UDC: 004.738 INFO M: str. 49-57

IZGRADNJA INFRASTRUKTURE JAVNIH KLJUČEVA (PKI)
BUILDING PUBLIC KEY INFRASTRUCTURE (PKI)

Jelena Milojković

REZIME: Uvođenje elektronskog poslovanja u državnu upravu zahteva obezbeđivanje okvira za siguran rad sa informacijama. Ovo podrazumeva da se moraju primeniti sve neophodne mere zaštite u informacionim sistemima eUprave kako bi se na najmanju moguću meru smanjila mogućnost gubitka informacija ili njihovo neovlašćeno menjanje/korišćenje, što bi u određenim slučajevima moglo da izazove nesagledive posledice. Zbog toga je potrebno razviti rešenja i definisati postupke i mere koje će obezbediti informaciono - komunikacionu sigurnost, i stvoriti mehanizme za njihovu primenu. Jedno deo rešenja problema zaštite podataka je primena Infrastrukture javnih ključeva (engl. Public Key Infrastructure - PKI).Ovaj rad se bavi metodologijom izgradnje infrastrukture javnih ključeva (PKI) kroz primer izgradnje PKI u organu državne uprave - Republičkom zavodu za statistiku Srbije.
KLJUČNE REČI: Bezbednost, elektronsko poslovanje, infrastruktura javnih ključeva, PKI, javna uprava, eUprava
ABSTRACT: Introduction of e-business in government necessitates the framework for secure information handling. This means that all necessary information protection measures must be in place in the e-Government systems, so that the possibility of the information loss, or its unauthorized change/use could be minimized, since in some cases this misuse could have enormous consequences. Because of this, it is necessary to develop solutions and define procedures and measures which will secure information communication and will create the mechanisms for their implementation. One part of the information protection solution is the implementation of Public Key Infrastructure. This paper deals with the Public Key Infrastructure construction methodology, using the example of the PKI construction in the part of the Serbian government administration – its Statistical Office.
KEY WORDS: words: security, e-business, public key infrastructure, PKI, public administration, e-government

1. UVOD

Obezbeđivanje informaciono - komunikacion sigurnosti je od ključnog značaja, jer se time stvaraju uslovi da svi subjekti koji koriste servise eUprave steknu poverenje da su transakcije koje obavljaju sa upravom pouzdane, zaštićene i sa zahtevanim stepenom poverljivosti. Mere zaštite informaciono – komunikacionih podataka u javnoj upravi takođe, direktno i indirektno, imaju značajan uticaj i na povećanje elektronske sigurnosti u celom društvu. Sigurnosni mehanizmi takođe moraju da uzmu u obzir Zakon o zaštiti ličnih podataka, i da onemoguće neautorizovano korišćenje ličnih podataka koji su predmet zakonske zaštite.

Infrastruktura javnih ključeva (engl. *Public Key Infrastructure - PKI*) je kompleksan sistem koji se sastoji od kriptografskih tehnologija, protokola, standarda, politika, procedura, servisa i aplikacija. Osnovni koncept na kome se zasniva PKI sistem je asimetrična kriptografija ili kriptografija javnih kriptografskih ključeva (Public Key Cryptography).

PKI sistem predstavlja osnovu za primenu rešenja zaštite elektronskih podataka, kojima se obezbeđuju četiri osnovne funkcije zaštite:

1. **Tajnost** (Confidentiality) - garantuje se da sadržaj poruke može da sazna jedino korisnik kome je poruka namenjena.
1. **Autentifikacija** (Authentication) - verifikuje se identitet korisnika koji komuniciraju preko mreže.
2. **Integritet** (Integrity) - garantuje se da poruka nije promenjena prilikom prenosa.
3. **Neporecivost** (Nonrepudiation) - onemogućava se poricanje izvršene transakcije.

Zaštita tajnosti poruke realizuje se šifrovanjem poruke primenom odgovarajućeg **kriptografskog sistema**, dok se ostale tri funkcije zaštite realizuju **tehnologijom digitalnog potpisa**.

2. INFRASTRUKTURA JAVNOG KLJUČA

Šifrovanje javnim ključem kod asimetričnih kriptosistema podrazumeva da je identitet vlasnika para ključeva nesumnjivo dokazan. **Digitalni sertifikat** (engl. *digital sertificate*), ili samo *sertifikat* je skup podataka koji potpuno identifikuju neki entitet (osobu, ustanovu i sl.). Organizacija ovlašćena za izdavanje sertifikata od poverenja **sertifikaciono telo** (engl. *Certificate Authority, CA*) izdaje sertifikate posle provere identiteta entiteta. CA organizacija je poverljivi posrednik za kriptografiju javnim ključem.

Osnovni zadatak sertifikata je da poveže javni ključ sa identitetom entiteta. Sami sertifikati nisu tajni niti zaštićeni. Oni mogu biti objavljeni na nekoj Web stranici na Internetu. Format sertifikata definisan je standardom X.509. Osnovni podaci koji su navedeni u svakom X.509 sertifikatu su javni ključ vlasnika kome je sertifikat izdat, serijski broj sertifikata, vreme važenje sertifikata, jedinstveno ime vlasnika kome je sertifikat izdat (engl. *user's/server's domain name*), jedinstveno ime izdavača koji je izdao sertifikat (engl. *issuer's domain name*) i digitalni potpis izdavača sertifikata. Uz sertifikat, izdavač vlasniku izdaje i pripadajući privatni-tajni ključ.

Problem koji se nameće je određivanje organizacije ovlašćene za izdavanje sertifikata. Jedna organizacija za ceo svet ne bi bila dobro rešenje. Ona ne bi mogla da izdrži toliko opterećenje a i teško je zamisliti ustanovu koju bi čitav svet

smatrao legitimnom i od poverenja. U nekim zemljama se insistira da CA organizacijom upravlja vlada, dok je u drugima trend upravo suprotan.

Zbog opisanih nedoumica, razvijen je nov način sertifikovanja javnih ključeva [1], tzv. **infrastruktura za sertifikovanje javnih ključeva** (engl. *Public Key Infrastructure, PKI*).

