SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINAR

Provjera X.509 certifikata u PKI sustavu

Maja Grubić

Voditelj: *Marin Golub*

Zagreb, listopad, 2008

Sadržaj

1. Uvod

Prema statistikama iz lipnja 2008. godine, Internet danas koristi 1.463 miljarda ljudi[1]. To znači da su stotine tisuća ljudi *online* svakog dana. Internet postaje globalna enciklopedija, mjesto gdje se pronalaze informacije o raznoraznim temama, te informacije koje nisu lako dostupne drugdje. Internet je i globalni medij za razmjenu novosti i vijesti. Mnogi posežu za Internetom i zbog komunikacije s rodbinom ili prijateljima s drugog kraja svijeta. Drugi pak koriste Internet kao razonodu u trenucima slobodnog vremena. Posljednjih godina, na Internetu se sve brže razvija i trgovina te svakim danom postaje sve popularnija među širokim brojem korisnika. Ljudi kupuju knjige, rezerviraju hotele u stranom gradu, plaćaju račune, a sve to u samo nekoliko klikova mišem. To podrazumijeva da se svakodnevno izvrše tisuće transakcija u kojima korisnici razmijenjuju svoje privatne i poslovne podatke. Ovakav način poslovanja onemogućio je tradicionalne metode provjere identiteta (kao npr. provjere osobnih iskaznica) i otvorio vrata mnogim problemima. Neki od najčešćih sigurnosnih problema su prisluškivanje podataka, mijenjanje podataka, izmišljanje podataka, prekidanje komunikacijskog kanala, te lažno predstavljanje. Prilikom prisluškivanja podataka napadač presreće vezu između izvorišta i odredišta podataka, te čita podatke koji su namijenjeni nekom drugom. Brojevi kreditnih kartica, kreditnih računa i JMBG mogu biti ukradeni prisluškivanjem podataka. Prilikom mijenjanja podataka napadač presreće podatke u prolasku Napadač mijenja podatke, te takve zamijenjene šalje primaocu. Tako se može npr. promijeniti broj bankovnog računa na koji korisnik šalje novac. Prilikom izmišljanja podataka napadač uspostavlja komunikaciju s odredištem lažno se predstavljajući kao izvorište, te primaocu šalje izmišljene ili stare poruke. Prilikom lažnog predstavljanja napadač se predstavlja kao neki drugi korisnik (primjerice, provalivši na nečiji tuđi račun).

Sustav javnih ključeva (eng. Public Key Infrastructure ili skraćeno PKI) osmišljen je da bi ponudio rješenje ovih problema.

U ovom radu pobliže je opisana infrastruktura javnog ključa i svi njezini sastavni dijelovi, razvoj infrastrukture kroz povijest, te prednosti i mane ovakvog sustava. Prikazan je i objašnjen X.509 digitalni certifikat. Na kraju je opisan praktični dio te funkcije i razredi korišteni u praktičnom dijelu.

2. PKI (Public Key Infrastructure) sustav

PKI ili infrastruktura javnog ključa je sustav koji povezuje korisnike, digitalne certifikate, certifikacijske i registracijske autoritete, te baze važećih i opozvanih certifikata. Certifikacijski autoriteti vrše provjeru identiteta svih strana uključenih u internetsku transakciju uporabom para ključeva. Par ključeva sačinjava javni i tajni/privatni ključ. Javni ključ je dostupan svima i koristi se za kriptiranje poruka, dok je privatni ključ poznat samo vlasniku i koristi se za dekriptiranje. Svaki korisnik ima svoj par ključeva. Identitet korisnika mora biti jedinstven unutar certifikacijskog centra. Povezivanje korisnika s njegovim identitetom ostvaruje se kroz proces registracije i izdavanja certfikata, koji, ovisno o razini zahtijevane sigurnosti može biti obavljen samo softwareom unutar certifikacijskog centra ili mora biti nadgledan od strane čovjeka. PKI je sustav koji omogućuje autentifikaciju, povjerljivost i integritet podataka, neporecivost, te upravljanje ključevima, odnosno certifikatima.

2.1 Struktura PKI sustava

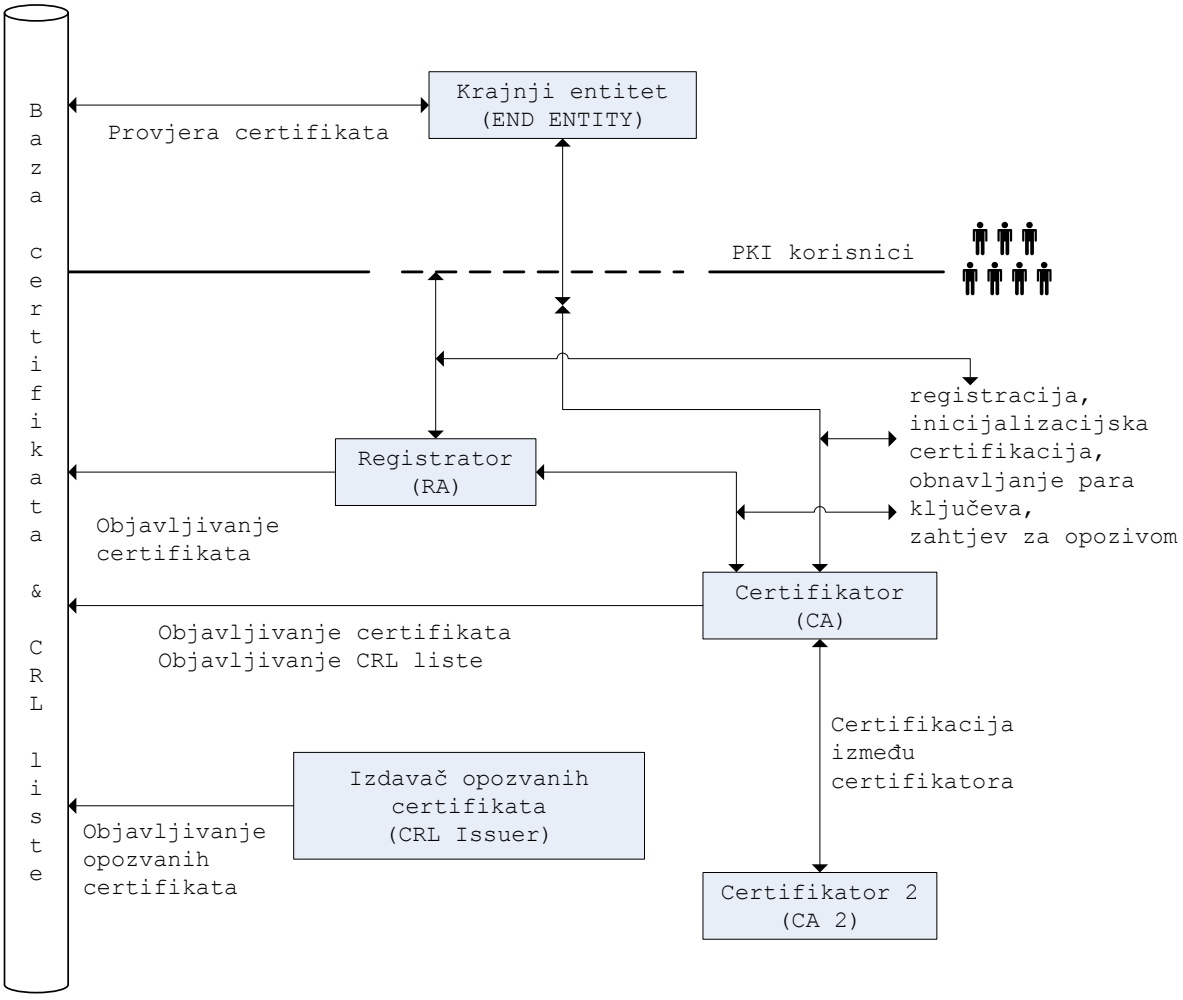
PKI se sastoji od više međusobno povezanih objekata, aplikacija i servisa:

- alata za upravljanje i nadgledanje sustava
- registracijskog centra ili registratora (*Registration Authority* ili skraćeno RA) koji obavlja registraciju korisnika
- certifikacijskog centra (*Certification Authority* ili skraćeno CA) koji se brine za izdavanje i valjanost certifikata
- baze izdanih certifikata (najčešće se koristi LDAP imenički servis) i liste opozvanih certifikat (*Certification Revocation List* ili skraćeno CRL)
- izdavača opozvanih certifikata
- korisničkog certifikata
- korisničkih aplikacija, servera itd., koji koriste PKI autorizaciju.

