



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I RAČUNARSTVO

**Digitalno potpisivanje dokumenata u
lokalnoj mreži sa sopstvenim CA**
- Diplomski rad -

Mentor:
doc. dr. Aleksandar Jevremović

Student:
Branislav Kozma
Br. indeksa: 2011/202130

Beograd, 2013.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Branislav Kozma

Broj indeksa: 2011/202130

Smer: Informatika i računarstvo

Tema: Digitalno potpisivanje dokumenata u lokalnoj mreži sa sopstvenim CA

Zadatak: Na osnovu teorijskog pregleda tradicionalne šeme PKI infrastrukture dizajnirati generičku šemu za digitalno potpisivanje dokumenata u lokalnoj mreži sa sopstvenim CA. Komparativnom analizom standardne PKI šeme i predložene šeme prikazati doprinose predloženog rešenja.

Datum odobrenja rada:
Beograd, _____._____._____.

MENTOR

doc. dr Aleksandar Jevremović

DEKAN

Prof. dr Miroslav Lutovac

Digitalno potpisivanje dokumenata u lokalnoj mreži sa sopstvenim CA

Sažetak: U radu ćemo raditi na dizajnu sopstvenog rešenja za digitalno potpisivanje dokumenata koji se razmenjuju u lokalnom okruženju. Na osnovu teorijskog pregleda tradicionalne šeme PKI infrastrukture, napravićemo novu generičku šemu za postizanje istog, ako ne i višeg nivoa bezbednosti sa primenom na lokalnom nivou. Lokalni nivo predstavlja određeno radno okruženje ili neku instituciju od visokog značaja (policija, vlada, diplomatija). Doprinosi ovog rada biće predstavljeni ekvivalentnom šemom sa pojednostavljenim funkcionalnim komponentama koje se odnose na primenu algoritma za digitalno potpisivanje i generisanje kriptoloških ključeva za ovu namenu. Komparativnom analizom standardne PKI šeme i predložene šeme našeg rešenja ukazaćemo na postojeće probleme na globalnom nivou u cilju pronalaska rešenja za iste u primeni na lokalnom nivou. Osnovni doprinos ovog rada pored predloženog rešenja je prvenstveno podizanje nivoa svesti o potrebi za primenom ove tehnike koja će uskoro predstavljati poslovnu kulturu u savremenim aplikacijama za razmenu digitalnih sadržaja u cilju prevencije od krađe ili zloupotrebe identiteta.

Ključne reči: digitalno potpisivanje, CA, lokalna mreža, PKI

Digitally signing documents with own CA in the local network

Abstract: In this paper, we will design our own solution for digitally signing documents that are exchanged in the local environment. According to a theoretical examination of traditional PKI schemes, a new generic scheme will be created achieving the same or even a higher level of security for the application at the local level. The local level is specified operating environment or an institution of higher importance (police, government, diplomacy). The contributions of this work will be presented with simplified functional components in an equivalent scheme related to the algorithm for generating digital signatures and cipher keys. Using comparative analysis of standard PKI scheme and the proposed one, the existing problems at the global level will be pointed out in the scope of finding solutions for the implementation at the local level. In addition to the proposed solution the main contribution of this work is to raise primarily awareness of the need for the implementation of this technique, which will soon be the business culture in contemporary applications used for digital content exchange in order to prevent the theft or misuse of identity.

Keywords: digital signature, CA, local network, PKI

SADRŽAJ

Spisak tabela	- 3 -
Spisak slika.....	- 3 -
1 Uvod	- 4 -
1.1 Predmet istraživanja.....	- 4 -
1.2 Doprinosi rada	- 4 -
1.3 Struktura rada.....	- 5 -
2 Pregled u oblasti istraživanja	- 6 -
2.1 Prednosti i nedostaci globalne i lokalne PKI.....	- 6 -
2.2 Razvoj tradicionalne PKI infrastrukture i kriptoloških mehanizama	- 8 -
2.3 Primena tehnologije zasnovane na infrastrukturi javnih ključeva.....	- 9 -
3 Teorijske osnove istraživanja	- 11 -
3.1 Tradicionalna PKI infrastruktura.....	- 11 -
3.2 Osnovna strukturna podela PKI [5]	- 12 -
3.3 Sadržaj i format digitalnog sertifikata	- 14 -
3.4 Digitalni potpis	- 15 -
3.5 Generisanje sertifikata	- 16 -
3.6 SSL protokol.....	- 17 -
3.6.1 Uspostavljanje bebedne veze – SSL rukovanje	- 17 -
3.6.2 Korišćenje bezbedne veze.....	- 18 -
3.7 Heš funkcija.....	- 18 -
3.7.1 MD5.....	- 19 -
3.7.2 SHA	- 19 -
3.8 Simetrični šifarski sistemi	- 19 -
3.8.1 DES.....	- 19 -
3.9 Asimetrični šifarski sistemi	- 21 -
3.9.1 RSA.....	- 21 -
3.9.2 Difi-Helman	- 23 -
3.10 Režimi rada blokovskih šifara	- 23 -

3.10.1 ECB.....	- 24 -
3.10.2 CBC	- 24 -
4 Pregled predloženog rešenja	- 26 -
4.1 Generička šema predloženog rešenja.....	- 26 -
4.1.1 Kompresija.....	- 26 -
4.1.2 Blok za šifrovanje	- 27 -
4.1.3 Provera sertifikata	- 27 -
4.1.4 Dešifrovanje.....	- 27 -
4.1.5 Dekompresija	- 27 -
4.1.6 Diskusija o generičkoj šemi predloženog rešenja	- 27 -
4.2 Postavka i objašnjenje eksperimentalnog okruženja	- 29 -
4.2.1 Razvojno okruženje	- 29 -
4.2.2 Matlab, Cryptool	- 29 -
4.2.3 Specifikacija hardverske platforme.....	- 30 -
4.3 Sprovedene analize koje su prethodile projektovanju celokupnog rešenja .	- 31 -
4.4 Evaluacija predloženog okruženja sa prikazom softverskog rešenja	- 33 -
4.5 Oblast primene predloženog rešenja.....	- 33 -
5 Zaključak.....	- 35 -
5.1 Sumarni ciljevi rada i ostvareni rezultati	- 35 -
5.2 Predlog za budući rad	- 35 -
Literatura	- 37 -

Spisak tabela

Tabela 2.1: Prednosti i nedostaci PKI	- 7 -
Tabela 4.1: Karakteristike računara korišćenog za kompresiju.....	- 30 -
Tabela 4.2: Kompresovani fajlovi različitih formata.....	- 33 -

Spisak slika

Slika 2.1: Digitalni koverat.....	- 9 -
Slika 3.1: Tradicionalna PKI struktura	- 12 -
Slika 3.2: Hijerarhijska arhitektura CA	- 13 -
Slika 3.3: Izgled sertifikata.....	- 15 -
Slika 3.4: Šema digitalnog potpisivanja	- 16 -
Slika 3.5: Generisanje sertifikata.....	- 16 -
Slika 3.6: Uspostavljanje bezbedne veze – SSL rukovanje.....	- 18 -
Slika 3.7: DES šifra	- 20 -
Slika 3.8: Proces jedne runde DES algoritma	- 21 -
Slika 3.9: Šema DH algoritma.....	- 23 -
Slika 4.1: Generička šema razmene dokumenata	- 26 -
Slika 4.2: Šema razmene na bezbednom nivou	- 28 -
Slika 4.3: Detaljna šema algoritma digitalnog potpisivanja dokumenta	- 29 -
Slika 4.4: Generisanje kompresovanog fajla u programu Matlab	- 30 -
Slika 4.5: Šifrovanje kompresovanog dokumenta.....	- 30 -
Slika 4.6: Predložena arhitektura PKI	- 32 -

1 Uvod

1.1 Predmet istraživanja

Razvoj tehnologije na globalnom planu sa aspekta komunikacija, elektronike, transporta u mnogome je uticao i izmenio način života kako na poslovnom tako i na privatnom planu. Danas kada se informacije smatraju važnijim i vrednijim u odnosu na materijalno, a u zavisnosti od brzine i bezbednosti prenosa, isporuke kome su namenjene i tačnosti istih, sve više se pridaje značaj njihovoj zaštiti.