3. PREGLED POSTOJEćEG STANJA U OBLASTI PKI

Od kada je nastao, PKI predstavlja rešenje koje obećava. Međutim broj izgrađenih sistema nije ni blizu onog što se očekivalo pre nekih 10 godina kada su se počela prodavati prva komercijalna rešenja PKI. OASIS PKI tehnički komitet je istraživao razloge relativno sporog rasta broja implementiranih PKI. Njihovi zaključci ukazuju da su glavne smetnje: nedostatak aplikacija koje podržavaju i koriste mogućnosti PKI, veliki troškovi uvođenja PKI i velika složenost PKI rešenja [2].

Primedba na mali broj aplikacija se odnosi na aplikacije posebne namene iz različitih oblasti, dok osnovni skup aplikacija opšte namene kao što su WEB pretraživači i e-mail klijenti standardno podržavaju sertifikate i PKI. Samo korišćenjem savremenih WEB pretraživača i e-mail kilenata koji se isporučuju kao standardni deo svih savremenih operativnih sistema moguće je iskoristiti PKI.

Troškovi uvođenja PKI mogu biti veoma veliki, jedno prosečno PKI rešenje košta par stotina hiljada EUR, dok rešenja za velike organizacije mogu biti i nekoliko miliona EUR. U slučaju angažovanja spoljašnje firme za izgradnju PKI cena po korisniku kreće od 50 EUR naviše [3].

PKI sistemi mogu biti veoma složeni za uvođenje i održavanje. Administrativne procedure registracije i izdavanja sertifikata zahtevaju potvrđivanja identiteta svakog subjekta. Procedure upravljanja sa sertifikatima i ključevima, a pogotovo proveravanje statusa sertifikata preko lista opozvanih sertifikata mogu biti komplikovane i predstavljati veliko opterećenje na računarsku infrastrukturu. U slučajevima kada postoji međusobno sertifikovanje sa CA iz drugih domena utvrđivanje lanca poverenja do CA kojoj korisnik veruje i lociranje listi opozvanih sertifikata može postati komplikovano do neizvodljivosti [4].

Pored ovih organizacionih problema postoji i problem korisnika [5], a tiče se upotrebljivosti sigurnosnih sistema. Savremene aplikacije koje omogućavaju šifrovanje, 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 reši sve probleme sigurnih elektronskih komunikacija i ostvari sve namene kriptografije na globalnom nivou. Ova su očekivanja bila nerealna pa se danas ide u pravcu jednostavnijeg PKI rešenja ograničene namene tj. za zatvorene sisteme. Pod zatvorenim sistemom se podrazumeva organizacija čiji su svi članovi na neki način, nezavisno od PKI, evidentirani u administrativnim službama i čiji se broj menja na relativno predvidiv način.

4. STANJE U DRŽAVNOJ UPRAVI SRBIJE

Jedan od ciljeva razvoja ICT-a u državnoj upravi Srbije je i implementacija infrastrukture javnih ključeva (Public Key Infrastructure PKI) i smart card tehnologija, koja treba da podrži rad većeg broja aplikacija, kao što su: zaštita web transakcija, zaštita e-mail servisa, VPN – virtuelne privatne mreže, bezbedno upravljanje elektronskom dokumentacijom.

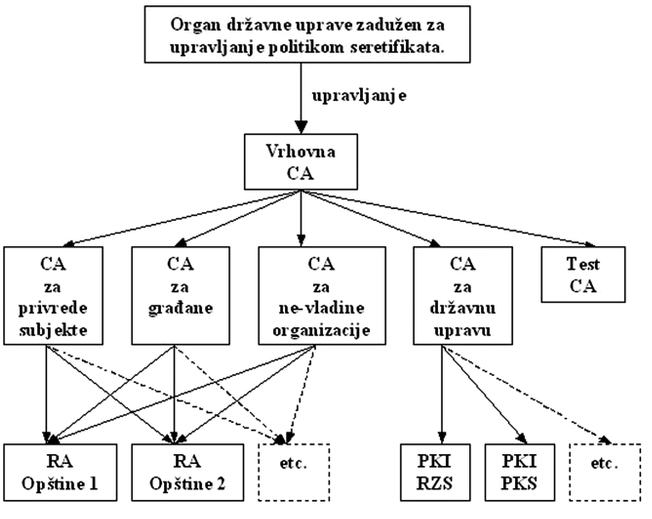
U državnoj upravi mogao bi se definisati sledeći skup usluga koje PKI treba da podržava:

- javni servisi namenjeni građanima - G2C komunikacija
- javni servisi namenjeni privredi - G2B komunikacija
- interni servisi namenjeni zaposlenima u upravi – G2E komunikacija
- međusobna komunikacija aplikacija, saradnja organa raznih nivoa državne uprave – G2G komunikacija.
- sigurna razmena elektronske pošte
- pristup korisnika dokumentima za koja imaju ovlašćenja
- mogućnost objavljivanja digitalno potpisanih dokumanata od strane ovlašćenih korisnika
- izdavanje elektronskih identifikacionih legitimacija.

I sledeće grupe korisnika:

- građani (fizička lica)
- privreda (pravna lica)
- zaposleni u državnoj upravi
- servisi uprave
- mrežni resursi – računari i aktivna mrežna oprema.
- administratori

Republički zavod za statistiku Srbije kao organ državne uprave u okviru plana razvoja treba da izgradi svoj deo infrastrukture javnih ključeva koji bi bio u skladu sa državnom sertfikacionom politikom. Moguće mesto infrastrukture javnih ključeva Republičkog zavoda za statistiku Srbije u okviru državne PKI prikazano je na slici 1.



Slika 1. – *Mesto PKI RZS-a u jednoj od mogućih varijanti državne PKI.*

PKI organa uprave kao što su Republički zavod za statistiku – RZS, Privredna komora Srbije – PKS i sl. mogu se sastojati od jednog ili više CA koji su povezani nekim od modela poverenja.

5. PLAN IZGRADNJE INFRASTRUKTURE JAVNIH KLJUČEVA U RZS

Praksa je pokazala da je PKI dobro i izvodljivo rešenje za zatvorene sisteme, tj. organizacije čiji su svi članovi na neki način, nezavisno od PKI, evidentirani u administrativnim službama i čiji se broj menja na relativno predvidiv način. Republički zavod za statistiku Srbije je tipičan primer ovakvog sistema.