PKI autorizaciju koriste subjekti certifikata (ponekad se zovu i krajnji korisnici), koji ne moraju biti fizičke ili pravne osobe već i uređaji kao što su serveri i routeri, zatim programi i procesi, odnosno sve što može biti identificirano imenom na certifikatu. Certifikacijski centar (CA) je ustanova koja potpisuje i izdaje certifikate. Osnovne operacije certifikacijskog centra su izdavanje certifikata, njihovo obnavljanje i po potrebi njihov opoziv. CA svojim potpisom jamči ispravnost podataka u certifikatu. CA izravno ili preko registracijskog centra (RA) registrira krajnje entitete ili korisnike i verificira njihov identitet na odgovarajući način. Ponekad obavlja i funkciju sigurnog pohranjivanja ključeva. On je izvor povjerenja u PKI, a povjerenje je osnova na kojoj se zasniva PKI. Registracijski centar (RA) je opcionalna komponenta PKI sustava, a može biti i dio certifikacijskog centra. Njegova uloga je registriranje korisnika PKI sustava. Osim ove uloge, RA može provjeravati posjeduje li korisnik privatni ključ koji odgovara javnom ključu koji će se nalaziti na certifikatu, ili može sam generirati par ključeva. On može biti i posrednik između korisnika certifikacijskog centra prilikom informiranja o kompromitiranju privatnog ključa. Sve ove funkcije su obavezni dio PKI sustava, te ako ih ne obavlja RA mora ih obavljati CA. RA je također i korisnik PKI

sustava te ima svoj javni ključ i certifikat. RA ne smije obavljati funkcije izdavanja i opoziva certifikata. Baza važećih certifikata je sustav ili skup distribuiranih sustava koje pohranjuju certifikate i listu opozvanih certifikata, dostupnih svim unutarnjim ali i vanjskim korisnicima PKI sustava koji koriste certifikate za identifikaciju. Izdavač opozvanih certifikata je komponenta PKI sustava koja izdaje listu opozvanih certifikata. Certifikati se izdaju s određenim periodom valjanosti. Postoji više razloga zašto certifikati mogu postati nevažeći i prije isteka tog perioda, a jedan od njih je kompromitiranje privatnog ključa. Svaki opozvani certifikat identificiran je svojim serijskim brojem u listi opozvanih certifikata. Lista opozvanih certifikata je javno dostupna svima.

Na prikazani su osnovni dijelovi PKI sustava.



Slika 2-1 Osnovni dijelovi PKI sustava

U PKI sustavu povjerljivost podataka se osigurava enkripcijom poruka odnosno korištenjem tajnog (*private key*) i javnog (*public key*) ključa u asocijaciji s kompleksnim matematičkim algoritmom (tzv. asimetrična enkripcija). Svaka osoba u PKI sustavu ima vlastiti javni i tajni ključ, nadopunjen certifikatom. Osnovni princip sustava je sigurno pohranjivanje tajnog ključa koji mora biti dostupan i poznat samo korisniku. Korisnički certifikat, u kojem se nalazi javni ključ, je dostupan svima i najčešće se pohranjuje pomoću LDAP imeničkog servisa. Korištenjem kombinacije tajnog i javnog ključa prilikom slanja poruke, sadržaj poruke se kriptira čime poruka postaje nečitljiva. Primjenom pripadajućeg tajnog ključa, koji svaka osoba u PKI sustavu čuva za sebe, poruka se dekriptira te nanovo postaje čitljiva.

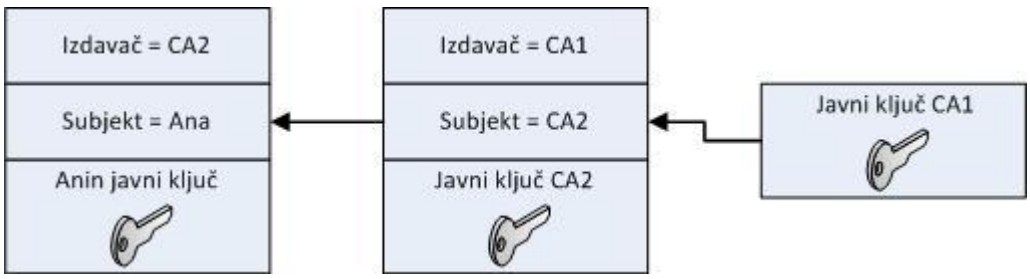
Dodatna sigurnost se postiže upotrebom višenamjenske pametne kartice (*smartcard*) za pohranu korisničkih ključeva i certifikata.

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

Digitalni potpis (*digital ID*) je dodatak koji se dodaje digitalnom dokumentu i služi kao autentifikacija osobe ili računala koje koristi neku uslugu, aplikaciju ili komunicira s drugim korisnicima putem Interneta ili drugačije. Sam certifikat u sebi sadrži korisnički javni ključ koji, korištenje HASH algoritma, mora biti potpisan, odnosno odobren od organizacije koja garantira da je certifikat izdan po pravilima.

Ispravnost certifikata se garantira certifikatom višeg nivoa hijerarhije, tzv. *root certifikatom* odnosno certifikatom potpisanim od nekog *sub CA* operatera koji je potpisan od *root CA*. Često korisnik nema listu certifikata od korijenskog CA. Ako korisnik nema ispravnu kopiju javnog ključa od CA koji je potpisao korisnikov certifikat, zahtijeva se još jedan certifikat od CA koji je potpisao njegov certifikat. Ovaj pristup se primijenjuje rekurzivno, sve dok se ne izgradi lanac certifikata (engl. *certification path*) i ne otkrije se „sidro“ (*anchor*), tj. CA najviše hijerarhije (*end-entity*). Taj CA je obično specificiran certifikatom koji je izdao CA kojemu korisnik direktno vjeruje. U praksi, lanac certifikata je uređena lista certifikata, izgrađena od jednog certifikata kojeg je izdao CA najviše hijerarhije, te nula ili više dodatnih certifikata. Lista certifikata obično je kodirana jednim ili više načinom kodiranja, čime se omogućava siguran prijenos liste kroz mrežu i između različitih operacijskih sustava.

Slika 2-2 Lista certifikataprikazuje listu certifikata od onog najviše hijerarhije (CA1) do korisnikovog certifikata(Alice). Lista certifikata uspostavlja povjerenje u Anin javni ključ preko posredničkog CA, CA2.



Slika 2-2 Lista certifikata

Lista certifikata mora proći provjeru prije nego li se može osloniti na korisnikov javni ključ. Provjera se sastoji od raznih provjera nad certifikatima sadržanima u listi certifikata, kao npr.

provjera potpisa i provjera da pojedini certifikat nije opozvan. Sustavi koji koriste javne ključeve moraju omogućiti izgradnju ili otkrivanje liste certifikata. RFC 2587 definira LDAP (*Lightweight Directory Access Protocol*) koji omogućava otkrivanje liste X.509 certifikatata.

2.2 Primjer korištenja PKI sustava za autentifikaciju korisnika

Protokol autentifikacije sudionika *A* se sastoji od šest koraka. Protokol opisan u idućih šest točaka pretpostavlja da su oba sudionika – *A* i *B* prijavljena u istom certifikacijskom centru.

1. Sudionik *A* šalje u razgovijetnom obliku svoj identifikator sudioniku *B* u poruci

   $$M_1 = (ID_A).$$

2. Po primitku M_1 sudionik *B* generira slučajni broj *N* i šalje u razgovijetnom obliku sudioniku *A* poruku

   $$M_2 = (N).$$

3. Po primitku M_2 sudionik *A* kriptira svojim privatnim ključem *N* i šalje poruku

   $$M_3 = E\ (N, K_{DA}).$$

4. Sudionik *B* po primitku M_3 šalje certifikacijskom centru *C* u razgovijetnom obliku poruku

   $$M_4 = (ID_A, R_B),$$

   gdje je R_B kod kojim sudionik *B* zahtijeva od CA certifikat sudionika s identifikatorom ID_A.

5. Po primitku M_4 poslužitelj certifikacijskog centra *C*:

   - iz svoje tablice na temelju ID_A pročita CER_A^C;
   - s pomoću svojeg privatnog ključa K_{DC} kriptira CER_A^C i šalje poruku

     $$M_5 = E\ (CER_A^C, K_{DC}).$$

6. Po primitku M_5 sudionik *B*:

   - javnim ključem poslužitelja dekritpira M5 i dobiva

     $$CER_A^C = D\ (E\ (CER_A^C, K_{DC}), K_{EC});$$

   - iz CER_A^C saznaje

     $$ID_A, K_{EA} \text{ i } E\ (H\ (ID_A, K_{EA}), K_{DC}));$$

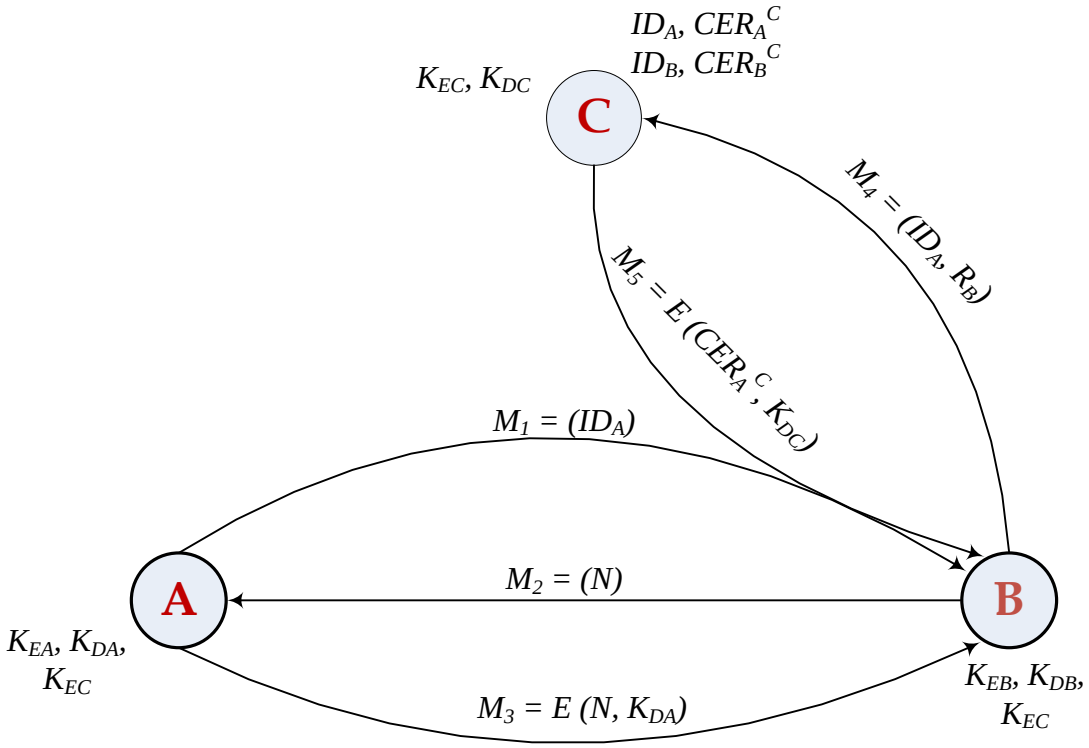
   - izračunava $H\ (ID_A, K_{EA})$ i dobiveni rezultat uspoređuje s dekriptiranom vrijednošću $D\ (E\ (H\ (ID_A, K_{EA}), K_{DC})), K_{EC})$ čime provjerava dobiveni K_{EA}, čime je ustvari proveo operaciju utvrđivanja ključa sudionika A pomoću ključa certifikacijskog centra C;

