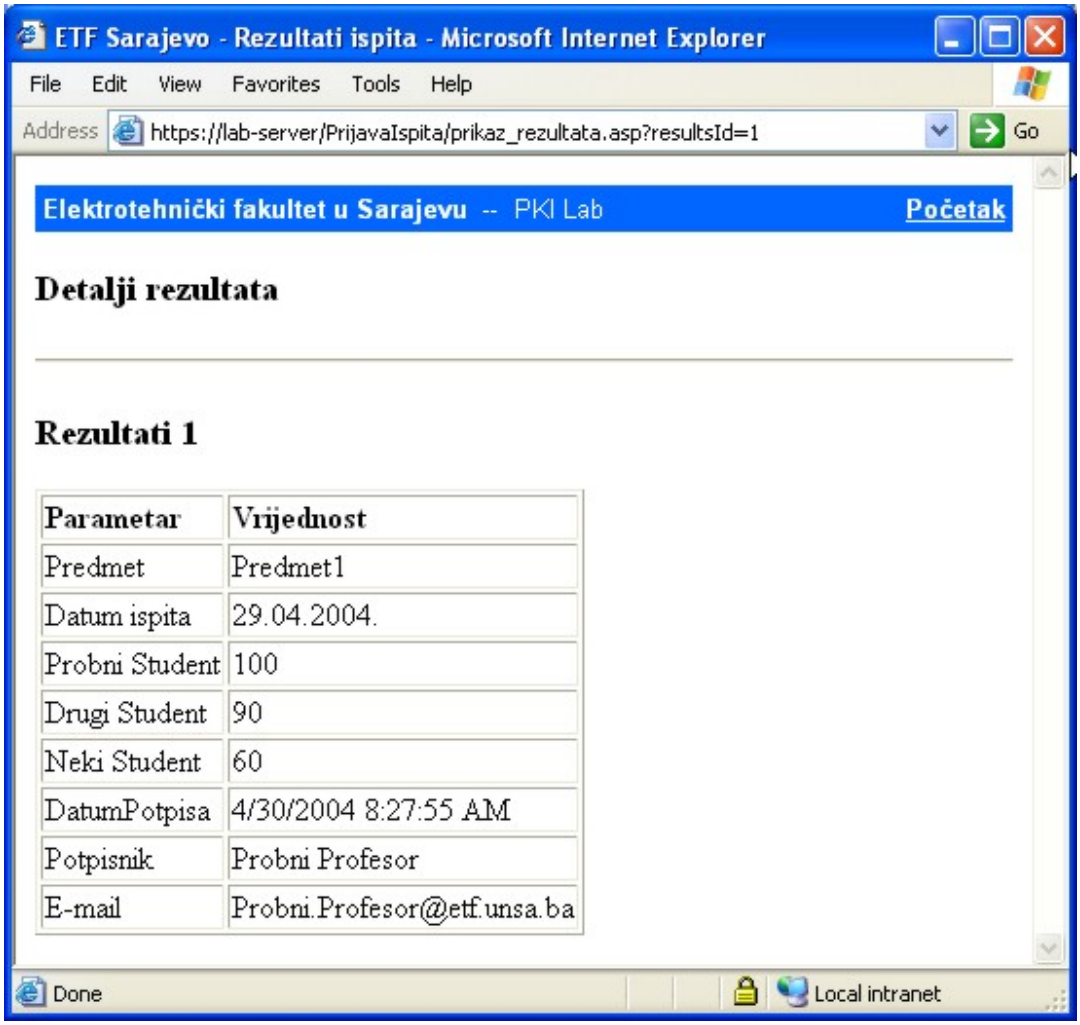
A.4 Objavljivanje rezultata ispita

Objavljivanje rezultata ispita radi se na vrlo sličan način s tim što su podaci koji se unose na *Web* formu i korisnici koji imaju pravo objavljivanja rezultata različiti. Nastavno osoblje se prijavljuje u sistem nakon čega im se pruža mogućnost da objave rezultate ispita i digitalno ih potpišu. Unošenje rezultata i digitalno potpisivanje se vrše preko forme na slici 22.



Slika 22

Pritiskom na dugme "Potpiši i pošalji" odvija se procedura identična onoj opisanoj za potpisivanje i provjeru prijava ispita. Rezultati ispita se upisuju u bazu podataka i dostupni su na uvid i studentima. Dostupnost ovih podataka se može podesiti na osnovu politike visokoškolske ustanove o tome ko može vidjeti rezultate kojih ispita. Na slici 23 dat je jednostavan prikaz rezultata ispita upisanih u bazu.