Plan izgradnje PKI prolazi kroz sledeće faze:

- definisanje potreba – utvrđivanje aplikacija i subjekata sertifikovanja
- definisanje potrebne konfiguracije CA i RA
- definisanje odgovarajuće konfiguracije digitalnih sertifikata
- definisanje plana upravljanja sertifikatima gde se pored administrativnih procedura razmatra i repozitorij sertifikata i lista opozvanih sertifikata.

6.DEFINISANJE POTREBA ZA DIGITALNIM SERTIFIKATOM

Prvi korak u izgradnji infrastrukture javnih ključeva, kao i kod svakog drugog projekta, je utvrđivanje potreba koje se žele zadovoljiti i ograničenja resursa kao što su novčana, vremenska i dr. koja predstavljaju granicu za ono šta možemo stvarno napraviti. Ako je moguće napraviti kompromis između želja, potreba i mogućnosti ima smisla krenuti u planiranje PKI u suprotnom loš i nefunkcionalan PKI je gori od nikakvog.

Definisanje potreba je zapravo utvrđivanje usluga koje želimo da naš sistem pruži svojim korisnicima. Usluge informacionog sistema pružaju se korisnicima putem računarskih aplikacija, pa je definisanje usluga zapravo definisanje aplikacija koje će pružati te usluge. Pored usluga potrebno je definisati i grupe korisnika sistema. Korisnici ne moraju biti jednaki po svojim pravima i ne moraju imati pristup svim resursima sistema. Potrebno je utvrditi koje aplikacije će sistem nuditi kojim korisnicima.

7. DEFINISANJE APLIKACIJA

Aplikacije se kako je ranije rečeno mogu uslovno podeliti na dve grupe. Prvu grupu predstavljaju standardne aplikacije koje dolaze kao deo operativnog sistema ili softverskih paketa koji se standardno instaliraju na korisničke računare (tipično WEB pretraživači i e-mail klijenti) i imaju ugrađenu podršku za PKI. Drugu grupu predstavljaju aplikacije posebne namene koje mogu biti nabavljene od proizvođača softvera ili razvijene samostalno. Kod ove druge grupe aplikacija treba voditi računa da se predvidi ugradnja podrške za PKI.

Osnovne usluge koje se pružaju kroz PKI su: šifrovanje i dešifrovanje podataka u transportu i pri čuvanju, digitalni potpisi i autentifikacija. Različite aplikacije, zbog različite namene nude ove sigurnosne usluge u različitim oblicima. Sigurna elektronska pošta podrazumeva mogućnosti šifrovanja/dešifrovanja poruka i/ili njihovo digitalno potpisivanje. Sigurni WEB prenos omogućava autentifikaciju obe strane u komunikaciji i šifrovanje podataka koje one razmenjuju. Potpisivanje koda programa omogućava, kao i svako drugo digitalno potpisivanje, autorima zaštitu rada, a korisnicima potvrdu izvora programa.

U Republičkom zavodu za statistiku Srbije mogao bi se definisati sledeći skup usluga koje PKI interno treba da podržava:

- autentifikacija zaposlenih
- interni servisi namenjeni zaposlenima u RZS
- sigurna razmena elektronske pošte (šifrirana i potpisana)
- siguran pristup korisnika dokumentima i ostalim resursima za koja imaju ovlašćenja
- mogućnost objavljivanja digitalno potpisanih dokumanata od strane ovlašćenih korisnika na intranetu

Razvoj informacionog sistema treba koncipirati tako da se većina usluga koje PKI treba da podržava može realizovati korišćenjem savremenih e-mail klijenata (Outlook Express, MS Outlook, Lotus Notes) i WEB pretraživača (Internet Explorer, Netscape) tj WEB aplikacija. Korišćenje ove dve vrste aplikacija, koje su standardni deo svakog poslovnog računarskog okruženja omogućava izgradnju operativne PKI uz minimalne zahteve za materijalnim i ljudskim resursima.

Unutar RZS postoje i aplikacije posebne namene za koje je potrebno ugraditi podršku za PKI. PKI treba izgraditi tako da se ove aplikacije bez problema mogu dodavati.

7. DEFINISANJE KORISNIKA

Nakon utvrđivanja aplikacija potrebno je definisati kategorije korisnika PKI. Pod korisnicima se podrazumevaju ljudi, računari i računarski programi. Korisnici će se aplikacijama predstavljati putem sertifikata i na osnovu tipa sertifikata će im biti dodeljena odgovarajuća prava i odgovornosti.

U RZS-u mogle bi se definisati sledeće grupe i broj korisnika:

- zaposleni - 600
- rukovodstvo - 100
- administratori računarske mreže i PKI - 10.

8. DEFINISANJE I DOKUMENTOVANJE POLITIKE KORIŠĆENJA SERTIFIKATA

Nakon što su definisane aplikacije i korisnici neophodno je definisati namenu, prava i obaveze koje proističu iz korišćenja infrastrukture. Digitalni sertifikati imaju funkciju ličnih dokumenata kojima se dokazuje identitet u svetu elektronskih komunikacija. Sertifikat povezuje neki subjekat (čovek, računar,

aplikacija) sa njegovim javnim ključem. Sertifikat izdaje sertifikaciono telo CA. CA garantuje trećim subjektima ispravnost podataka na sertifikatu. Treći subjekti na osnovu digitalnog potpisa CA proveravaju autentičnost sertifikata.. Kao i kod ličnih dokumenata, funkcionisanje infrastrukture javnih ključeva zasniva se na poverenju. I ovde je poverenje zasnovano na jasno definisanoj, odobrenoj i objavljenoj politici i procedurama izdavanja sertifikata. Skup uslova kreiranja, izdavanja i korišćenja digitalnih sertifikata naziva se Politika sertifikovanja (engl. *Certificate Policy*). IETF je objavio dokument 'Certificate policy and Certification Practices Framework'' [6] koji daje okvir onog što bi se trebalo definisati u politici sertifikovanja. Skup procedura pomoću kojih se sprovodi politika sertifikovanja, naziva se Izjava o praksi sertifikovanja (engl. *Certification Practice Statement*).