   - s dobivenim K_{EA} dekriptira raniju poruku M_3 i dobiva

     $$N = D\ (E\ (N, K_{DA}), K_{EA});$$

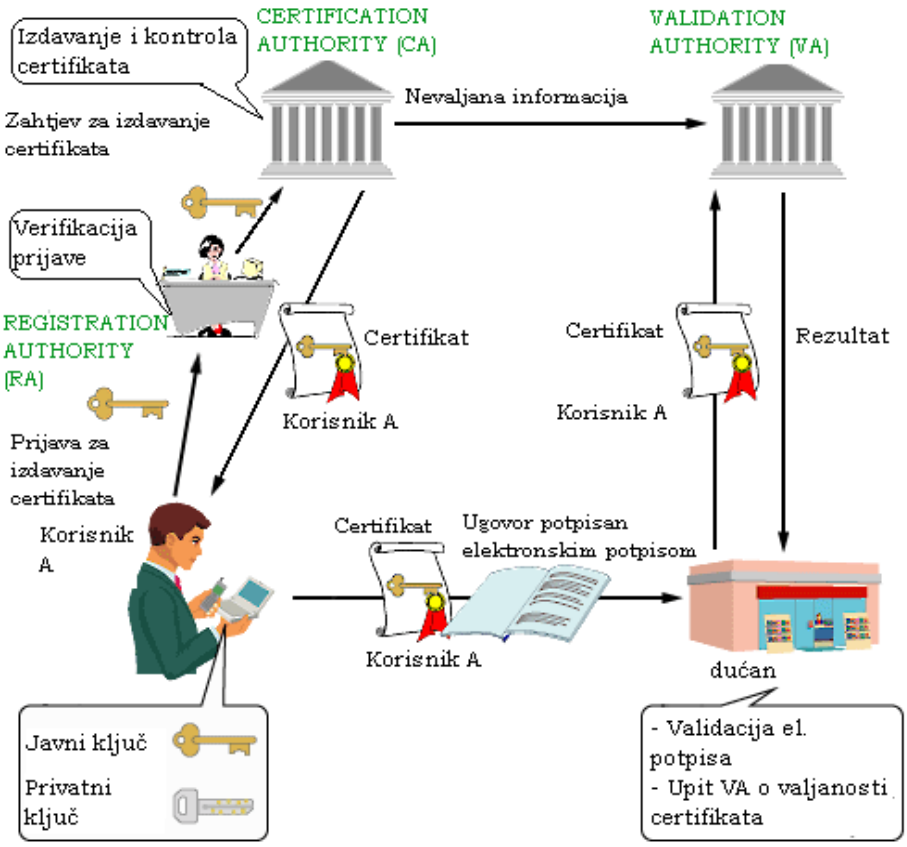
   - dobiveni *N* uspoređuje s originalom, čime prihvaća ili odbacuje sudionika *A*

Opisani protokol prikazan je slikom



Slika 2-3 Postupak jednostrane autentifikacije uz pomoć certifikata

Slika 2-4 prikazuje primjer korištenja PKI sustava prilikom elektronske kupovine.



Slika 2-4 Primjer korištenja PKI sustava

2.3 Povijesni razvoj PKI sustava

1976. Whitfield Diffie i Martin Hellman izdaju članak „New Directions in Cryprography“. U svom su članku predstavili, u tom trenutku revolucionarnu, metodu asimetrične kriptografije. U konceptu asimetričnh kriptografskih algoritama postoje dva ključa, za razliku od simetričnih u kojima postoji samo jedan. Algoritam DES je bio standard u to doba i osnovni algoritam temeljen na simetričnoj kriptografiji. Glavni problem simetrične kriptografije bio je sigurna razmjena tajnog ključa preko nesigurnog kanala. Diffie i Hellman su predložili da vrijednosti dvaju ključa budu povezani nekom matematičkom funkcijom, sporom za izračunavanje, i da se jedan vrijednost koristi za kriptiranje, a druga za dekriptiranje poruke. Budući da bi veza između dvije vrijednosti ključa bila netrivijalna za izračunati, jedan ključ bi bio javan, bez gubitka sigurnosti. Iako autori u tom trenutku nisu imali ideju praktične realizacije kriptografije javnim ključem, ona je pobudila prilično veliko zanimanje i intenzivirala aktivnost kriptografske zajednice.

Autori predlažu i stvaranje bijelih stranica javnog ključa (*Public Key White Pages*), tako da svatko može doći do javnog ključa pojedine osobe. Jednim potezom, izumili su kriptografiju temeljenu na javnom ključu i PKI.

Kriptografija javnog ključa oslanja se koncept da privatni ključ ostaje tajan. 1978. student Kohnfelder objavljuje ideju o offline certifikacijskom centru (CA) koji bi povezivao identitet i javni ključ pojedinca potpisujuću certifikat svojim privatnim ključem. Centar daje svoje povjerenje, preko svog potpisa kombinaciji identita i pripadnog javnog ključa. Online server može sada izdavati certifikate, i svatko može dohvatiti certifikate i provjeriti njihovu autentičnost koristeći javni ključ CA.

Da je povijest bila malo drugačija, imali bismo danas pravi PKI. No dvije stvari su se umiješale. Prva je da je RSA dobio patente na prvoj radnoj implementaciji javnog ključa, i tehnologija javnog ključa se počela izbjegavati zbog problema s licencama – sve dok patenti nisu istekli. Phil Zimmerman je kreirao PGP, koji je zaobilazio RSA patente, ali je upotrijebio anarhični pristup distribuciji javnog ključa. Drugi veliki problem je posve nepovezan s prvim – X.500 direktoriji.

X.500 direktoriji osmišljeni su da budu online globalna baza korištena za elektroničku poštu i ostale aplikacije korištene od strane OSI-ja (*Open System Interconnections*) u 1980-ima. X.500 se oslanja na na ASN.1 (*Abstract Syntax Notation One*) za definiciju sadržaja direktorija. ASN.1 je standard i fleksibilna notacija koja opisuje podatkovne strukutre za prikaz, kodiranje, prijenos i dekodiranje podataka, te će o njoj biti govora kasnije. X.509 certifikat je prvi put izdan 3. srpnja 1988. i bio je kreiran za autentifikaciju pristupa X.500 direktorijima. Verzije 1 i 2 X.509 certifikata su ispale iz široke upotrebe jer su im nedostajala ključna polja za upotrebu u Internet aplikacijama. Npr. niti jedna verzija nema polje za korisnikovu e-mail adresu. Struktura imena koju DN upotrebljava nije povezana s imenovanjem kakvo koristimo u stvarnom životu, i stoga je DN velikim dijelom zaslužan zašto PKI nije u širokoj upotrebi danas. Verzija 3 X.509 certifikata uvodi dovoljno fleksibilnosti za širu upotrebu.

2.4 Prednosti i ograničenja PKI sustava

PKI svakako pruža osnovnu sigurnost potrebnu za sigurnu komunikaciju, i to takvu da korisnici, koji se međusobno ne poznaju ili su dosta udaljeni, mogu sigurno komunicirati kroz lanac povjerenja. Povjerenje je građevni blok infrastrukture javnog ključa i ono se ostvaruje osiguravanjem:

- Privatnosti. Ostvaruje se korištenjem kriptiranja. Poruka se pretvara u drugačiji tekst korištenjem algoritama enkripcije i samo osobe s ispravnim ključem za dekriptiranje mogu dobiti izvornu poruku.
- Integriteta. Jamči da je ono što je primatelj primio upravo ono što je pošiljatelj poslao. Nema gubitka informacija.
- Neporecivosti. Osigurava da korisnik ne može negirati da je poslao poruku ili sudjelovao u transakciji.
- Autentikacije. Utvrđuje da je entitet ono što tvrdi da jest. Digitalni certifikat povezuje identitet s jedinstvenim ključem.

PKI sustav nažalost ima i nekoliko mana.

Sve sadžano u poljima X.509 certifikata potpisuje se privatnim ključem certifikacijskog centra. Niti jedan bit unutar certifikata ne može se promijeniti bez da certifikat postane nevažeći. Svaka promjena, kao npr. promjena e-mail adrese ili organizacijske jedinice uzrokuje ne samo izdavanje novog certifikata nego i poništavanje starog.