Slika 23

Prikazana je implementacija funkcija sigurnog prijavljivanja ispita i objavljivanja njihovih rezultata preko *Web*-a. Ostali ciljevi uvođenja PKI odnosili su se na mogućnost digitalnog potpisivanja dokumenata i e-mail poruka kao i njihovo šifriranje. Digitalno potpisivanje dokumenata certifikatima instaliranim na računaru je već integrisano u programe za rad sa dokumentima (MS Office i Acrobat aplikacije). Digitalno potpisivanje i šifriranje e-mail poruka uz korištenje certifikata je sastavni dio e-mail aplikacija (Outlook, Outlook Express, Notes). Način na koji se obavljaju navedene funkcije je detaljno opisan u korisničkoj dokumentaciji navedenih programa i ovdje neće biti posebno predstavljan. Iz ovih razloga nije bio potreban nikakav dodatni rad, osim opisanog izdavanja i instaliranja certifikata, da bi se ispunila ova dva cilja. To je još argument koji ide u prilog teze o jednostavnom PKI.

BIBLIOGRAFIJA

[1] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976, pp. 644-654.

[2] L. Kohnfelder, "Toward a Practical Public Key Cryptosystem," Bachelor's thesis, MIT Department of Electrical Engineering, Maj 1978.

[3] IETF PKIX working group http://www.ietf.org/html.charters/pkix-charter.html

[4] P. Doyle, S. Hanna, "Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage", OASIS Public Key Infrastructure Technical Committee, Avg 2003

[5] Tech Spotlights "PKI Status: 2003" Infineon Technologies AG http://www.silicontrust.com/background/sp_pki2003.asp

[6] Y. Dodis, J. Katz, S. Xu, M. Yung, "Key-Insulated Public Key Cryptosystems", EUROCRYPT 2002, pp. 65-82

[7] S. Al-Riyami, K. Paterson "Certificateless Public Key Cryptography", ASIACRYPT 2003

[8] Centralna Banka Bosne i Hercegovine, "Odluka o reguliranju pravila za utvrđivanje elemenata za vjerodostojnost elektronskog potpisa", Službeni glasnik BiH, broj 10/02, 24.05.2002.

[9] Centralna Banka Bosne i Hercegovine, "Odluka o minimalnim uvjetima koje mora ispunjavati kvalificirano certifikaciono tijelo koje izdaje kvalificirane certifikate za elektronski potpis", Službeni glasnik BiH, broj 10/02, 24.05.2002.

[10] D. Kahn, "The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet", Scribner; Revised edition, 1996

[11] W.F. Friedman, "The Index of Coincidence and Its Applications in Cryptography", Riverbank Publication No. 22, Riverbank Labs, 1920. Reprinted by Aegean Park Press, 1987.

[12] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, v. 28, n. 4, 1949, pp. 656–715.

[13] J.L. Smith, "The Design of Lucifer, A Cryptographic Device for Data Communications," IBM Research Report RC3326, 1971.

[14] Federal Information Processing Standards, "Data Encryption Standard (DES)", Publication 46 – 3, Okt 1999

[15] Federal Information Processing Standards, "Advanced Encryption Standard (AES)", Publication 197, Nov 2001

[16] R.L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public–Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120–126.

[17] S.Singh, "The Code Book: The Secret History of Codes and Code Breaking", Fourth Estate, 1999

[18] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[19] R.A. Rueppel, "Stream Ciphers," Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, pp. 65–134.

[20] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C", John Wiley & Sons, Inc., 1996

[21] EFF, "Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design", O'Reilly & Associates, 1998

[22] T. ElGamal, "A Public–Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology: Proceedings of CRYPTO 84, Springer–Verlag, 1985, pp. 10–18.

[23] V.S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology—CRYPTO '85 Proceedings, Springer–Verlag, 1986, pp. 417–426.

[24] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, v. 48, n. 177, 1987, pp. 203–209.

[25] B.S. Kaliski, "The MD2 Message Digest Algorithm," RFC 1319, Apr 1992.

[26] R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apr 1992.

[27] Federal Information Processing Standards, "Secure Hash Standard", Publication 180-1, Apr 1995.

[28] Federal Information Processing Standards, "Digital Signature Standard," Publication 186, Maj 1994.

[29] C.P. Schnorr, "Efficient Signature Generation for Smart Cards," Advances in Cryptology—CRYPTO '89 Proceedings, Springer–Verlag, 1990, pp. 239–252.

[30] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, Apr 2002.

[31] ITU-T X.509 Recommendation, "Information Technology – Open Systems Interconnection – The Directory Public Key and Attribute

Certificate Frameworks", Jun 2000 (Equivalent to ISO/IEC 9594-8, 2000)

[32] "An Introduction to Cryptography", PGP Corporation, Maj 2003

[33] S. Kiran, P. Lareau, S. Lloyd, "PKI Basics - A Technical Perspective", PKI Forum, Nov 2002

[34] S. Boeyen, T. Howes, P. Richard, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", RFC2587, Jun 1999

[35] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC 2560, Jun 1999.