Politika sertifikovanja – CP i Izjava o praksi sertifikovanja – CPS su obavezujući dokumenti za sertifikaciono telo CA. Na osnovu ovih dokumenata treći subjekti mogu oceniti koliko poverenja mogu imati u sertifikate izdate od strane CA. Treći subjekti mogu biti iz istog sigurnosnog domena kao i CA ili iz drugog sigurnosnog domena.

Konkretna politika sertifikovanja direktno zavisi od namene infrastrukture javnih ključeva za koju se definiše ova politika. Politika sertifikovanja se može posmatrati kao dokumentovanje onoga šta se želi uraditi [7]. Obim dokumenta može biti različit u zavisnosti od vrste CA ali za svaki dokument Politike sertifikovanja neophodni elementi koji treba da su u njemu definisani su odgovori na sledeća pitanja [8]:

- Ko je odgovoran za rad CA?
- Koju zajednicu CA opslužuje?
- Koja su pravila identifikacije subjekta sertifikovanja?
- Šta je sadržaj sertifikata?
- Kakva ograničenja su postavljena na rad CA?
- Šta se treba da se uraditi u slučaju bilo kakve neregularnosti?

Na osnovu definisane Politike sertifikovanja kreira se Izjava o praksi sertifikovanja. CPS se može posmatrati kao dokumentovanje onoga kako je potrebno uraditi ono što je definisano u Politici sertifikovanja [7]. Obim i veličina CPS-a zavisi od veličine i obima CP-a..

Na prva dva pitanja je u ovom trenutku moguće dati odgovore i to:

- Za rad CA odgovoran je RZS
- CA opslužuje samo RZS.

Odgovori na ostala pitanja biće dati kasnije.

Neki od linkova na kojima se mogu naći primeri i uputstva za izradu CP i CPS dokumenata:

- S. Chokhani, 'Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework'', RFC2527, March 1999. http://www.ietf.org/ rfc/ rfc2527.txt
- S. Chokhani at all, ž'Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework'', RFC3647, Nov 2003. http://www.ietf.org/rfc/rfc3647.txt
- 'X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework'', Oct 2006. http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

9. DEFINISANJE KONFIGURACIJE CA

Osnova PKI je Sertifikaciono telo – CA. Prvi korak u izgradnji PKI nakon definisanja potreba, je utvrđivanje kakva CA je potrebna da bi se zadovoljile definisane potrebe.

Model poverenja

Republički zavod za statistiku Srbije je hijerarhijska organizacija koja se kao celina nalazi u hijerarhijski organizovnoj državnoj upravi. Ovakvim sistemima odgovara **hijerarhijski model poverenja**. Ovaj model odgovara čvrsto ustrojenim organizacijama gde hijerarhija CA odslikava hijerarhiju organizacije. Standardni hijerarhijski model poverenja je zasnovan na jednoj vrhovnoj CA koja izdaje sertifikate podređenim CA i eventualno kranjim korisnicima. Podređene CA mogu izdavati sertifikate sledećem nižem nivou CA i/ili krajnjim korisnicima. Na ovaj način se svaki sertifikat izdat unutar domena može povezati sa vrhovnim sertifikatom i poverenje u sertifikate se zasniva na poverenju u vrhovnu CA i kompletan lanac poverenja do korisničkih sertifikata. Dobre strane ovog modela su mogućnost centralizovanog upravljanja infrastrukturom javnih ključeva. Vrhovna CA može kroz formu sertifikata nametnuti dogovorenu politiku za sve sertifikate u domenu. Uspostavljanje poverenja sa sertifikatima van domena ostvaruje se uzajamnim sertifikovanjem (engl. *cross-sertification*) vrhovnih sertifikacijskih ustanova iz dva domena [9].

Osnovna podela CA u hijerarhijskom modelu poverenja je na:

- Vrhovnu CA – sama potpisuje svoj sertifikat i poverenje svih korisnika unutar domena je zasnovano na poverenju u ovo sertifikaciono telo.
- Podređenu CA – njen sertifikat je potpisan od strane druge nadređene CA.

Unutar jednog domena u standardnom hijerarhijskom modelu poverenja nalazi se samo jedan vrhovni CA. Broj podređenih CA tebalo bi da bude u skladu sa logičkom organizacijom okruženja za koji se projektuje PKI. Moguće su varijante i bez podređenih CA, gde je vrhovna CA istovremeno i jedina. Takođe je moguće postojanje velikog broja podređenih CA raspoređenih u više hijerarhijskih nivoa. Pošto je osnovni zadatak CA izdavanje sertifikata uobičajena je podela CA na osnovu toga kome izdaju sertifikate:

- CA koja izdaje sertifikate drugim CA
- CA koja izdaje sertifikate krajnjim korisnicima

Moguće je da isti CA izdaje sertifikate i drugim CA i krajnjim korisnicima, ali nije uobičajeno i ne smatra se dobrom praksom.

Podređene CA mogu biti:

- CA koja izdaje sertifikate drugim CA, i u ovom slučaju to su **posredničke CA** između njima nadređenih i podređenih CA
- CA koje izdaju sertifikate krajnjim korisnicima – **izdavačke CA**.

Unutrašnja - spoljašnja CA

Jedna od odluka koju je potrebno doneti pri definisanju CA je da li će ona biti **unutrašnja ili spoljašnja CA**. Unutrašnja CA se formira unutar organizacione jedinice u kojoj se gradi PKI i održava se unutrašnjim resursima. Spoljašnja CA podrazumeva korišćenje CA koja je uspostavljena i održavana od strane nekog van organizacije. Obe varijante imaju svoje prednosti i mane, ne isključuju jedna drugu i moguća je njihova kombinacija.

Unutrašnja CA se smatra dobrim izborom za organizacije čiji će se sertifikati uglavnom koristiti unutar same organizacije. Glavne prednosti su Š10Ć:

- Omogućava da organizacija ima direktnu kontrolu nad svojom sigurnosnom politikom
- Omogućava usklađivanje politike sertifikovanja 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 unutrašnje CA:

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

Spoljašnja CA je dobro rešenje za organizacije koje veliki broj poslova za koje su potrebni sertifikati obavljaju sa subjektima izvan organizacije. Prednosti ovog izbora su:

- Spoljni partneri mogu imati veće poverenje u sertifikate treće, profesionalne strane
- Koristi se tehnološko znanje organizacije koja se specijalizovala za CA
- Koristi se poznavanje tehničkih, pravnih i poslovnih aspekata korišćenja sertifikata koje kompanija koja prodaje CA poseduje.