Drugi veliki problem su liste opozvanih certifikata (CRL). Ideja je poprilično jednostavna – svaki CA sadrži listu opozvanih certifikata koja se može koristiti svaki put kad aplikacija želi koristiti certfikat. Ovo dovodi do novog problema – certifikati se ne mogu više koristiti *offline*, jer se mora koristit *online* pristup najnovijoj listi. CRL sama po sebi može biti dugačka, pa je i sam proces downloadanja liste netrivijalan, i za aplikaciju i za samu mrežu. Kako svaki certifikat sadrži i podatke o točki distribucije liste opozvanih certifikata (Certificate Revocation List Distribution Point), promjena nekog parametra CRL-a, npr. URL-a, uzrokuje poništavanje svih certifikata. CRL ne prate nikakvu paradigmu stvarnog svijeta. Osim sporog downloadanja velike liste opozvanih certifikata, postoji još jedan problem, a to je mehanizam koji se već pokazao neučinkovit. Kada se iz nekog razloga certifikat opoziva, moraju se istovremeno opozvati sve njegove kopije unutar raspodijeljenog sustava. U načelu se to može izvesti kao što se radi s ukradenim kreditnim karticama. Banke su nekoć koristile listu ukradenih ili opozvanih kreditnih kartica, ali su to prestale. Umjesto toga, izdavatelj kartice šalje svim prodajnim mjestima popis opozvanih kartica s tim da se na svakom mjestu prije odobrenja kupovine mora provjeriti je li kartica još važeća. Sličan mehanizam postoji i u PKI-ju, u kojem umjesto downloadanja CRL-a aplikacija koja provodi provjeru certifikata provjerava kod izdavajućeg CA je li certifikat bio opozvan. Online Certificate Status Protocol (OCSP) pokušava se baviti s ovim problemom.

Još jedan problem X.509 certifikata jest da je previše fleksibilan. Većina proizvođača stvara certifikate koju su nekompatibilni sa certifikatima drugih proizvođača. To se događa jer koriste polja kao npr. polje upotrebe ključeva (Key Usage) na razne načine. Želi li se postići interoperabilnost, najbolje je koristiti jedan proizvod na više mjesta. Drugim riječima, nema

prave interoperabilnosti. Neki proizvodi podržavaju unakrsnu certfikaciju. Unakrsna certifikacija dozvoljava različitim CA da izdaju certifikate jedan drugome. Npr. zamislimo dvije tvrtke, svaku sa svojim internim CA koje žele upogoniti PKI komunikaciju između sebe. Unakrsna certifikacija dozvoljava korisnicima unutar svake od te dvije tvrtke da prepoznaju i validiraju certifikate druge tvrtke. Ovo je naravno izvedivo samo ako su polja unutar certifikata kompatibilna između dviju tvrtki. Različite organizacije mogu imati različite načine zapisivanja imena da bi se izbjegle kolizije.

2.5 PKI u Hrvatskoj

FINA je preko Registra digitalnih certifikata jedini pružatelj usluga certificiranja u RH, registrirana kod Ministarstva gospodarstva, rada i poduzetništva, od kojeg je dobila dozvolu za izdavanje kvalificiranih digitalnih certifikata.

FINA izdaje 2 tipa certifikata: autentifikacijski (normalizirani) certifikat, te potpisni (kvalificirani) certifikat. Autentifikacijski osigurava autentičnost, cjelovitost, izvornost i tajnost dokumenta ili elektroničke transakcije, ali ne osigurava neporecivost. Potpisni (kvalificirani) certifikat se koristi za elektroničko potpisivanje dokumenata ili transakcija naprednim elektroničkim potpisom. Jamči autentičnost, cjelovitost i izvornost, priskrbljuje i neporecivost zamjenjujući u cijelosti vlastoručni potpis ili vlastoručni potpis i otisak pečata.

Certifikati, prema namjeni, mogu biti:

1. Osobni (za građane – fizičke osobe)
2. Poslovni (za poslovne subjekte)
3. TDU (za tijela državne uprave)

Certifikati se po razini sigurnosti svrstavaju u 3 kategorije:

1. Standardna

- ova je razina prikladna u okolinama u kojima postoje rizici i posljedice prouzročene kompromitiranjem podataka, koji nemaju veću važnost. To može biti pristup tajnim podacima za koje vjerojatnost zlonamjernog pristupa nije velika. Za ovu se sigurnosnu razinu podrazumjeva da je vjerojatnost da korisnici budu zlonamjerni mala.

2. Srednja

- ova je razina prikladna za okoline u kojima su rizici i posljedice kompromitiranja podataka umjereni. Može se koristiti u transakcijama koje imaju znatnu novčanu vrijednost ili rizik od krivotvorenja ili u onima u koje je uključen pristup tajnim informacijama za koje je vjerojatnost zlonamjernoga pristupa znatna.

3. Visoka

- ova je razina prikladna za uporabu u transakcijama u kojima je ugroženost podataka visoka ili su posljedice propusta u sustavu zaštite velike. To su transakcije vrlo visoke vrijednosti ili s velikim rizikom od krivotvorenja

3. X.509 certifikati

Digitalni certifikat je digitalno potpisani dokument koji povezuje javni ključ s osobom kojoj pripada (vlasnikom javnog ključa). Uveden je iz tog razloga što sudionici u komunikaciji, da bi uopće mogli komunicirati, moraju na neki način doznati ključeve svojih partnera. Osim toga, moraju biti uvjereni da partneri nisu uljezi koji se lažno predstavljaju. Ideju digitalnog certifikata predložio je L. Kohnfelder 1978. godine. Certifikat se digitalno potpisuje da bi se osigurao njegov integritet, koji jamči potpisnik. Norma X.509 određuje format zapisa i semantiku pojedinih polja certifikata. Osim toga navodi numeričke identifikatore pojedinih polja i normira neka proširenja. Također navodi metodu opoziva certifikata, načine provjere i nabraja podržane kriptografske algoritme. Formalni opis certifikata dan je ASN.1 zapisom, a kodiranje se izvodi izdvojenim pravilima.

3.1 Verzije X.509 certifikata

Najstarija verzija, verzija 1, potječe iz 1988. godine, kada je tek definiran X.500 standard. U proširenju 1993. godine, dodana su dva nova polja, rezultirajući formatom verzije 2 (v2). Verzija 2 uvela je koncept jedinstvenih identifikatora subjekta i izdavača da bi se dozvolila mogućnost promjene imena subjekta ili izdavača tijekom vremena. Većina dokumenata predlaže da se imena subjekta i izdavača ne mijenjaju s vremenom, te da se ne koriste jedinstveni identifikatori. Verzija 2 nije u širokoj upotrebi. Najnovija i najčešće upotrebljavana verzija je verzija 3. Ova verzija podržava proširenja. Proširenja su zamišljena tako da svatko može definirati proširenje i uključiti ga u certfikat. Neka danas česta proširenja su upotreba ključa (*KeyUsage*) koja dozvoljava upotrebu u ključa za određene svrhe, npr. samo za potpisivanje dokumenata, alternativno ime (*AlternativeNames*) koje dozvoljava da više identiteta bude povezano s istim javnim kjučem, dodatni podaci o identifikaciji vlasnika certifikata, podaci o atributima ključa, ograničenja u stazi certifikacije, ... Proširenja se mogu označiti kao kritična (*critical*) kako bi se indiciralo da se proširenja moraju provjeriti. Npr. ako certifikats ima upotrebu ključa označenu kao *critical*, a postavljenu na *keyCertSign*, a certifikat se prezentira tijekom SSL komunikacije, certifikat treba odbiti, jer proširenja na certifikatu indiciraju da se privatni ključ smije koristiti samo za potpisivanje certifikata, i ništa drugo.

3.2 Struktura X.509 certifikata verzije 3

Standard X.509 propisuje da svaki certifikat sadrži sljedeće podatke:

Verzija

Označava koja verzija X.509 certifikata se primijenjuje na taj certifikat.

Serijski broj

Pozitivan cijeli broj koji je jedinstven unutar CA. CA koji izdaje certifikat odgovoran je za dodjelu jedinstvenog serijskog broja certifikatu tako da se on može razlikovati od ostalih certifikata koje taj CA izdaje. Ovaj broj se koristi u različite svrhe. Npr. prilikom opoziva certifikata serijski broj se smješta u listu opozvanih certifikata (Certificate Revocation List, CRL).

Identifikator algoritma potpisa

Identificira algoritam koji je korišten od strane CA prilikom izdavanja certifikata za digitalno potpisivanje certifikata.

Izdavač

Označava X.500 ime entiteta koji je potpisao certifikat. Ovo je obično CA. Upotreba certifikata implicira povjerenje u entitet koji je potpisao certifikat.

Razdoblje valjanosti

Svaki certifikat je valjan samo određeno vrijeme. Ovo vrijeme je određeno datumom početka i datumom kraja, a može varirati od samo nekoliko sekundi do gotovo stoljeća. Trajanje valjanosti ovisi o brojnim faktorima, kao npr. snaga privatnog ključa koji se koristi za potpisivanje certifikata ili o iznosu plaćenom za certifikat.

Ime subjekta

Identificira entitet povezan s javnim ključem. Ime koristi X.500 standard, uz namjeru da bude jedinstveno na Internetu. Za kvalificirani certifikat ovo polje mora imati vrijednost prepoznatljivog imena subjekta (*Distinguished Name*, DN), npr.

```
CN = webmail.fer.hr,  OU = CIP, O = FER,  C = HR
```

gdje su oznake redom: CN – Common Name, OU – Organizational Unit, O – Organization, C – Country.

Podaci o javnom ključu subjekta

Sadrži javni ključ imenovanog subjekta, zajedno s identifikatorom kriptografskog algoritma, te parametrima ključa.