[36] H. Johner, S. Fujiwara, A. S. Yeung, A. Stephanou, J. Whitmore "Deploying a Public Key Infrastructure", IBM Redbook, Feb 2000

[37] K.E.B. Hickman, "The SSL Protocol", Dec 1995.

[38] T. Dierks, C. Allen, "The TLS Protocol, RFC 2560, Jan 1999.

[39] "Total Cost of Ownership for PKI", Verisign, Feb 2002

[40] P. Gutmann, "PKI: It's Not Dead, Just Resting", IEEE Computer, 35(8):41–49, Avg 2002.

[41] A. Whitten, J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", Carnegie Mellon University, Proceedings of the 8th USENIX Security Symposium, Avg 1999

[42] C. Ellison, "SPKI Requirements", RFC 2692, Sep 1999.

[43] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylönen, "SPKI Certificate Theory", RFC 2693, Sep 1999.

[44] F.Hillier, G.Lieberman, "Operations Research", Holden-Day, Inc., 1974

[45] S.Zimonjić, "Teorija optimalnih rješenja – I dio", Univerzitet u Sarajevu, 1977

[46] "Designing a Public Key Infrastructure", Microsoft, 2003 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dssch_pki_xsdq.asp

[47] J. Sabo, Y. Dzambasow, "PKI Policy White Paper", PKI Forum, March 2001

[48] S. Chokhani at al, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC3647, Nov 2003

[49] "EuroPKI Certificate Policy", EuroPKI, Okt 2000

[50] D. Wasley, "Higher Ed PKI Certificate Policy", I2 Middleware Camp, Feb 2002

[51] "VeriSign Certification Practice Statement", VeriSign, Dec 2003

[52] "HEPKI Model Campus Certificate Policy", Internet2, Middleware, Oct 2002
http://middleware.internet2.edu/certpolicies/

[53] "PKI-Light Project Goals/Assumptions/Questions", HEPKI Lite, Aug 2001
http://middleware.internet2.edu/hepki-tag/pki-lite/pkilite-assumptions.html

[54] "X.509 Certification Authority Policy & Practices", HEPKI Lite, Dec 2001
http://middleware.internet2.edu/hepki-tag/pki-lite/pki-lite-policy-practices-current.html

[55] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", EC, 1999.

[56] S. Santesson, M. Nystrom, T. Polk, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3739, Mar 2004.

[57] L. Bassham, W. Polk, R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation Lists (CRL) Profile", RFC 3279, Apr 2002.

[58] "Factorization of RSA-576", RSA Security, RSA Laboratories, http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa576.html

[59] Franke, J. "RSA576." Privately circulated email reposted to prime numbers Yahoo! Group, Dec 2003

[60] Wikipedia,
http://en.wikipedia.org/wiki/Million_instructions_per_second

[61] S. Gilheany, "Evolution of Intel Microprocessors: 1971 to 2007",
Berghell Associates, LLC
http://www.berghell.com/whitepapers.htm

[62] M. Gardner, "A New Kind of Cipher That Would Take Millions of Years to Break," Scientific American, v. 237, n. 8, Aug 1977, pp. 120–124.

[63] G. Moore, "Cramming more components onto integrated circuits", Electronics, Volume 38, Number 8, Apr 1965

[64] V. Welch et al, "X.509 Proxy Certificates for Dynamic Delegation", 3rd Annual PKI R&D Workshop, 2004

[65] http://www.verisign.com

[66] X. Wang, "Intrusion-Tolerant Password-Enabled PKI", 3rd Annual PKI Research Workshop, pages 44-53, Apr 2003

[67] T. Kwon, “Virtual software tokens - a practical way to secure PKI roaming”, Proceedings of the Infrastructure Security (InfraSec), volume 2437 of Lecture Notes in Computer Science, pages 288-302. Springer-Verlag, 2002.

[68] R. Sandhu, M. Bellare, R. Ganesan. “Password enabled PKI: Virtual smartcards vs. virtual soft tokens”, Proceedings of the 1stAnnual PKI Research Workshop, pages 89-96, Apr 2002.

[69] “Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology”, United States, General Accounting Office report GAO-01-277, Feb 2001.

[70] "SET Secure Electronic Transaction Specification", Version 1.0, MasterCard and Visa, Maj 1997.

[71] R. Rivest, “Can We Eliminate Certificate Revocation Lists?”, Proceedings of Financial Cryptography ’98, Feb 1998, pages 178–183.