Nedostaci ovog rešenja su:

- Visoka cena po sertifikatu u slučaju komercijalnih rešenja
- Smanjena fleksibilnost pri konfigurisanju i upravljanju sertifikatima
- Neophodno je imati stalnu vezu sa spoljašnjom CA
- Ograničena integracija sa internim informatičkim resursima.

Moguća je kombinacija ova dva rešenja sa ciljem korišćenja dobrih strana svakog od njih. Upotreba spoljašnje CA za vrhovnu (ili nadređenu) CA koja samo sertifikuje unutrašnje (ili posredničku) CA koji obavljaju ostale poslove sa sertifikatima, je jedno od rešenja koje pruža poverenje spoljašnjim partnerima, a većinu kontrole zadržava unutar organizacije.

Za izgradnju PKI RZS-a potrebno je izabrati kombinovano rešenje za CA. Vrhovna (nadređena) CA treba da bude spoljašnja i da pripada sistemu državne PKI. Nadređena CA treba da sertifikuje internu posredničku CA u RZS-u, dok bi posrednička CA izdavala sertifikate samo podređenima CA u RZS, ali ne i krajnjim korisnicima. Posredničke CA bi bile zadužene za izdavanje sertifikata krajnjim korisnicima u RZS. Ovim rešenjem se postiže da za validnost sertifikata koje izdaje RZS praktično garantuje država dok RZS ima fleksibilnost pri konfigurisanju i upravljanju sertifikatima koje izdaje.

10. POTREBAN BROJ CA I NJIHOVA FUNKCIJA

Za utvrđivanje broja podređenih CA treba razmotriti sledeće [10]:

- Broj krajnjih korisnika sertifikata. Veći broj korisnika može zahtevati veći broj CA da bi se mogao izdavati i održavati potreban broj sertifikata.
- Logička struktura organizacije. Ako je organizacija u kojoj se izdaju sertifikati podeljena tako da su potrebe korisnika za sertifikatima različite, može biti potrebno imati CA za svaku od organizacionih jedinica koja će izdavati odgovarajuće sertifikate.
- Geografska distribuiranost organizacije. Ako je organizacija u kojoj se izdaju sertifikati geografski razuđena moze biti potrebno imati CA na svakoj lokaciji da bi se smanjio mrežni saobraćaj između udaljenih lokacija i obezbedilo dovoljno brzo izdavanje sertifikata.
- Povećanje pouzdanosti. Redudantne CA mogu osigurati besprekidan rad infrastrukture javnih ključeva i u slučaju ispada neke od CA.
- Namena sertifikata. Potrebe za različitim tipovima sertifikata mogu nametnuti potrebu za više CA od kojih će svaka izdavati određeni tip sertifikata.

Za PKI RZS-a broj korisnika je relativno mali tako da bi jedna podređena CA koja izdaje sertifikate krajnjim korisnicima bila sasvim dovoljna. S obzirom da postoji registracijski proces, nezavisan od PKI nema potrebe za postavljanjem registracionog tela RA. Potrebno je dodati proceduru registracije korisnika kod PKI prilikom uobičajene registracije korisnika (pri zapošljavanju, postavljanju na rukovodeće mesto i sl.). U prvoj fazi razvoja PKI RZS bila bi postavljena samo jedna podređena CA RZS-a dok bi u kasnijim fazama njihov broj mogao da se poveća u zavisnosti od potreba.

11. BEZBEDNOST CA

Kod hijerarhijskog modela, poverenje unutar celog sigurnosnog domena zasnovano je na poverenju u vrhovnu CA. Ako dođe do kompromitacije vrhovne CA ruši se osnova poverenja i kompletan sistem sigurne komunikacije unutar domena. Takođe kompromitacijom neke od CA sa nižih nivoa hijerarhije ruši

se poverenje od te tačke skroz na dole. Sigurnost vrhovne CA (ili posredničke CA) može se povećati ako ona izda potrebne sertifikate 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. Uobičajeni termin za ovakvu nepovezanu CA je *offline* CA Š10Ć. Ovo ne bi bilo moguće ako bi vrhovna CA (posrednička CA) izdavala i sertifikate krajnjim korisnicima jer bi onda stalno ili dovoljno često morala biti povezana na sistem i spremna da opsluži zahteve za novim sertifikatom. Nepovezanost vrhovne CA ne utiče na verifikaciju zahteva jer se važeći sertifikati objavljuju u bazi aktivnih digitalnih sertifikata za CA sistem – repozitorijumu, a lista povučenih sertifikata u CRL. Važno je samo da te liste budu ažurne.

Pored ovih mera neophodno je smestiti računar sa vrhovnim CA na fizički sigurnu lokaciju sa ograničenim i kontrolisanim pristupom samo minimalno potrebnom broju lica. Dodatna mera sigurnosti koju je dobro uvesti je mogućnost prijavljivanja na računar sa CA samo uz pomoć pametne kartice sa sertifikatom. Poželjno je sprovesti i druge mere zaštite za slučaj fizičke kompromitacije prostorije u kojoj se računar nalazi. Ovde se misli na onemogućavanje pokretanja operativnog sistema sa spoljašnjih medija (floppy disk, CD/DVD, USB, ...) i zaštita BIOS-a putem lozinke, pa čak i fizičko onemogućavanje otvaranja kućišta računara. Sve ove mere ne mogu zameniti fizičku sigurnost jer je stručnom licu potrebno do pola sata fizičkog pristupa računaru za njegovu potpunu kompromitaciju.

12. POTREBAN HARDVER

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

1. Procesor – kriptografske operacije zahtevaju mnogo računanja sa velikim brojevima. Ovde dužina izabranog ključa ima presudnu ulogu. Ovo znači da je CA aplikacija koja intenzivno koristi procesorske resurse, tako da je procesor kritični resurs za CA. Poboljšanje procesora i-/ili povećanje njihovog broja ima direktan pozitivan efekat na efikasnost CA.