Potreba za tajnom komunikacijom postoji od davnina i može se posmatrati kroz vekove sa aspekta različitih načina zaštite i prenosa podataka. Sa stanovišta informacione zaštite danas, u praksi se najčešće postavljaju sledeća osnovna pitanja koja zahtevaju detaljnu analizu i permanentnu evaluaciju odgovora: šta, od koga, zbog čega ili zašto i kako se zaštititi. Ovaj proces zaštite nikada se ne završava već permanentno traje i razvija se u skladu sa potrebama korisnika, zahtevima nove tehnologije i eventualnih propusta nastalih u procesu razvoja.

Posmatrajući kompleksnu PKI infrastrukturu na globalnom nivou koja je opšte prihvaćena u primenama Internet elektronske trgovine, bankarstvu, komunikaciji, postavlja se pitanje koliko su izdavaoci sertifikata kao „treće strane“ zaista institucije od poverenja, nezavisne i objektivne. Najčešće su to institucije koje su smeštene izvan granica jedne države. Koliko su zaista korisnici bezbedni i zaštićeni od slučajne ili namerne zloupotrebe od strane neovlašćenih lica odnosno institucija. Ovo pitanje dolazi još više do izražaja kada se razmatraju PKI infrastrukture za institucije od visokog značaja. Danas smo svedoci u permanentnom narušavanju bezbednosti institucija od najvišeg ranga u celom svetu.

S obzirom na iznete činjenice, u ovom radu će se razmotriti i predložiti jednostavnije rešenje PKI infrastrukture namenjene lokalnom okruženju, a sa istim, ako ne i boljim nivoom bezbednosti dokumenata.

U radu će se podrazumevati da je između korisnika u lokalnom okruženju ostvarena bezbedna komunikacija preko SSL protokola.

Osnovna ideja rada će se zasnivati na kompresiji dokumenata bilo kog formata Hafmanovim kodom na strani pošiljaoca, a pre šifrovanja, potpisivanja i slanja primaocu. Na strani primaoca podrazumeva se provera integriteta dokumenta, a zatim dekompresija istog. Na ovaj način dokument koji se šalje u lokalnom okruženju je dodatno zaštićen.

1.2 Doprinosi rada

U osnovne doprinose ovog rada spadaju:

1. Razvoj šeme PKI infrastrukture za primenu u manjim poslovnim okruženjima.
2. Analiza tradicionalne PKI infrastrukture sa posebnim osvrtom na bezbednosne slabosti ili ranjivosti koje nije moguće rešavati na globalnom nivou.
3. Uvođenje novih bezbednosnih mehanizama na osnovu detaljne analize PKI-a.

4. Razvoj mehanizma za kompresiju podataka sa implementacijom u lokalnoj PKI infrastrukturi.
5. Implementacija sopstvenog rešenja čija je uloga obezbeđenje servisa za digitalno potpisivanje, što ujedno predstavlja osnovni cilj i glavni doprinos.

U nastavku rada svi doprinosi će biti detaljno opisani.

1.3 Struktura rada

U narednim poglavljima razmatraće se uporedno, prednosti i nedostaci tradicionalne PKI infrastrukture na globalnom nivou i u lokalnom okruženju, sa osvrtom na bezbednosne slabosti. Na bazi teorijskih osnova istraživanja prikazaće se elementarna strukturna podela PKI sa svim činiocima koji jednu PKI strukturu čine bezbednom (digitalni sertifikat, digitalni potpis, SSL protokol za zaštićeni prenos kroz mrežu).

Na osnovu analize prethodno iznetih činjenica biće predstavljeno predloženo rešenje PKI infrastrukture u lokalnom okruženju sa prikazom postignutih rezultata. Prikazom implementacije rešenja navešće se predlozi za budući rad.

2 Pregled u oblasti istraživanja

Istraživanjem oblasti o infrastrukturi javnih ključeva i korišćenih kriptoloških mehanizama za zaštitu podataka i učesnika u komunikaciji, pregledan je ogroman broj radova. Navedeni zaključci su zajednički za sve strukture:

- Mehanizam funkcionisanja PKI je glomazan, zahteva veliki broj resursa
- Poverenje korisnika digitalnih sertifikata u treću stranu je stalni problem
- Mehanizam čuvanja i distribucije liste sertifikata, bilo opozvanih ili važećih je komplikovan i zahtevan, često neusaglašen sa infrastrukturnom, npr. ugradnja registra opozvanih sertifikata u digitalno potpisani dokument
- Problem razmene ključeva preko mreže je stalno aktuelan
- Vreme potrebno da se kriptanalizom dozna tajni ključ u zavisnosti od njegove dužine sve je kraće, zahvaljujući sve bržim IT resursima.
- Mehanizam izdavanja sertifikata je komplikovan

Kao kriptološki mehanizmi u infrastrukturi javnih ključeva koriste se asimetrični sistemi za razmenu ključeva i digitalni sertifikati kako bi se obezbedila autentifikacija korisnika, zaštita podataka i neporecivost poslanih informacija.

Veoma je važno razumeti da PKI (engl. *Public Key Infrastructure*) ne predstavlja samo po sebi autentifikaciju, aplikaciju, autorizaciju ili bezbednosni mehanizam nego je infrastruktura koja podržava ove i druge razne tehničke i poslovne potrebe. [1]

Sertifikati predstavljaju digitalne pasoše izdate od sertifikacionih tela CA (engl. *Certificate Authority*, CA u daljem tekstu) raznim učesnicima u komunikaciji, pri tome garantujući njihov identitet i potvrdu istog ostalim učesnicima na Internetu. Korisnici u komunikaciji utvrđuju autentičnost sertifikata proverom da li je sertifikat izdat od pouzdanog CA i ukoliko jeste komunikacija se ostvaruje između odgovarajućih korisnika. Ukoliko sertifikat nije validan komunikacija može biti odbijena.

Validnost sertifikata može biti opozvana iz brojnih razloga, a osnovna uloga poverenja u CA kompromitovana. Dosadašnja praksa je pokazala da su najčešće kompromitovani sertifikati CA izdatih za bankarsko odnosno finansijsko poslovanje, vladine organizacije i pojedine državne bezbednosne agencije. Jednom kompromitovani CA veoma teško vraća poverenje korisnika. Značaj kompromitovanih podataka, vrsta klijenata i vreme oporavka ukoliko je moguće, direktno utiče na ugled i poslovno okruženje izdavaoca sertifikata, a šteta može biti trajna. Jedan od primera je dat u analizi kompromitacije sertifikata firme *DigiNotar Certificate Authority* [2]. Najveći problem za korisnike predstavlja nebezbednost u periodu od nastanka kompromitacije CA do vremena kada su preduzetim akcijama otklonjeni uzroci. Vreme otkrivanja i rešavanja problema može biti kratko npr. 1 sat, a ponekad i toliko dugo da se meri u nedeljama. Zapaženo je da ovo vreme direktno utiče na posledice primene lažnih sertifikata.

2.1 Prednosti i nedostaci globalne i lokalne PKI

Prilikom razmatranja prednosti i nedostataka PKI infrastrukture uopšte, potrebno je imati u vidu vremenski okvir primene, čuvanja podataka. Posebnu pažnju treba posvetiti

podacima kao što su sertifikati, javni i tajni ključevi, liste isteklih i opozvanih sertifikata koji se nalaze u CRL (engl. *Certificate Revocation List*). Korišćenje ovih podataka u zlonamerne svrhe od strane neovlašćenih lica nema vremensko ograničenje jer se svi podaci snimaju (čak i hešovani). Treba takođe imati u vidu da svi podaci ikada snimljeni, nakon određenog perioda postaju javno dostupni.