Jedinstveni ID izdavača

Ovo polje je propisano u verziji 2 preporuke i opcionalno je. U polju se odreduje niz bitova koji jedinstveno identificiraju X.500 ime izdavača, u slučaju da je jedan X.500 DN kroz vrijeme bio dodijeljen više nego jednom certifikatoru.

Jedinstveni ID subjekta

Polje je propisano u verziji 2 preporuke i opcionalno je. U polju se odreduje niz bitova koji jedinstveno identificiraju subjekt, u slučaju da je jedan X.500 DN kroz vrijeme bio dodijeljen više nego jednom entitetu (npr. zaposlenik napusti poduzeće, a kroz nekoliko mjeseci u poduzeću se zaposli osoba istog imena i prezimena).

Proširenja

Proširenja su propisana u verziji 3. U preporuci se definiraju *standardna proširenja* za neke šire primjenjiva proširenja verzije 2 preporuke. Ali certifikati nisu ograničeni samo na standardna proširenja već svatko može registrirati proširenje kod odgovarajućih ustanova (npr. ISO). Svako proširenje se sastoji od tri polja:

1. *type* – tip,
2. *critcality* – kritičnost i
3. *value* – vrijednost.

Struktura proširenja je prikazana na Slika 3-1.

Slika 3-1 Struktura proširenja verzije 3 X.509 certifikata

Polje *extension type* definira tip podatka u polju *extension value*. Tip može biti tekst, numerička vrijednost, datum, grafika ili neka složena struktura podataka.
Polje *extension criticality* je jednobitna oznaka. Kada je polje označeno kao kritično znači da polje *extension value* sadrži podatak toliko važan da se ne smije zanemariti. Ako se kritično proširenje ne može obraditi, certifikat se mora odbaciti.
Postoji razlika izmedu kritičnog proširenja i nužnog podatka u certifikatu. Određeno proširenje može biti nužno nekoj aplikaciji, ali to ne znači da takvo polje mora biti označeno kao kritično. Kritična polja su namijenjena samo za podatke tolike važnosti da ga moraju razumjeti sve aplikacije, npr. informacije važne za sprečavanje pogrešne uporabe certifikata. Velika većina proširenja je nekritična. Kritična proširenja se trebaju dodavati s oprezom i tek nakon pažljivog razmatranja jer mogu prouzročiti probleme pri korištenju certifikata.
Polje *extension value* sadrži podatke. Tip podataka je definiran u polju *extension type*.
Neka od standardnih proširenja su: informacije o ključu (sadrže informacije o namjeni certifikata i para ključeva), informacije o politici (daju mehanizam koji omogućuje certifikatoru da definira način na koji se određeni certifikat mora koristiti i interpretirati), atributi korisnika i certifikatora (omogućuju dodatne mehanizme kojima se odreduju informacije za identifikaciju korisnika i certifikatora), ograničenja na stazu certifikacije (omogućuju mehanizme kojima certifikator upravlja i ograničava povjerenje "prošireno" na treće osobe, te se primjenjuje kod unakrsne certifikacije).
Dodatak A prikazuje najčešće korištene ekstenzije u verziji 3 X.509 certifikata, uz kratki opis i OID (*Object Identifier*).

Digitalni potpis

Digitalni potpis ostvaruje se tako da se tijelo certifikata sažme odabranom funkcijom sažimanja. Nakon toga, oblikuje se i proslijeđuje algoritmu enkripcije. Tako dobiveni rezultat zapisuje se u ovo polje.

Struktura X.509 certifikata prikazana je na Slika 3-2.

Slika 3-2 Struktura X.509 certifikata

3.3 Podržani kriptografski algoritmi

Norma X.509 propisuje koje je funkcije sažimanja i enkriptiranja moguće upotrebljavati pri stvaranju digitalnih certifikata. SHA-1 je preferirana funkcija izračunavanja sažetka dok su MD5 i MD2 uključene radi očuvanja kompatibilnosti sa starijim normama.

MD2 je funkcija sažimanja koju je razvio Ronald Rivest 1989. godine, specificirana sa RFC 1319. MD2 proizvodi sažetak duljine 128 bita tako što se na

MD5 kao i MD2 proizvodi sažetak duljine 128 bita. Izvorni tekst se dijeli na blokove duljine 512 bitova. Zadnji blok koji ne mora biti dugačak 512 bitova nadopunjuje se na 512 bitova tako da se iza zadnjeg bita teksta dodaje jedna jedinica, nakon koje se upisuje toliko nula

koliko je potrebno da u bloku preostanu 64 bita, a zatim se u preostale bitove upisuje bitovna duljina izvorne poruke. Svaki se blok dijeli na 16 podblokova duljine 32 bita. Svaki podblok sudjeluje u izračunavanju 4 puta, pa se izračunavanje obavlja u 64 koraka podijeljena u 4 kruga.

Funkcija sažimanja SHA-1 proizvodi 160 bitovni sažetak. Izvorni tekst dijeli se na podblokove duljine 512 bita. Zadnji blok teksta nadopunjuje se na 512 bitova na jednaki način kao i kod MD5. Sažetak od 160 bitova sastoji se od 5 nadovezanih 32-bitovnih varijabli, koje se inicijaliziraju na određene početne vrijednosti. SHA-1 postupak ima 4 kruga s 20 koraka, tj. ukupno 80 koraka.

Certifikati mogu biti potpisani bilo kojim enkripcijskim algoritmom javnog ključa. Najčešće su korišteni DSA i RSA.

4. Programsko ostvarenje

U praktičnom dijelu seminarskog rada napravljena je aplikacija za provjeru X.509 certifikata. Implementirana su četiri osnovna koraka u provjere certifikata: provjera ispravnog formata datoteke, provjera vremenske valjanosti certifikata, provjera je li certifikat izdao CA kojem se može vjerovati, te provjera je li certifikat opozvan.

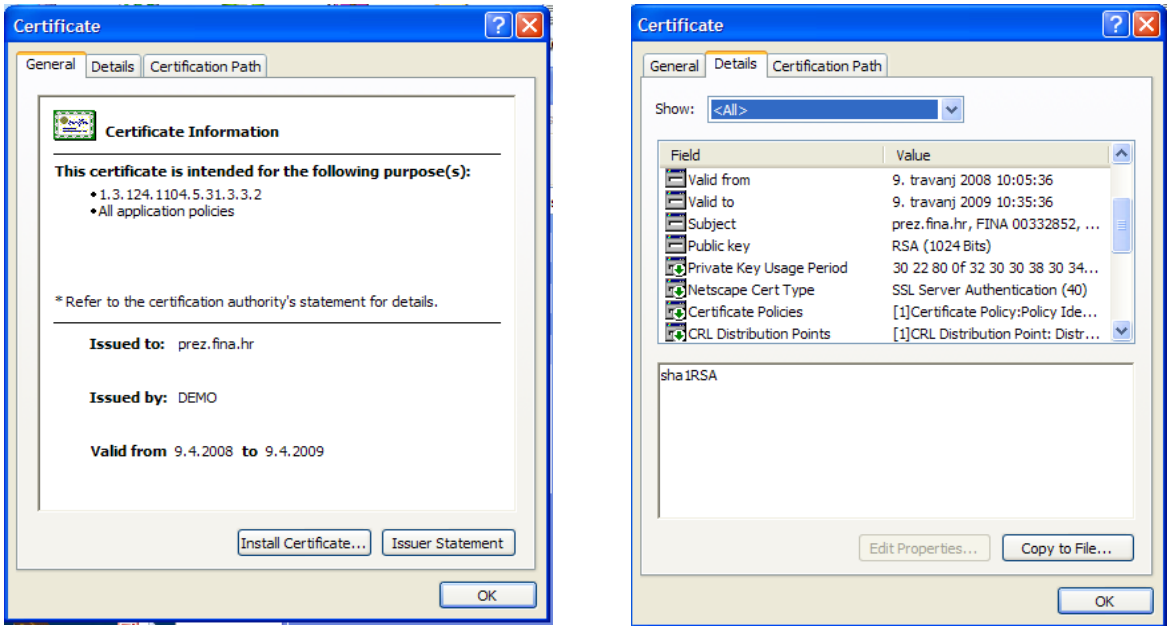
Aplikacija je razvijena u programskog jeziku Java (verzija 6), koristeći ugrađene pakete i razrede za kriptografiju (Java crypto API). Za izradu korisničkog sučelja korišten je Javin SWT skup alata.

Dohvat liste opozvanih certifikata može se napraviti na dva načina: dohvatom liste sa servera ili učitavanjem lokalne kopije. Kako je napomenuto u poglavlju 2.4, PKI bi trebao omogućiti offline provjeru liste opozvanih certifikata, no time se riskira da lokalno spremljena kopija nije najnovija kopija koja postoji. Na korisniku je da odabere koji način želi koristiti. Treba napomenuti da se url na kojem se nalazi lista opozvanih certifikata nalazi zapisan u nekritičnim proširenjima, odnosno certifikat ga ne mora imati zapisanog. U tom slučaju preskače se provjera liste opozvanih certifikata.