2. Kapacitet diskova – potreban kapacitet diskova najviše zavisi od broja sertifikata, jer veličina sertifikata ne zavisi od dužine ključa Prostor potreban za smeštanje jednog sertifikata je oko 30 KB Š10Ć. Veća brzina diska omogućava brže izdavanje sertifikata. Korišćenje SCSI diskova i RAID tehnologije ima pozitivan uticaj na performanse. Korišćenjem odgovarajuće RAID konfiguracije smanjuje se opasnost usled otkaza nekog od diskova.

3. Memorija – CA nije memorijsko zahtevna aplikacija tako da su količina i tip memorije koji su odgovarajući za instalirani operativni sistem sasvim dovoljni.

Pored hardverskih komponenti 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 i iz sigurnosnih razloga preporučuje se izvrašavanje CA na sopstvenom serveru.

Broj predviđenih sertifikata u RZS je relativno mali tako da je bilo koji savremeni disk sasvim dovoljan za smeštanje svih sertifikata. Intenzitet izdavanja sertifikata bi trebalo da bude ujednačen i mali. Jedini trenutak kada bi se očekivao visok intenzitet izdavanja sertifikata je inicijalno izdavanje sertifikata. Za savremene CA aplikacije ovaj intenzitet ne predstavlja nikakav problem. Windows server 2003 na serveru sa dual-procesorom i 512 MB RAM-a može izdati 2 miliona sertifikata sa standardnom dužinom ključa (512) dnevno [10].

Na osnovu navedenog može se zaključiti da bilo koja savremena serverska konfiguracija može zadovoljiti potrebe CA aplikacije. Zbog funkcije koju ovaj server treba da obavlja potrebno je staviti naglasak na pouzdanost. Serverska mašina treba da bude nabavljena od pouzdanih proizvođača koji svojim imenom garantuju kvalitet servera kao što su: HP, IBM, DELL i sl. Potrebno je da diskovi servera budu u RAID konfiguraciji. RAID konfiguracija treba da bude isključivo hardverska i zavisi od broja diskova koji su na raspolaganju. Jedno od mogućih rešenja sa dva diska je RAID_1 ili preslikavanje (engl. *mirroring*).

13. POTREBAN SOFTVER

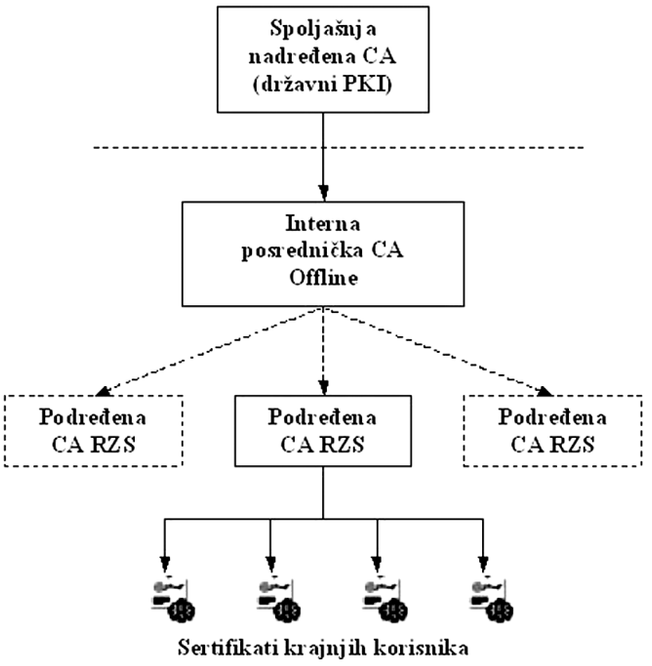
Uspostavljanje CA je zapravo instalacija softverske aplikacije koja obavlja ovu funkciju. Na izabranom hardveru potrebno je pre toga instalirati operativni sistem. Informacioni sistem RZS-a bazira se na dve platforme: MS Windows i IBM ZOS Mainframe. CA treba postaviti na MS Windows platformi tako da se za operativni sistem predlaže Windows Server 2003 Standard Edition. Za CA aplikaciju može se koristiti komponenta Windows Server 2003 Certification Services. Ova komponenta je standardan deo Windows serverskih operativnih sistema od verzije 2000. Ova procedura je detaljno opisana u korisničkoj dokumentaciji Server 2003 i ovde neće biti izlagana.

14. PREDLOG REŠENJA ZA CA RZS-a

Sumirajući predhodna razmatranja, na slici 2. prikazan je predlog za CA Republičkog zavoda za statistiku Srbije.

Definisanje konfiguracije sertifikata

Digitalni sertifikat je struktura podataka koja za cilj ima pouzdano povezivanje javnog ključa sa podacima o njegovom nosiocu, obezbeđujući na taj način proveru identiteta pri, na primer, digitalnom potpisivanju. Sertifikat može biti samopotpisani ili kvalifikovani – oni su u tehničkom pogledu jednaki, ali samopotpisani može da izda bilo ko, a to možete uraditi i sasvim sami. Samopotpisani sertifikat uglavnom se koriste



Slika 2. – *Predlog konfiguracije CA RZS-a.*

interno, ili se pravna snaga dobija potpisivanjem posebnog obavezujućeg ugovora sa korisnikom (kao u e-banking sistemima). Daleko značajniji je kvalifikovani digitalni sertifikat, koji po Zakonu o digitalnom potpisu i pripadajućim podzakonskim aktima može da izda samo sertifikaciono telo koje ispunjava određene zakonske uslove i ima dozvolu za rad. Kvalifikovani digitalni sertifikat sa odgovarajućim parom ključeva se može upotrebiti za kreiranje „kvalifikovanog digitalnog potpisa" elektronskog dokumenta, koji je po pravnoj snazi ekvivalentan papirnom dokumentu potpisanom na klasičan način – olovkom i pečatom.