Uvidom u globalne koncepcije PKI uočeno je da veliki broj, čak 98% trenutno primenjenih infrastruktura ne podrazumeva primenu kompresovanja podataka u razmeni nakon autentifikacije korisnika, iako je to moguće i dostupno. Drugim rečima, nije primenjeno kompresovanje podataka pre šifrovanja i razmene između korisnika.

Nedostaci tradicionalne PKI su takođe, nemogućnost bezbedne komunikacije bez znanja javnog ključa druge strane, gde se dobijaju i čuvaju sertifikati. Takođe, najčešće zbog problema finansijske prirode, uvođenje i implementacije PKI u organizacijama, kao podizanje nivoa svesti zaposlenih je teško.

Danas su poznata pod nazivom u načelu dva tipa PKI, *open* i *closed* PKI. Koja od ove dve strukture će biti primenjena najviše zavisi od toga da li će se veći deo odgovornosti prebaciti na treću stranu, odnosno spoljni CA ili će se odgovornost preneti na korisnika.

Tabela 2.1: Prednosti i nedostaci PKI

Globalni PKI		Lokalni PKI	
PREDNOSTI	NEDOSTATAK	PREDNOSTI	NEDOSTATAK
Par javni/tajni ključ	Potvrda da je pošiljalac javnog ključa stvarno on. Ovo je rešeno sa DC		Zahteva poseban softver za bezbedan prenos podataka
Digitalni sertifikat DC izdaje CA na osnovu vodiča <i>Certification Practice Statement</i> (CPS)		Upravljanje rizikom. Poznat je način i broj korisnika, jer je izdavalac sertifikata sopstveni CA	Nesigurnost da li je kod i ostala PKI zaista bezbedna.
Poverenje između korisnika obezbeđuje CA		Tajnost koda koji nije dostupan javnosti. Pretpostavka da je kod bezbedan	
Integracija PKI u postojeće arhitekture jednostavnija		Certifikat se izdaje kome korisnik želi, a sa spoljnim korisnicima – uzajamno sertifikovanje	Veliki teret na pojedinačnog korisnika u mreži
Lako proširenje PKI arhitekture na korisničku mrežu			Ažuriranje programa i kompaktibilnost istih na svim računarima u komunikaciji
Odgovornost za		Direktna procena i	

bezbednu komunikaciju snosi treća strana		prihvatanje gubitaka usled kompromitovanja	
	MIM napad, prisluškivanje, lažno predstavljanje		MIM napad, prisluškivanje, lažno predstavljanje
	Metodologija komplikovanog dodeljivanja CA	Metodologija lakog dodeljivanja CA	Realizacija obično je duža nego kod eksterne CA
	Troškovi implementacija sa finansijskog aspekta	Troškovi implementacija sa finansijskog aspekta relativno manji	
	Ugradnja liste CRL u potpisani dokument	Može biti integrisana sa postojećom informatičkom infrastrukturom	
	stalna veza sa CA		

2.2 Razvoj tradicionalne PKI infrastrukture i kriptoloških mehanizama

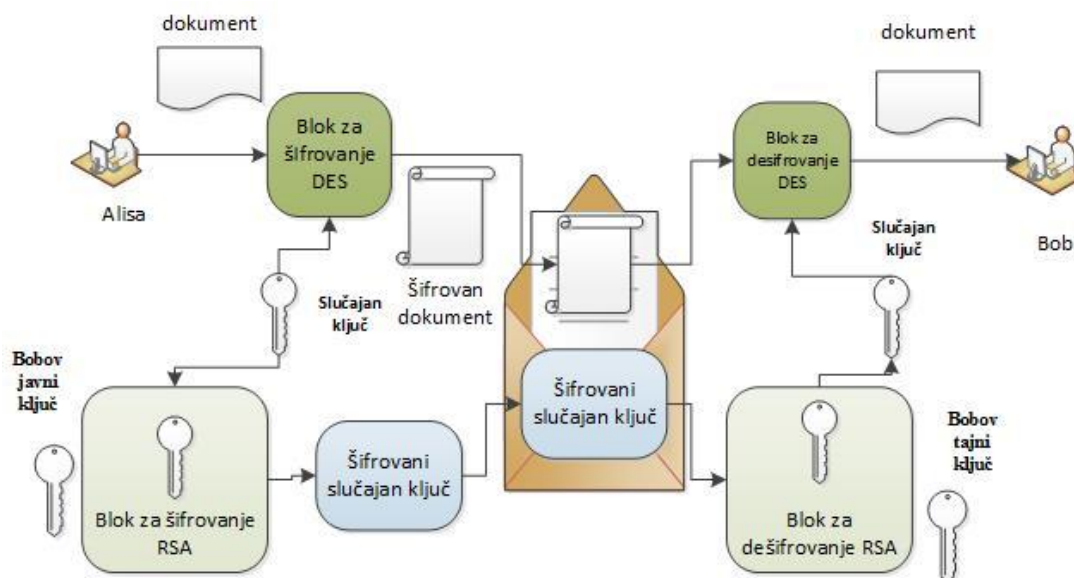
Simetrična kriptografija koristi isti ključ za šifrovanje i dešifrovanje. Jednostavna je za korišćenje i implementaciju, algoritmi su brzi, ali se pojavljuju dva osnovna problema: razmena podataka nije bezbedna, odnosno nema pouzdane autentifikacije korisnika, a drugo broj potrebnih ključeva, višestruko je veći od broja korisnika. Najpoznatiji algoritmi za šifrovanje simetričnim ključevima su DES, TripleDES, AES o kojima će više reći biti u nastavku.

Ovi problemi mogu da se uklone pomoću asimetrične kriptografije. Asimetrična kriptografija koristi dva ključa: privatni ključ poznat samo vlasniku i javni ključ koji može biti poznat svakome. Kada neko želi da pošalje poruku osobi, on mora da pronađe javni ključ te osobe i njime šifruje poruku. Primalac potom dešifruje poruku sa svojim privatnim ključem i dobija otvoreni tekst. Međutim opšte je poznato da su asimetrični algoritmi zbog dužine ključeva i kompleksnosti rada isuviše tromi i spori u odnosu na simetrične algoritme. Najpoznatiji asimetrični algoritmi koji se danas koriste su RSA, Diffi – Helman.

Kombinacija kriptografije sa simetričnim i asimetričnim ključem može rešiti nedostatke koji nastaju pojedinačnim korišćenjem.

Tako na primer kombinacija asimetričnog RSA algoritma sa tajnim i javnim ključem i simetričnim algoritmom DES za šifrovanje poruke poznata je kao digitalni koverat.

Pretpostavimo da Alice želi da pošalje šifrovanu poruku Bobu. Ona je prvo šifruje poruku sa DES, koristeći slučajno izabran DES ključ. Zatim pronalazi Bobov javni ključ i koristi ga za šifrovanje DES ključa. Poruka šifrovana sa DES i RSA šifrovani DES ključ, zajedno čine RSA digitalni koverat i šalju se Bobu. Nakon prijema digitalne koverte, Bob dešifruje DES ključ sa svojim privatnim ključem, zatim koristi DES ključ za dešifrovanje same poruke. Na slici 2.1 je prikazan scenario.



Slika 2.1: Digitalni koverat

Da bi se dodao digitalni koverat u poruku, pošiljalac mora da dobije javni ključ primaoca. Isto tako, da verifikuje digitalni potpis, primalac mora da dobije javni ključ pošiljaoca. Jednostavan način je da se javni ključ pošiljaoca uključi u svaku poruku. Na ovaj način se neće narušiti bezbednost, ali se dobija mnogo dodatnih zaglavlja i sadržaja koji su često duži od originalne poruke.