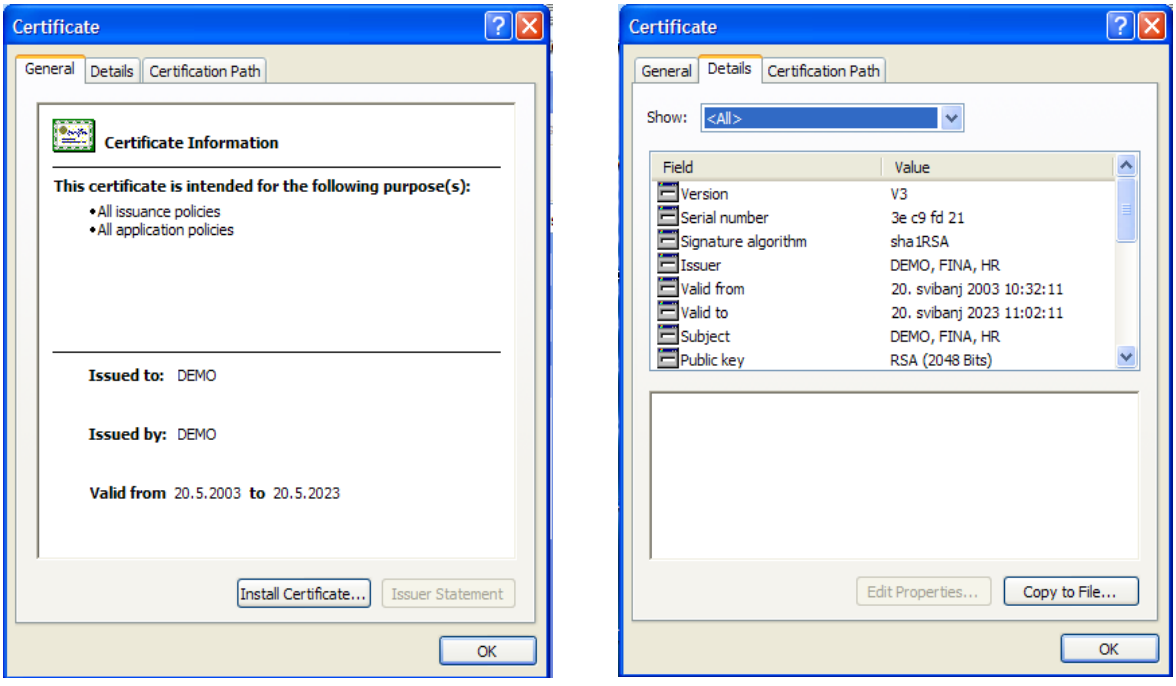
Provjera je li certifikat izdan od strane CA kojem se može vjerovati uvelike je pojednostavljena. Provjerava se postoji li u lokalnom spremniku certifikata korijenski certifikat koji je izdavač traženog certifikata. Ukoliko je certifikat pronađen, generira se lanac certifikata od krajnjeg do korijenskog, te je CA označen kao izdavač kojemu se može vjerovati. Ukoliko nije pronađen takav certifikat, korisniku je dana mogućnost da unese certifikat izdavatelja, te se onda provjerava je li zadani izdavatelj izdao zadani certifikat. U praksi je izrada lanca certifikata od krajnjeg do korijenskog jako složen proces, te kompliciran za implementaciju.

4.1 Korišteni certifikati

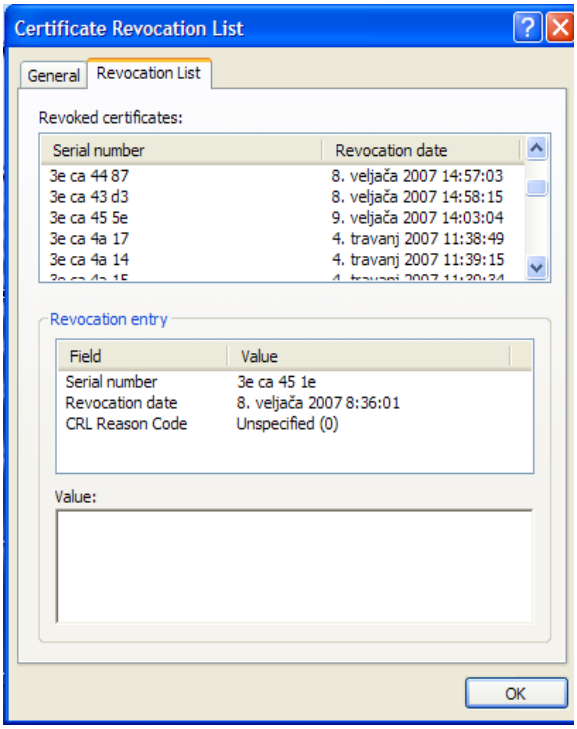
Za potrebe izrade seminara, korišteni su FINA demo certifikati. Fina demo certifikati izdaju se besplatno fizičkim osobama na rok od godinu dana. Certifikati su pogodni za korištenje u ovom seminaru jer imaju ekstenziju u kojoj je zapisan url liste opozvanih certifikata, a sa Fininih web stranica omogućeno je preuzimanje liste opozvanih certifikata, te preuzimanje certifikata koji pripada certifikacijskom centru. Na iduće tri slike prikazani su korišteni demo certifikat, korijenski certifikat demo certifikacijskog centra, te odgovarajuća lista opozvanih certifikata.



Slika 4-1 Prikaz korisničkog demo certifikata



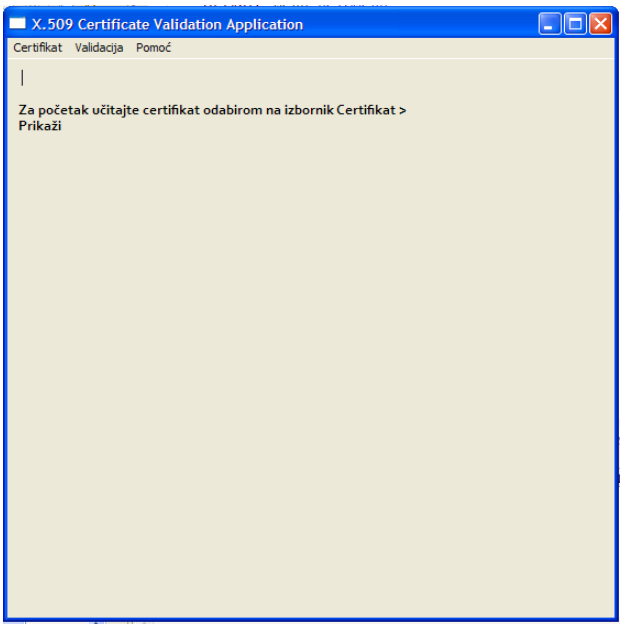
Slika 4-2 Prikaz korijenskog (samopotpisanog) certfikata za Demo CA



Slika 4-3 Prikaz CRL liste za Demo CA

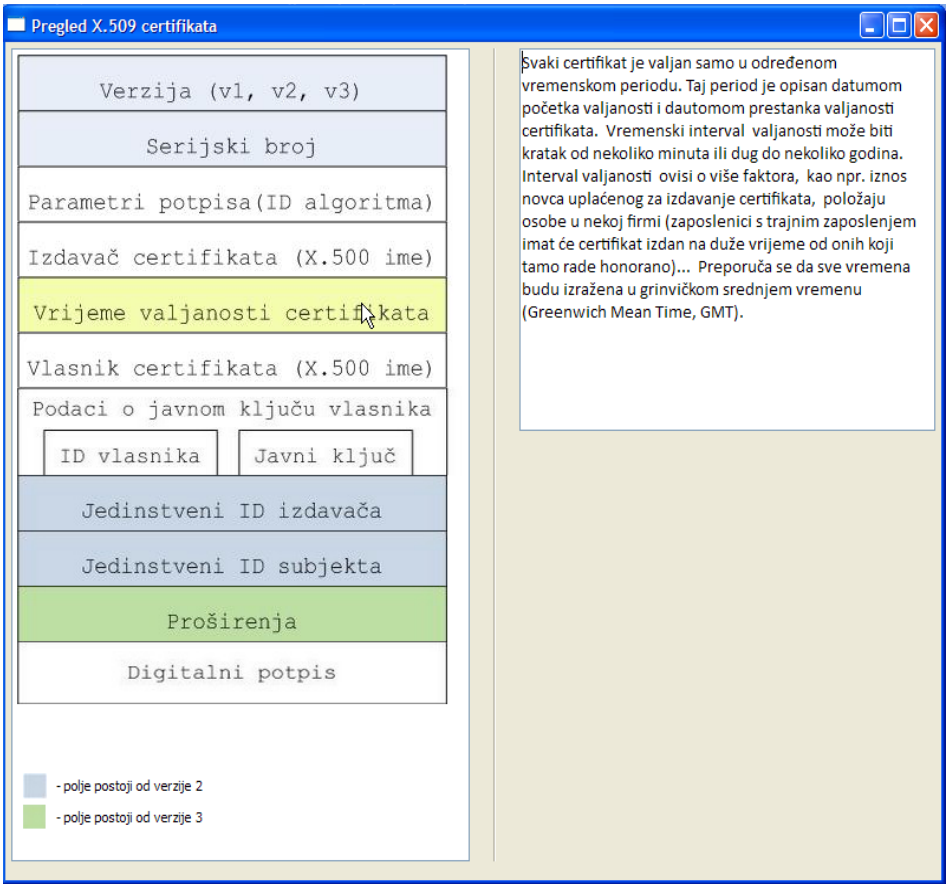
4.2 Primjer korištenja aplikacije

Pokretanjem aplikacije otvara se prozor kao na Slika 4-4 Početni prozor aplikacije.