Termin kvalifikovani digitalni sertifikat se koristi u Direktivi Evropskog parlamenta i saveta o pravnim okvirima za digitalni potpis [11]. Ovaj dokument je uputsto članicama

Verzija formata sertifikata (v3)
Serijski broj sertifikata
Identifikator algoritma za potpisivanje
Naziv CA koja je izdala sertifikat
Period važenja
Ime korisnika sertifikata
Javni ključ korisnika sertifikata (i identifikator algoritma koji ga koristi)
Identifikator davaoca sertifikata (neobavezno)
Identifikator korisnika sertifikata (neobavezno)
Proširenja
DIGITALNI POTPIS SERTIFIKATA TAJNIM KLJUČEM SERTIFIKACIONOG TELA

Slika 2. – *Sadržaj digitalnog sertifikata. [1]*

Evropske unije za kreiranje pravnih okvira koji podržavaju elektronski potpis. Ovaj dokument treba da bude polazna osnova i za ostale zemlje iz okruženja.

Opšteprihvaćeni standard unutrašnje strukture i podataka digitalnih sertifikata je X.509, koji je od 1988. godine do danas imao tri verzije. Aktuelna varijanta obuhvata verziju, jedinstveni serijski broj (jedan od najvažnijih podataka), ID algoritma za hešovanje, vreme važenja od-do, ID algoritma javnog ključa, sam javni ključ, ID algoritma digitalnog potpisa, digitalni potpis. Opciona polja su: identifikator izdavača, identifikator nosioca i ekstenzije.

Glavno unapređenje u verziji 2 je uvođenje jedinstvenih identifikatora izdavača i nosioca, a u verziji 3 uvođenje tzv. proširenja. Proširenja su važna, jer u suštini omogućavaju da se u sam digitalni sertifikat unesu bilo kakvi potrebni podaci. Recimo, tu može stajati informacija o dozvoli za obavljanje nekih poslova ili o pravu potpisa neke vrste ugovora koje ima zaposleni. Sistem koji se implementira može ih prepoznati i reagovati na odgovarajući način. Međutim, ako se prava upisana u ekstenziju izmene, recimo zbog promene radnog mesta, sertifikat mora biti opozvan i nosiocu treba izdati novi. Digitalni sertifikat se prema standardu X.509v3 sastoji iz polja prikazanih na slici 2.

Tabela 1.

POLJE	PREDLOG
Verzija formata sertifikata	v3
Serijski broj sertifikata	Pozitivan celi broj jedinstven unutar CA.
Identifikator algoritma za potpisivanje	Aplikacija CA automatski generiše
Naziv CA koja je izdala sertifikat	Zvaničan naziv organa uprave koji je izdao sertifikat
Period važenja	Zavisno od vrste korisnika od 1 do 10 godina.
Ime korisnika sertifikata	Ime i prezime, JMBG
Javni ključ korisnika sertifikata (i identifikator algoritma koji ga koristi)	aplikacija CA vodi računa o ovom podatku
Identifikator davaoca sertifikata (neobavezno)	RFC3280 preporučuje da se ne koristi
Identifikator korisnika sertifikata (neobavezno)	RFC3280 preporučuje da se ne koristi

Digitalni sertifikati koji treba da se koriste u PKI državne uprave Srbije pa i u RZS-u treba da budu kvalifikovani i zamena za svojeručni potpis. Takođe je predlog da se koristi standard X.509v3 zbog mogućnosti proširenja. Osnovna polja sa predloženim sadržajem data su u Tabeli 1:

Na osnovu EU Direktive [11], a u skladu sa RFC3739 [12] o formatu kvalifikovanih sertifikata mogu se predložiti sledeća proširenja podataka u sertifikatu:

- **Izjava o kvalifikovanom sertifikatu**. Ovo polje je neophodno da bi sertifikat bio kvalifikovan jer u njemu se daja izjava izdavača sertifikata da je sertifikat izdat u skladu sa važećim zakonom u odgovarajućem pravnom sistemu.
- **Namena ključa**. Ove namene su: digitalno potpisivanje, neporicanje, šifriranje ključa, šifriranje podataka, razmena ključeva, verifikacija sertifikata, potpisivanje CRL, samo šifrirovanje i samo dešifrovanje. Moguće namena za ograničene izbranim kriptografskim algoritmom. Za kvalifikovane sertifikate obavezna namena je digitalno potpisivanje i neporicanje
- **Identifikator politike sertifikacije**. Vrednost ovog polja ukazuje na lokaciju gede se može naći Izjava o praksi sertifikovanja. Predložena vrednost je URL adresa ove izjave
- **Dodatni podaci o korisniku** Ovo su podaci koji mogu biti od koristi za različite namene. Dodatni podaci mogu biti: datum rođenja, mesto rođenja, pol, državljanstvo, zemlja boravka etc.
- **Identifikator ključa ustanove**. Ovo polje treba da omogući identifikaciju javnog ključa koji odgovara privatnom ključu kojim je sertifikat potpisan. Namena ovog polja je da omogući utvrđivanje putanje sertifikovanja [9]. RFC3280 preporučuje korišćenje ovog proširenja.

Definisanje plana upravljanja sertifikatima

Ovde će biti pomenuti samo oni aspekti upravljanja sertifikatima koji obično predstavljaju najveću smetnju kod uvođenja PKI. To su:

- metode dobijanja sertifikata
- sigurnost privatnih ključeva

Metode dobijanja sertifikata

Procedure inicijalnog izdavanja sertifikata obično su jedan od najvećih uzroka administrativne komplikovanosti izgradnje infrastrukture javnih ključeva. Razlog za ovo leži u činjenici da je za kvalitetan setifikat neophodno da krajnji korisnik, bude nedvosmisleno identifikovan. Što su precizniji podaci o korisniku, upotrebna vrednost sertifikata je veća, ali potrebno je i više truda u cilju proveravanja ovh podataka. Potrebna preciznost podataka o korisniku koji se nalaze na sertifikatu zavisi od namene sertifikata. Kvalifikovani sertifikati koje je potrebno koristiti u procesu elektronskog poslovanja RZS-a, moraju sadržati prepoznatljivo (engl. *distinguished*) ime korisnika [11]. Za ovo je neophodno da je korisnik kome se izdaje sertifikat poznat sertifikacionom telu. Najsigurniji način da se ova identifikacija obavi je je lično pojavljivanje osobe sa zvaničnim identifikacionim dokumentim.