Međutim, i dalje postoji problem kako možemo biti sigurni da je javni ključ prosleđen bilo kome ispravno. Rešenje u ovom slučaju je da se koristi sertifikovan ključ izdat od hijerarhijski utvrđenog sertifikovanog organa odnosno CA. Tako, svako sada može da proveri javni ključ uvidom u sertifikat korisnika. Drugi problem je kako možemo biti sigurni da je poruka prosleđena ispravno, odnosno da je stigla kome je namenjena, a na prijemnoj strani biti siguran od koga je poslata. Rešenje ovog problema je uvođenje digitalnog potpisivanja od autentifikovanog pošiljaoca.

Digitalni potpis je kao rešenje predložen od strane Kohnfelder 1978.godine [3,4]. On je uveo termin certifikat kao digitalno potpisan elektronski dokument koji povezuje javni ključ sa onim kome pripada.

2.3 Primena tehnologije zasnovane na infrastrukturi javnih ključeva

Stepen poverljivosti, značaj i posledice koje dokumenta odnosno informacije prouzrokuju direktno utiču na procenu primene rešenja kako za zaštitu samih dokumenata, tako i na definisanje infrastrukture (hardversku i softversku).

Infrastruktura javnih ključeva nalazi danas veliku primenu u svim oblastima od javnog značaja, finansijskom poslovanju kompanija, finansijskim transakcijama građana, dokazivanju identiteta osoba, pa čak i u proizvodnoj delatnosti IT opreme. Proizvođači koriste sopstvene sertifikate da bi ugradili šifrovanje javnog ključa u svoje uređaje.

Tako na primer, privatni korisnici imaju potrebu zaštite svojih podataka ukoliko postoji više korisnika personalnog računara, a poslovni korisnici potrebu zaštite poverljivih dokumenata poslovanja kompanije. Jedan od načina da korisnici štite dokumenta koja smatraju poverljivim jeste primena digitalnog potpisa.

Za nepobitnu autentifikaciju korisnika do sada su korišćeni različiti mediji čuvanja identifikacionih podataka kao što su smart kartice, USB flashevi, tokeni, biometrijska lična dokumenta. Svi ovi mediji mogu biti kompromitovani ako ih koristi neovlašćena osoba, a vlasnik trajno gubi dokaz o autentifikaciji. Znači poznati kriptološki slogan "ono što imam" biće narušen.

Ne tako davno, biometrijski podaci (otisak prsta, glas, iris) nalaze primenu prvenstveno u autentifikaciji osoba, a u kombinaciji sa infrastrukturom javnih ključeva u digitalnom potpisivanju i razmeni dokumenata.

Aplikacije zasnovane na PKI infastrukturi nalaze veliku primenu u sistemima zaštite transportnog sloja OSI modela u računarskim mrežama, E mail servisima, internet transakcijama, obezbeđivanju tajnosti razmenjenih podataka.

3 Teorijske osnove istraživanja

Asimetrična kriptografija ili infrastruktura sa javnim ključem (PKI) je najbitnija infrastrukturna komponenta zaštite računarskih mreža iz više razloga [5]:

- Više je zastupljena od simetrične kriptografije po broju korisnika,
- Svakom korisniku potreban je par ključeva za međusobnu komunikaciju,
- Problem koji postoji kod distribucije ključa sa simetričnom kriptografijom je rešen,
- Zaštite transakcija i digitalno potpisivanje je obezbeđeno

U PKI javni ključ je dostupan svim korisnicima u mreži, a privatni se strogo čuva kod vlasnika. Glavni nedostatak PKI sistema je izgrađivanje poverenja korisnika u povezanost javnog ključa i nominalnog vlasnika.

Iz tih razloga svaka mrežna bezbednosna infrastruktura treba da obezbedi rešenje za četiri glavna bezbednosna problema:

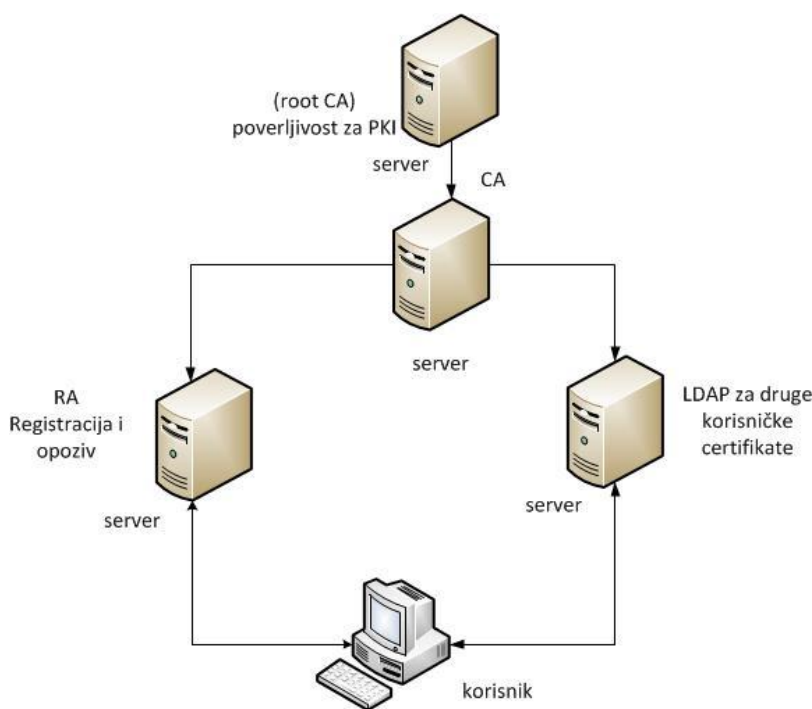
1. **Poverljivost** - da informacije koje se prenose ne budu otkrivene neovlašćenim korisnicima.
2. **Integritet podataka** – prenošena informacija nije dirana ili menjana na bilo koji način
3. **Autentifikaciju podataka** - korisnici mogu da provere identitet pošiljaoca
4. **Neopovrgavanje** - sigurnosna infrastruktura obezbeđuje primaocu i nepobitno dokazuje da je primljena informacija od određenog pošiljaoca, takođe se tumači i kao neporecivost

3.1 Tradicionalna PKI infrastruktura

Tradicionalna infrastruktura javnih ključeva PKI zasnovana je na hardverskim i softverskim komponentama, procedurama za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i sertifikata. Osnovna namena i težnja PKI je da omogući upravljanje, distribuciju i korišćenje javnih ključeva i sertifikata u cilju obezbeđenja sigurne komunikacije između različitih korisnika pri tome gradeći poverenje da korisnik bude siguran sa kim komunicira.

Na slici 3.1 je prikazana tradicionalna PKI struktura. Najčešće primenjivani osnovni model podrazumeva korišćenje sledećih komponenti:

- Najvišeg sertifikacionog tela, Rut CA (engl. *Root CA*)
- Sertifikacionog tela, CA
- Registracionog tela RA (engl. *Registration Authority*)
- Baza sa listom aktivnih i opozvanih digitalnih potpisa LDAP (engl. *Lightweight-Directory Access Protocol*) i CRL (engl. *Certification Revocation List*)
- Korisnici



Slika 3.1: Tradicionalna PKI struktura

- Rut CA kao najviše sertifikaciono telo izdaje i potpisuje sertifikat, uslovljava metode rada drugih CA zavisno od izgrađene arhitekture.
- Sertifikaciono telo vodi računa o izdavanju i ispravnosti sertifikata.
- Registraciono telo vrši identifikaciju, registraciju ili opoziv korisnika, kreira zahtev za izdavanje sertifikata, a delegiran je od CA.
- Baza podataka sadrži sve aktivne i opozvane sertifikate izdate od strane CA.