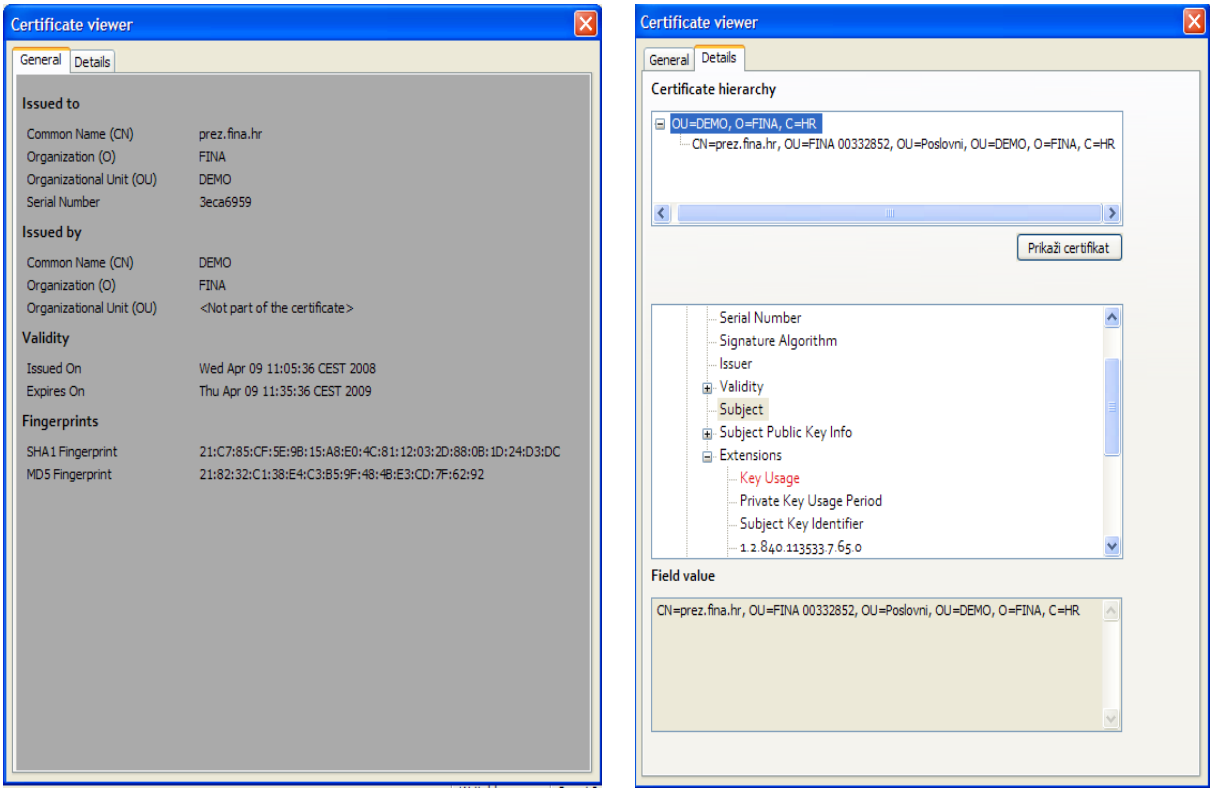
Slika 4-4 Početni prozor aplikacije

Aplikacija sadrži tri izbornika: Certifikat, Validacija, te Pomoć. Izbornik Certifikat sadrži opcije za unos certifikata, spremanje certifikata pod drugim imenom i/ili formatom, te unos certifikata izdavatelja. Izbornik Provjera sadrži opcije za provjeru certifikata, brzu provjeru, te provjeru digitalnog potpisa. Izbornik Pomoć sadrži pregled certifikata kao na Slika 4-5 , uz objašnjenja pojedinih polja, te upute za korištenje aplikacije.



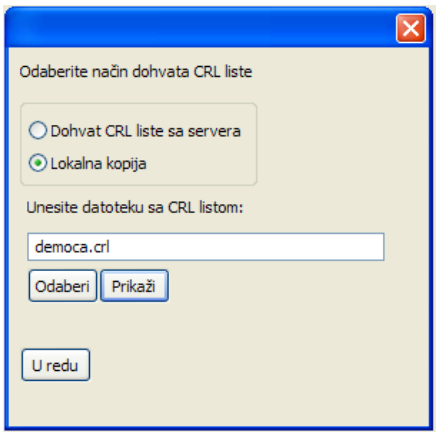
Slika 4-5 Prozor s općenitim podacima o certifikatima

Unosom certifikata otvara se pregled certifikata. Na prvoj kartici prikazani su najvažniji podaci o certifikatu: serijski broj, kome je izdan, tko je izdavatelj, kada je izdan, te kada ističe. Na drugoj kartici prikazana su sva polja certifikata, put do izdavateljevog certifikata, te ekstenzije. Kritične ekstenzije označene su crveno.



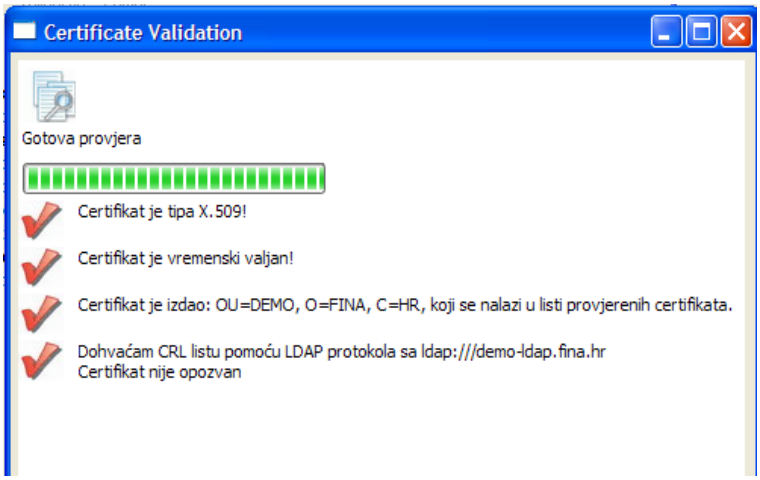
Slika 4-6 Prikaz certifikata

Nakon što je certifikat učitan, korisniku se nude opcije za promjenu certifikata, za spremanje certifikata pod drugačijim imenom, za spremanje certifikata kao .txt datoteke, te opcije za provjeru certifikata. Kao što je već rečeno na početku ovog poglavlja, provjeravaju se četiri stvari: je li zadana datoteka u formatu X.509 certifikata, je li certifikat vremenski valjan, je li ga izdao CA kojemu se može vjerovati, te postoji li certifikat u listi opozvanih certifikata. Lista opozvanih certifikata se provjera samo ako u certifikatu postoji ekstenzija sa OID-ijem 2.5.29.31, tj. ako je u certifikatu zapisan url za dohvat liste opozvanih certifikata. Listu opozvanih certifikata moguće je dohvatiti preko ldap protokola, ili http protokola. Preferirani način dohvata je ldap protokol.



Slika 4-7 Odabir načina dohvata CRL liste

Nakon odabira pokreće se provjera certifikata. Ispisuju se koraci u provjeri certifikata, te konačan rezultat. Ovo je prikazano slikom 4-8.

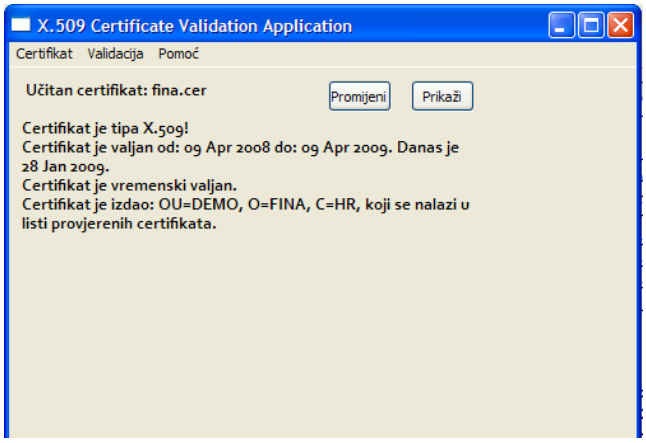


Slika 4-8 Koraci i rezultat provjere

Nakon provjere, i na glavnom prozoru aplikacije ostaje zapisana poruka o rezultatu provjere, kao što je prikazano Slika 4-9.

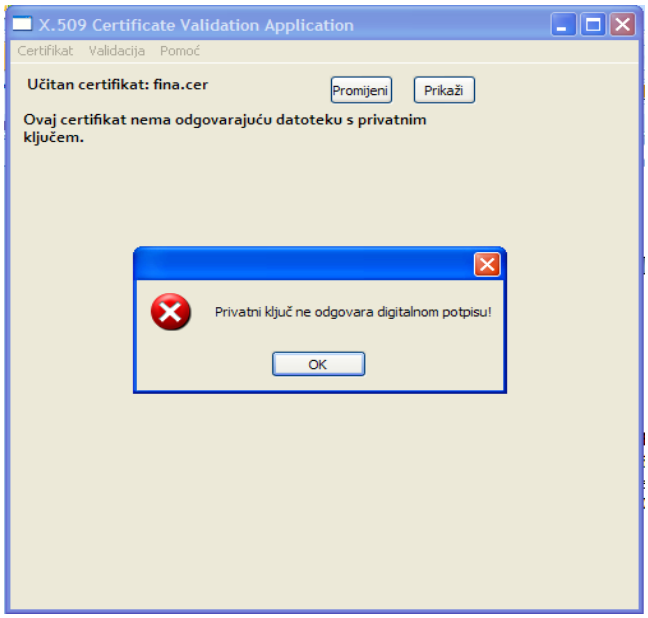
Slika 4-9 Glavni prozor nakon provjere

Korisniku se nudi i opcija brze provjere certifikata, gdje se provjerava samo format datoteke, vremenska valjanost, te izdavač. Nakon brze provjere, rezultat je sličan kao u prethodnom primjeru, samo bez podatka o opozvanosti certifikata. Rezultat je prikazan Slika 4-10.