RZS predstavlja zatvoreni sistem u kome su članovi sistema već poznati administrativnim strukturama. Ovakve sisteme čine sve organizacije koje svojim članovima izdaju identifikacijske dokumente na osnovu pripadnosti organizaciji. Postojeća infrastruktura identifikacije unutar ovih sistema čini ih pogodnim za izgradnju PKI.

Predlog je da se inicijalna registracija i izdavanje sertifikata za zaposlene u RZS izvrši prilikom zasnivanja radnog odnosa. Postojeća administrativna infrastruktura i procedure treba da budu iskorišćene i proširene koracima neophodnim za izdavanje sertifikata. Podaci kojim se identifikuje korisnik sertifikata se prikupljaju u sklopu postojećih procedura i krajnji korisnici se lično pojavljuju u odgovarajućim administrativnim službama RZS-a.

Osim načina identifikacije potrebno je utvrditi i proceduru generisanja para ključeva (javnog i privatnog) i uručivanja sertifikata. Postoje genaralno dva moguća načina generisanja para ključeva i kreiranja digitalnog sertifikata na bazi javnog ključa:

- CA generiše par javnog i privatnog ključa, formira digitalni sertifikat i dostavlja tajni ključ i sertifikat vlasniku.
- Generisanje para ključeva lokalno od samog vlasnika sertifikata korišćenjem hardverskih ili softverskih mehanizama. Zatim se izvrši kreiranje zahteva za izdavanjem sertifikata koji sadrži javni ključ vlasnika koji se šalje ka CA.

Predlog je da pri podnošenju zahteva odnosno pri zapošljavanju budući korisnik na licu mesta dobije identifikacionu karticu koja je odštampana ali u sebi ne sadrži ni digitalni sertifikat niti ključeve. Na računaru, na svom radnom mestu, uz priloženi softver, korisnik generiše par javni/privatni ključ na samoj kartici i pokreće proceduru kreiranja zahteva za izdavanje, koja će zahtev upotpuniti potrebnim podacima i napraviti skoro kompletan digitalni sertifikat. Ovako pripremljen dokument se prosleđuje sertifikacionom telu čiji je zadatak samo da ga digitalno potpiše koristeći svoj tajni ključ. Time je formiran kompletan digitalni sertifikat, koji se vraća nosiocu i koji ga, posredstvom posebnog softvera, smešta na svoju karticu. Na ovaj način privatni ključ nikada ne napušta karticu, što je jedan od najbitnijih razloga pouzdanosti ovakvog sistema.

Postupak dobijanja digitalnih sertifikata za servere bi trebao da bude sličan, sa tom razlikom da nadležni administrator treba na serveru, a ne na kartici, da generiše par ključeva.

15. SIGURNOST PRIVATNOG KLJUČA

Privatni ključ u PKI predstavlja vlasnika sertifikata. Posedovanje privatnog ključa omogućava vlasniku da se u elektronskim komunikacijama nedvosmisleno identifikuje.

U praksi kompromitacija ili gubitak privatnog ključa znače kompromitaciju ili gubitak digitalnog identiteta. Za ovakve slučajeve PKI predviđa opozivanje sertifikata, međutim postoji administrativni problem dobijanja novog sertifikata i njegove distribucije kao i pristupa dokumentima šifriranim starim javnim ključem. Postoji sigurnosni problem u periodu od kada je privatni ključ kompromitovan ili izgubljen do trenutka kada je to otkriveno i prijavljeno. Mogući su i pravni problemi vezani za odgovornost u zavisnosti od namene sertifikata i njegove upotrebe u ovom periodu.. Povećanjem sigurnosti privatnog ključa moguće je dobrim delom izbeći ove probleme.

Predlog rešenja predviđa korišćenje kontaktnih pametnih kartica (engl. *smart card*) na kojima se smešta privatni ključ. Privatni ključ nikada ne napušta karticu, što je jedan od najbitnijih razloga pouzdanosti ovakvog sistema. Pored ove očigledne veće sigurnosti, kartice imaju prednost što su fizička stvar poput pravog ključa prema kojoj se ljudi obično odnose kao nečemu što treba čuvati i za koju je lako otkriti da je izgubljena. Za pristup pomoću pametnih kartica po pravilu je neophodno uneti PIN kod. Na ovaj način se pametnim karticama postiže dvostepena autentifikacija korisnika koji mora nešto imati – pametnu karticu i nešto znati – PIN.

16. ZAKLJUČAK

Iako je stopostotna zaštita informacija i podataka teško ostvariva, pa i nemoguća, predlog izgradnje infrastrukture javnih ključeva u RZS može predstavljati sistem koji pruža određenu sigurnost korisnicima u razmeni i traženju informacija. Infrastuktura javnih ključeva samo je jedan od mogućih načina zaštite korisnika u komunikaciji putem mrežne infrastrukture. Svim učesnicima (davaocima usluga, korisnicima na privatnom, poslovnom i državnom nivou) PKI omogućava efikasniju i sigurniju komunikaciju.

Realizacijom PKI za potrebe RZS-a stvorio bi se sistem koji olakšava funkcionisanje i poslovanje RZS-a. Savremene pametne kartice poseduju resurse za prihvat velike količine podataka i mehanizme za očuvanje tajnosti ovakvih podataka. Ovakve kartice su idealne za odvijanje sigurnog elektronskog poslovanja RZS-a. U integrisanom informacionom sistemu RZS-a uz podršku PKI moguće je postići punu automatizaciju svih poslovnih aktivnosti.

LITERATURA

[1] Andrew S. Tanenbaum, "Računarske mreže, 4. izdanje", Mikroknjiga 2005

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

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

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

[5] A.Whitten, J.D.Tygar, "Why Johnny Can0t Encrypt: A Usability Evaluation of PGP 5.0", Carnegie Mellon University, Proceedings of the 8th USENIX Security Symposium, Avg 1999.

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

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

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

[9] 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.

[10] "Designing a Public Key Infrastructure", Microsoft, Nov 2004 http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/PGCH04.mspx

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

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

Jelena Milojković, Republički zavod za statistiku Srbije

e-mail: mima@statserb.sr.gov.yu

Oblasti interesovanja: Informaciono-komunikacione tehnologije, tehnologije zaštite, mobilno računarstvo