3.2 Osnovna strukturna podela PKI [5]

Prema načinu organizovanja CA, PKI se deli na tri osnovne strukture:

- a) hijerarhijsku koja uključuje primenu *root CA*
- b) rešetkastu koja direktno povezuje pojedinačne CA i svi CA su poverljivi
- c) tranziciona struktura odnosno BCA (engl. *Bridge CA*), rešetkasta sa *habom* ili hijerarhijska sa spoljnom vezom.

Razmotriće se prednosti i nedostaci svake od gore pomenutih arhitekture kako bi se došlo do nekog optimalnog rešenja primenljivog u lokalnom okruženju:

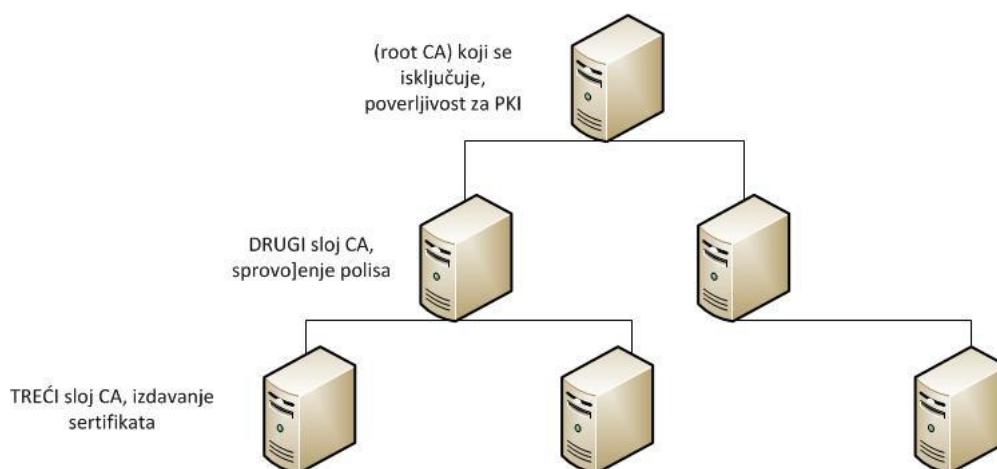
a) Hijerarhijska

Ova arhitektura podrazumeva korišćenje rut CA od najvišeg nivoa poverenja i na osnovu koje se zasniva cela koncepcija infrastrukture. Sadrži osnovni najviši digitalni potpis kojim se potpisuju CA na nižim nivoima, čuva tajni ključ, a javni dostavlja na više CA na nižem nivou tako da digitalni potpis podređenog CA sadrži potpis generisanog od rut CA. Način realizacije hijerarhijske arhitekture po pitanju tehnologije, metoda rada drugih CA direktno je određena od samog rut CA.

Prednost ovakve arhitekture je centralno upravljanje u jednom smeru (od vrha na dnu po dubini) i jednostavna struktura. Glavni nedostatak ove arhitekture je ugrožavanje kompletne PKI strukture u slučaju kompromitovanja rut CA kao jedinog od poverenja, nemogućnost brzog oporavka i teško upravljanje za veće PKI sisteme.

Zavisno od primenjene strukture CA se mogu podeliti po slojevima, odnosno može biti više CA na jednom ili više slojeva. Tako na primer CA na drugom sloju je podređen rut CA u istoj PKI, CA na trećem podređen je CA na drugom sloju itd.

Drugi sloj CA zatim se koristi za sprovođenje polisa i postupaka za izdavanje sertifikata za treći sloj CA. CA u ovom trećem sloju izdaju certifikate za korišćenje od strane računara, aplikacija i korisnika. Ovaj pristup je uobičajen kada se planira instalacija rut CA kao samostalnog u nekom okruženju, kao na slici 3.2.



Slika 3.2: Hijerarhijska arhitektura CA

Zbog ovih ozbiljnih nedostataka, praksa korisnika ovakve arhitekture je da se rut CA, nakon dodeljivanja sertifikata podređenim CA, isključuje sa mreže (ili barem njegovi hard diskovi) i čuva u sefu (ili nekoj drugoj fizički bezbednoj lokaciji) do isteka izdatog sertifikata, obično pet do deset godina.

b) Rešetkasta

Rešetkasta struktura podrazumeva direktno povezivanje pojedinačnih CA sa jednakom poverljivošću svakog od njih, odnosno ravnopravnom poverljivošću. U osnovi se sertifikati razmenjuju između povezanih CA dok samo CA koji poseduje privatni ključ izdaje sertifikate i javni ključ ostalima u mreži. Prednost ovakve arhitekture je uzajamno poverenje između CA i njegova distribucija, direktna povezanost CA. Nedostaci ovakve arhitekture su uslovljenost poverenja i neodređenost puta istog zbog mogućnosti da neki od CA ograniči poverenje. Mogućnost postojanja beskonačne petlje digitalnog potpisa čini oporavak od kompromitacije težim i složenijim.

c) Tranziciona

Tranziciona BCA je u suštini rešetkasta arhitektura sa habom ili hijerarhijska sa spoljnom vezom. Za razliku od hijerarhijske i rešetkaste arhitekture, tranziciona (BCA) ne izdaje digitalni sertifikat direktno korisnicima te prema tome ne predstavlja poverljivi

entitet za korisnike PKI. U načelu je to mehanizam koji povezuje ostale PKI. Prednosti ove arhitekture su brži oporavak u odnosu na mrežnu i mogućnost korišćenja postojećih digitalnih sertifikata do opoziva, te nemaju promene konfiguracije sistema. Nedostatak je što korisnici koriste vlastite i samopotpisane CA kao osnovne tačke poverenja, a izgradnja hardversko softverske infrastrukture za uspostavljanje za BCA sertifikate je na korisnicima.

3.3 Sadržaj i format digitalnog sertifikata

Digitalni sertifikati omogućavaju potvrdu identiteta pri elektronskim transakcijama, slično kao što to čine lične karte u međuljudskim interakcijama. On povezuje podatke o identitetu korisnika sa parom asimetričnih ključeva koji se koriste za šifrovanje i potpisivanje digitalne informacije čime potvrđuje nečije pravo na korišćenje kriptografskih ključeva. Digitalni sertifikat je izdat i digitalno potpisan od strane CA kome veruju svi učesnici u komunikaciji.

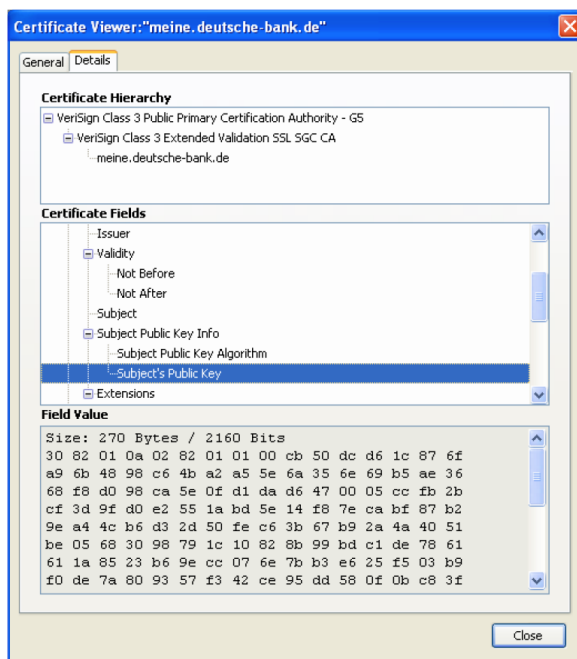
Digitalni sertifikat najčešće sadrži:

- Podatke o vlasniku
- Javni ključ vlasnika
- Period važenja
- Ime izdavača (CA koje je izdalo sertifikat)
- Serijski broj
- Digitalni potpis izdavača

Format digitalnog sertifikata je definisan X.509 v3. standardom, a polja koja treba da sadrži digitalni sertifikat su sledeća:

1. **Version** - informacija o verziji sertifikata. Trenutna verzija (koja se najčešće sreće) je 3.
2. **Serial number** – serijski broj sertifikata predstavlja jedinstveni identifikator sertifikata izdatih od određenog CA
3. **Signature** - identifikator algoritma (u formi identifikatora objekta (OID)) korišćenog od strane CA za potpisivanje sertifikata.
4. **Issuer** - jedinstveno ime CA koje je izdalo sertifikat.
5. **Validity** - označava period važenja sertifikata i sadrži dva datuma od kojih jedan označava trenutak od kada se sertifikat može smatrati važećim - polje *Not Valid Before*, a drugi, trenutak do kog se sertifikat može smatrati važećim – polje *Not Valid After*.
6. **Subject** - identifikuje korisnika kome je izdat sertifikat. Kao i polje *Issuer*, daje se u formi jedinstvenog imena.
7. **Subject public key info** - sadrži javni ključ korisnika, kao i identifikaciju algoritma koji je korišćen pri kreiranju istog (RSA, DSA ili Diffie-Hellman).
8. **Unique identifiers** - je dodatni jedinstveni identifikator sertifikata (ne preporučuje u verzijama 2 i 3)

9. **Extensions** - sadrži listu jednog ili više proširenja sertifikata koja se koriste za specificiranje dodatnih informacija o sertifikatu.



Slika 3.3: Izgled sertifikata

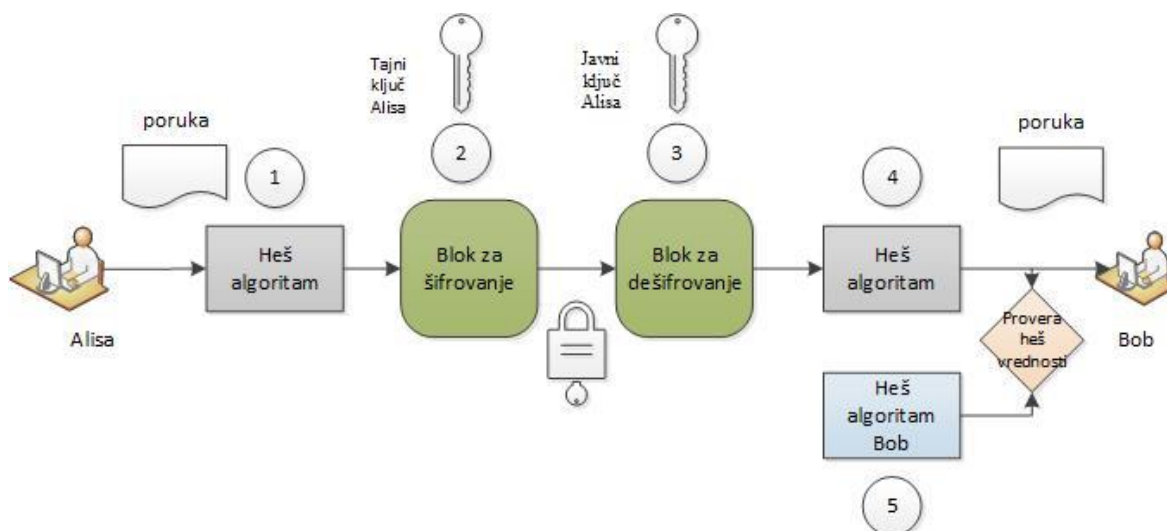
3.4 Digitalni potpis

Digitalni potpis obezbeđuje da primalac poruke bude siguran da nije došlo do izmene originalnog sadržaja poruke, kao i da bude siguran u identitet pošiljaoca poruke, odnosno garantuje integritet poruke i integritet pošiljaoca iste [6]. On je neporeciv tako da bilo kakva kasnija negiranja o slanju poruke od strane pošiljaoca ili sumnja u njegovu autentičnost su neprihvatljiva.

Digitalni potpis poruke se formira korišćenjem tehnike asimetričnih ključeva. Na slici 3.4 je predstavljena šema digitalnog potpisivanja.

Na predajnoj strani primenjuje se heš algoritam na originalnu poruku tako da ako bi došlo do najmanje promene u originalnoj poruci, promenio bi se i rezultujući heš poruke (1). Zatim se vrši šifrovanje heša tajnim ključem (2) pošiljaoca (Alisa). Ovako šifrovan heš predstavlja digitalni potpis poruke. Pošiljalac dodaje na kraj originalne poruke i njen digitalni potpis i šalje tako digitalno potpisanu poruku (katanac). Na prijemu, primaloc (Bob) pomoću javnog ključa pošiljaoca vrši dešifrovanje digitalnog potpisa poruke (3).

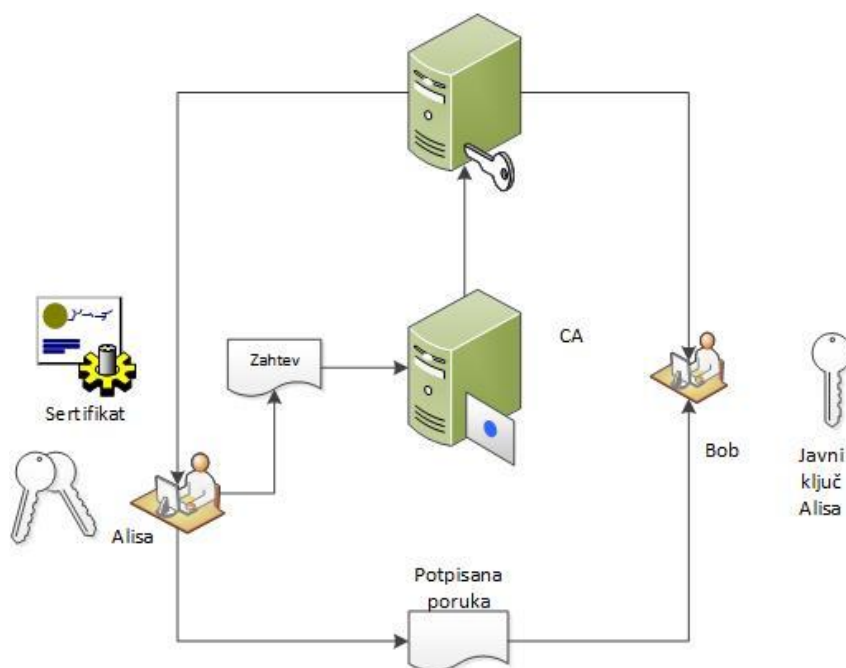
Dobijeni heš poslate poruke (4) poredi sa vrednošću heša koji je dobijen primenom istog heš algoritma na samu primljenu poruku (5). Ako se dobijene vrednosti ne razlikuju primalac može da bude siguran da poruka nije izmenjena. Ako se vrednosti razlikuju znači da je došlo do neovlašćenog menjanja sadržaja poruke i/ili da je neko drugi poslao poruku od onog za koga se izdaje, odnosno narušeni su autentifikacija pošiljaoca i integritet poruke. [7,8]



Slika 3.4: Šema digitalnog potpisivanja

3.5 Generisanje sertifikata

U okviru PKI infrastrukture korisnici koji imaju potrebu za bezbednom komunikacijom moraju posedovati važeći digitalni sertifikat izdat od ovlašćene institucije, u našem slučaju CA. Ovlašćena institucija na osnovu zahteva koji podnosi korisnik izdaje sertifikat, zatim se generišu javni i tajni ključ, pri čemu tajni ključ čuva korisnik, a javni se čuva u bazi sa ključevima. Iz baze javnih ključeva isti se distribuiraju drugim korisnicima u komunikaciji koji komuniciraju sa vlasnikom javnog ključa. Iako kombinacija ključeva može biti generisana od strane CA, radi postizanja veće bezbednosti preporuka je da ključeve generiše sam korisnik. U tom slučaju tajni ključ je poznat samo korisniku, a javni ključ se prosleđuje nadležnom CA za smeštaj u bazu ključeva. Na slici 3.5 je prikazano izdavanje sertifikata.