Slika 4-10 Rezultat brze provjere certifikata

Naposljetku, ukoliko korisnik ima datoteku s privatnim ključem, može provjeriti je li zadani certifikat potpisan s javnim ključem koji odgovara tom privatnom ključu. Odabirom opcije Provjera digitalnog potpisa iz izbornika Provjera, korisnik mora unijeti datoteku s privatnim ključem. Pošto se prilikom izdavanja demo certifikata od F ne dobije datoteka s privatnim ključem, u ovom slučaju će se javiti greška. Ovo je prikazano Slika 4-11.

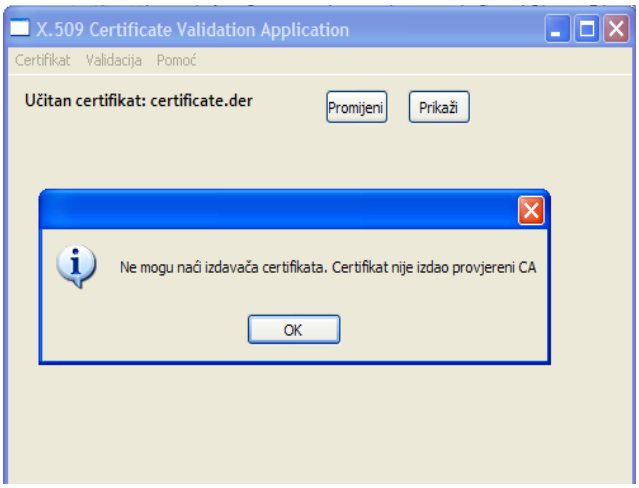


Slika 4-11 Rezultat provjere datoteke s privatnim ključem

Primjer neuspjele provjere

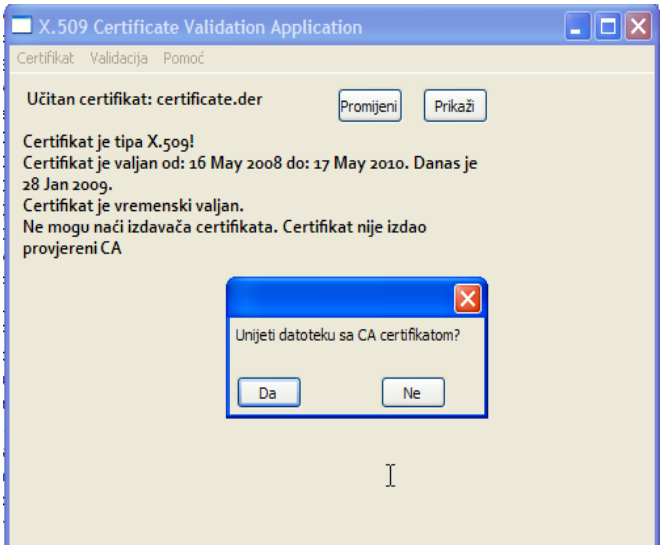
Primjer neuspjele provjere pokazat ćemo na primjeru certifikata koji ima nevaljani certifikat izdavačkog centra, odnosno koji ima certifikat drugog izdavačkog centra.

Nakon učitavanja certifikata pokreće se brza provjera certifikata. Tijekom provjere, korisnika se obavještava da certifikat certifikacijskog centra nije pronađen.



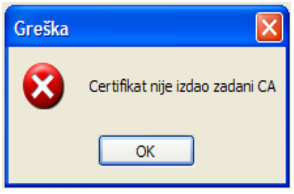
Slika 4-12 Obavijest da za zadani certifikat ne postoji CA certifikat

Korisniku se nudi opcija unosa datoteke sa CA certifikatom, kao što je prikazano slikom 4-13.



Slika 4-13 Mogućnost unosa CA certifikata

Nakon što je certifikat unesen, provjerava se je li zadani CA izdao zadani certifikat. Ako je, dodaje se u listu provjerenih CA certifikata i prilikom iduće provjere, bio bi označen kao valjan. Ukoliko uneseni CA certifikat nije izdao zadani certifikat, javlja se poruka o grešci, kako je to prikazano slikom 4-14.



Slika 4-14 Dojava greške kad uneseni CA certifikat nije izdao zadani korisnički certifikat

Kod samopotpisanih certifikata korisnika se obavještava o tome da je certifikat samopotpisan, te je na korisniku hoće li vjerovati tom izdavaču ili ne.

5. Zaključak

U ovom seminarskom radu cilj je bio razmotriti postupak provjere X.509 certifikata u PKI sustavu. Korisnici certifikata nalaze se u raznim okruženjima, na raznim mrežama i pripadaju različitim certifikacijskim centrima, te je zbog toga provjera certifikata složen postupak. Neki aspekti tog postupka su za potrebe seminarskog rada pojednostavljeni, te napravljeni ponajprije za certifikate u FINA Demo PKI sustava. Aplikacija bi se mogla proširiti i poboljšati tako da se implementira algoritam za pronalaženje staze certifikata od korisničkog do korijenskog. Mogla bi se napraviti još jedna aplikacija koja bi koristila certifikat u određene svrhe (npr. za digitalni potpis e-mailova), te bi se prilikom provjere izbacili svi certifikati koji nisu izdani za tu svrhu.

6. Literatura

[1] World Internet Usage Statistics News and Population Stats, dostupno na Internet adresi ***http://www.internetworldstats.com/stats.htm***

[2] Franjo Rebac: Infrastruktura javnog ključa, seminarski rad, dostupno na Internet adresi ***http://os2.zemris.fer.hr/pki/2005_rebac/index.html***

[3] Leo Budin, Marin Golub: Predavanja iz predmeta Operacijski sustavi 2, Zagreb, 2007.

[4] Sunove stranice o X509 certifikatima, dostupno na Internet adresi ***http://java.sun.com/j2se/1.3/docs/guide/security/cert3.html***

[5] Peter Škoda: Certifikati – X.509, Fakultet elektrotehnike i računarstva u Zagrebu, dostupno na Internet adresi ***http://spvp.zesoi.fer.hr/seminari/2004/certifikati_x_509-pskoda.pdf***

[6] RFC2459 Internet X.509 Public Key Infrastructure Certificate and Internet Protocol***: http://tools.ietf.org/html/rfc2459***

[7] RedHat Manual: ***http://tinyurl.com/b7tsj6***

[8] Jxplorer, open source ldap browser: ***http://www.jxplorer.org/***

[9] FINA DEMO PKI: ***http://demo-pki.fina.hr***

7. Dodatak A: Najčešće korištene ekstenzije verzije 3 X.509 certifikata

1. authorityInfoAccess
    - OID: 1.3.6.1.5.5.7.1.1
    - Kritičnost: nekritična
2. authorityKeyIdentifier
    - OID: 2.5.29.35
    - Kritičnost: nekritična
3. basicConstraints
    - OID: 2.5.29.19
    - Kritičnost: kritična
4. certificatePolicies
    - OID: 2.5.29.32
    - Kritičnost: kritična
5. CRLDistributionPoints
    - OID: 2.5.29.31
    - Kritičnost: nekritična
6. extKeyUsage
    - OID: 2.5.29.37
    - Kritičnost: ako je označena kao kritična, certifikat se smije koristiti samo u naznačene svrhe; ako nije označena kao kritična, polje se može koristiti za identifikaciju ključeva, ali ne ograničava certifikat za korištenje u samo navedene svrhe
7. issuerAltName Extension
    - OID: 2.5.29.18
    - Kritičnost: PKIX preporuča da bude označena kao nekritična
8. keyUsage
    - OID: 2.5.29.15
    - Kritičnost: PKIX prvi dio preporuča da bude označena kao kritična ako se koristi
9. nameConstraints
    - OID: 2.5.29.30
    - Kritičnost: PKIX prvi dio preporuča da bude označena kao kritična
10. OCSPNocheck
    - OID: 1.3.6.1.5.5.7.48.4

- Kritičnost: nekritična

11. policyConstraints
    - OID: 2.5.29.36
    - Kritičnost: može biti označena i kao kritična, i kao nekritična
12. policyMappings
    - OID: 2.5.29.33
    - Kritičnost: nekritična
13. privateKeyUsagePeriod
    - OID: 2.5.29.16
    - Kritičnost: izdavač smije specificirati vrijeme trajanja privatnog ključa dulje nego vrijeme trajanja certifikata; ekstenzija je namijenjena za uporabu sa ključevima digitalnog potpisa; PKIX se protivi korištenju ove ekstenzije
14. subjectAltName
    - OID: 2.5.29.17
    - Kritičnost: ako je polje subjekta u certifikatu prazno, ova ekstenzija mora biti kritična
15. subjectDirectoryAttributes
    - OID: 2.5.29.9
    - Kritičnost: nekritična
16. subjectKeyIdentifier
    - OID: 2.5.29.14
    - Kritičnost: nekritična

8. Sažetak

U današnje vrijeme, vrijeme svakodnevnog i učelastog korištenja Interneta, sigurnost na Internetu postaje sve ugroženija. Jedan od učestalih problema je lažno predstavljanje. PKI sustav sa X.509 certifikatima dizajniran je kao rješenje tog problema. Povezivanje korisnika s njegovim identitetom ostvaruje se kroz proces registracije i izdavanja certfikata. Certifikat se koristi za autentifikaciju na Internetu, npr. prilikom on-line trgovine. Zadatak ovog seminara je bio pokazati i implementirati način provjere X.509 certifikata u stvarnom PKI sustavu, te ukazati na prednosti i mane korištenja ovakvog načina identifikacije.