Slika 3.5: Generisanje sertifikata

3.6 SSL protokol

SSL (engl. *Secure Sockets Layer*) protokol se nalazi između transportnog i aplikacionog sloja OSI modela. Koristi se HTTP protokol na portu 443 i naziva se bezbednim HTTP, a obeležava se sa HTTPS. Da je veza bezbedna može se videti u pretraživaču ako je link definisan sa <https://www.....>

Nakon uspostavljanja bezbedne veze npr. sertifikaciono telo može da posluži za izdavanje sertifikata pri čemu komunikacija sa CA serverom nije deo protokola SSL, komunikacija i razmena podataka se ostvaruje preko SSL protokola. Ostvarivanje sesija se vrši na aplikativnom sloju.

Zadatak SSL protokola je da ostvari zaštićeni prenos podataka kroz mrežu. SSL obezbeđuje mehanizme za identifikaciju servera, identifikaciju klijenta i šifrovanu razmenu podataka između njih.

SSL sadrži dva protokola:

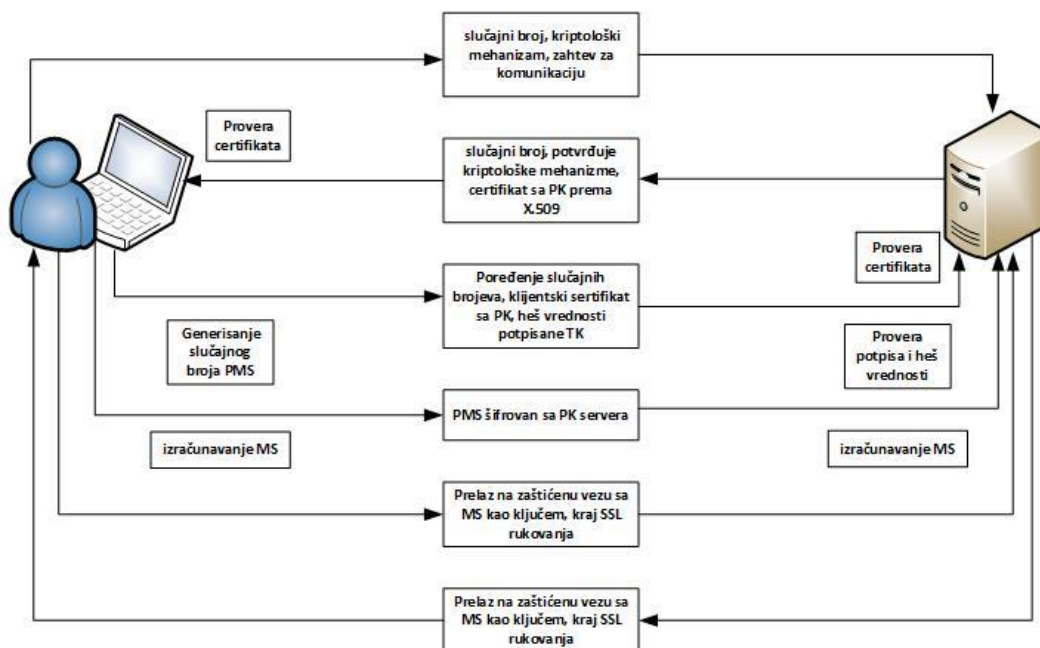
- a) **Uspostavljanje bezbedne veze** – SSL rukovanje (engl. *SSL Handshake*) u 9 koraka koji omogućava autentikaciju klijenta i servera, razmenu parametara za šifrovanje i dogovaranje tajnog ključa za simetrični algoritam šifrovanja
- b) **Korišćenje bezbedne veze** – (engl. *SSL Record*) koja podrazumeva sledeće faze protokola:
 - Deljenje na poruke određene dužine
 - Kompresija
 - Hešovanje kompresovanog dela + Tajni ključ
 - Šifrovanje i prenos poruka

3.6.1 Uspostavljanje bebedne veze – SSL rukovanje

Uspostavljanje bezbedne veze vrši se u sledećim koracima:

1. Klijent zahteva vezu pri čemu bira verziju protokola SSL v3.0, generiše slučajni 28-bitni broj (IV), kriptološke algoritme za razmenu ključa, simetrični ključ i indentifikaciju poslate poruke MAC (*Message authentication code*). Zatim određuje metodu kompresovanja poruke pre slanja. U ovom slučaju će se primeniti Hafmanov kod sa entropijskim kodovanjem.
2. Nakon provere parametara dobijenih od strane klijenta, na strani servera se generiše slučajni 28-bitni broj, server bira najbolje podešavanje za SSL, kompresuje poruku i šalje nazad klijentu uz potvrdu prihvatanja istih za komunikaciju.
3. U ovom koraku server šalje digitalno potpisane potrebne parametre za razmenu ključa (javni i tajni ključ) zavisno od izabranog algoritma sadržane u sertifikatu koji je potpisan od strane CA. Najčešće korišćeni protokoli su RSA i DH čije vrednosti parametrara su sadržani u sertifikatu (moduo N i javni ključ e za RSA ili p , q i S za DH). Klijent proverava digitalni potpis od strane servera.

4. Nakon provere digitalnog potpisa klijent generiše slučajni podatak IV od 46 bitova koji šifruje dogovorenim protokolom RSA ili DH uz upotrebu javnog ključa koji je sadržan u sertifikatu dobijenog od servera. Ovaj slučajni podatak IV poznat kao *pre master secret* korisnik šalje serveru, a zatim od njega generiše master ključ (*master secret*).
5. Nakon dobijanja generisanog slučajnog podatka IV od klijenta, server je u stanju da izračuna svoj master ključ. Međusobnom razmenom heshovanih vrednosti master ključeva u slučaju jednakih vrednosti sa obe strane, klijent i server potvrđuju autentifikaciju. Sva naredna komunikacija je šifrovana simetričnim algoritmom.



Slika 3.6: Uspostavljanje bezbedne veze – SSL rukovanje

3.6.2 Korišćenje bezbedne veze

Nakon uspostavljanja bezbedne veze SSL protokolom, komunikacija i razmena podataka između klijenta i servera može da započne. Da bi se podaci razmenili prema SSL *record* protokolu neophodno je izvršiti deljenje poruke na određene dužine, kompresiju, hešovanje kompresovanog dela + Tajni ključ, a zatim šifrovanje i prenos.

3.7 Heš funkcija

Heš funkcije [9] su jednosmerne i standardno se primenjuju kod provere integriteta dobijene poruke. Najčešću primenu imaju kod digitalnog potpisivanja. Otvoreni tekst proizvoljne dužine sažima se na tekst fiksne dužine, čime se ne opterećuje komunikacioni kanal i povećava efikasnost izračunavanja.

Najviše korišćene hesh funkcije su:

- **MD5** - Hash vrednost dužine 128 bita
- **RIPEMD-160** – 160 bitska varijanta MD5

- **SHA-1:** Hash vrednost dužine 160 bita
- **SHA-2:** Hash vrednost dužine do 512 bita

3.7.1 MD5

Ravijena 1991. godine od strane Rolanda Rivesta MD5 (engl. Message-Digest algorithm 5) predstavlja heš funkciju koja se najčešće koristila. Iako je od 2004. godine postala neotporna na smetnje, odnosno razbijeni algoritam je pokazao koliziju (za dva različita sertifikata dao je istu heš vrednost), sve manje je u u potrebi, ali zbog brzine rada koristi se za proveru integriteta većih fajlova. Dužina dobijene heš vrednosti (sažetka, sume) je 128 bitova. Tipično se predstavlja sa 32 heksadecimalne cifre.

3.7.2 SHA

Nove heš funkcije iz grupe SHA (engl. *Secure Hash Algorithm*) su uvedene ustandard nakon problema koji su se javili sa MD5. Heš vrednost je standardne dužine 160 bita.

Već danas su se funkcije iz grupe SHA-0 i SHA-1 kao nesigurnim jer je u SHA-1 pronađena kolizija, tako da već tokom 2002. godine nastaje nova grupa funkcija pod nazivom SHA-2 (SHA-256, SHA-384 i SHA-512. SHA-224). Nova grupa funkcija su znatno sigurnije u odnosu na SHA-0 i SHA-1 zbog dužine sažetka, promena u algoritmu, drugih vrednosti pomeranja ali u nema značajnih promena u odnosu na ranije algoritme. Međutim, bez obzira na poboljšanja koja su načinjena u novim algoritmima, SHA-1 i dalje predstavlja industrijski standard u kriptografiji.

Početkom oktobra 2012. godine NIST je objavio pobednika na takmičenju za izradu algoritma heš funkcije SHA-3, koja treba da zameni grupu SHA-2 u slučaju da ikad bude razbijena.

3.8 Simetrični šifarski sistemi

Simetrični šifarski sistemi zasnovani su na šifrovanju tajnim ključem koji se koristi u oba postupka simetrične kriptografije, za šifrovanje i dešifrovanje. Za proces šifrovanja u potrebno je znati kriptološki algoritam i tajni ključ. Svi savremeni algoritmi su javno dostupni pa skrivanje algoritma ne doprinosi bezbednosti. Zbog toga pored snage algoritma bezbednost pre svega od tajnosti i dužine ključa.

Osnovna podela šifarskih sistema sa simetričnim ključem je na klasične, sekvencijalne i blokove.

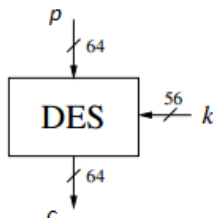
3.8.1 DES

Najpoznatiji simetrični algoritam je DES (engl. *Data Encryption Standard*) sa K= 56 bita, razvijen u IBM (1977). ostao je standardni simetrični algoritam sve do 2000. godine. Pripada blokovskim šiframa.

Cilj dizajna je bio da se uvedu principi *konfuzije* i *difuzije*.

- **Konfuzija** – Šifrat treba da zavisi od otvorenog teksta i ključa na složen način.
- **Difuzija** – Svaki bit šifrata treba da je funkcija svih bitova otvorenog teksta i svih bitova ključa.

DES vrši šifrovanje blokova dužine 64 bita ključem dužine 56 bita.



Slika 3.7: DES šifra

Svaki blok otvorenog teksta se transformiše u 16 rundi koje obavljaju identičnu operaciju. U svakoj rundi se koristi 48 bita ključa (podključ).

DES je Fejstel šifra. Fejstel šifra (nazvana po pioniru blokovskih šifara Horstu Fejstelu) ne predstavlja određenu šifru nego generalni princip dizajniranja šifri. Kod Fejstel šifri otvoreni tekst P se deli na blokove tako što se svaki blok deli na dva dela – levi L i desni R .

$$P = (L_0, R_0)$$

U svakoj rundi i ($i = 1, 2, \dots, n$), leva i desna strana se izračunavaju na sledeći način:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

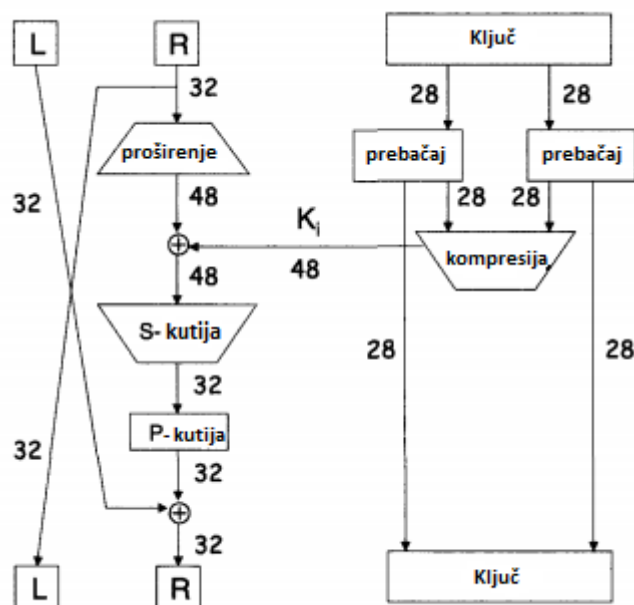
F je funkcija runde.

K_i je podključ za rundu i . podključ je izveden iz ključa K prema specifičnom algoritmu. Izlaz iz runde je šifrat C .

$$C = (L_n, R_n)$$

Pošto je DES Fejstel šifra, šifrovanje prati pravila prikazana u jednačini:

$$F(D_{i-1}, K_i) = P - kutija(S - kutija(proširenje(D_{i-1} \oplus K_i)))$$



Slika 3.8: Proces jedne runde DES algoritma

Trideset godina intenzivne kriptanalize nije otkrilo nikakve propuste tipa “*back door*”. Sa aspekta sigurnosti, danas je DES ranjiv na *brute-force* napade samo zbog male dužine ključa, a ne zato što postoji neki ozbiljniji skraćeni napad. Iako su razvijeni neki napadi koji teorijski zahtevaju neznatno manje posla u odnosu na potpunu pretragu ključeva, svi dosad napravljeni programi za razbijanje DES-a jednostavno isprobavaju sve kombinacije ključeva dok ne nađu na onu pravu, odnosno, primenjuju potpunu pretragu ključeva

3.9 Asimetrični šifarski sistemi

Asimetrični šifarski sistemi se najčešće kombinuju sa simetričnim šifarskim sistemima u cilju obezbeđenja sigurne razmene sesijskog ključa za šifrovanje i dešifrovanje u simetričnom šifarskom sistemu, zatim za zaštitu poverljivosti šifrovanjem i dešifrovanjem, kao i za digitalno potpisivanje čime se postiže zaštita integriteta, neporecivosti i autentifikacija.

Kriptografiju sa asimetričnim ključevima odlikuje upotreba dva ključa i to javni ključ primaoca koji koristi pošiljalac za šifrovanje i privatni (tajni) ključ primaoca kojim primalac dešifrovanje. Ovi sistemi se baziraju na korišćenju jednosmernih (*one way*) funkcija jer se lako izračunavaju u jednom, a teško izračunavaju u drugom smeru. Dva najpoznatija i najviše primenjivana algoritma su RSA i DH.

3.9.1 RSA

RSA algoritam je nastao 1978. godine kao rezultat istraživanja tri istraživača sa MIT Univerziteta: Ronald Rivest, Adi Šamir i Leonard Adelman na osnovu čijih početnih slova u imenu je algoritam i dobio ime.

Koncepcija algoritma je zasnovana na korišćenju jednosmerne funkcije koja otvoreni tekst poruke menja u šifrat C tako da se primenom neke tajne vrednosti nad

njenom inverznom funkcijom može doći do originalne poruke M . Odnosno da važe relacije:

$$C = E(M, K_e)$$

$$M = D(C, K_d)$$

$$M = D(E(M, K_e), K_d)$$

Funkcija koja daje konceptijsko rešenje ima oblik

$$f(x) = x^e \pmod{N}$$

Prema tome, vrednosti e i N mogu biti izabrane tako se ispuni uslov da je funkcija jednosmerna, uz poznavanje tajne vrednosti može da se nađe njena inverzna vrednost, bez poznavanja tajne vrednosti ona je praktično nerešiva.

3.9.1.1 Postupak šifrovanja i dešifrovanja:

Analogno prethodno iznetim stavovima šifrat se može posmatrati kao:

$$C = M^e \pmod{N}$$

gde je M je poruka (otvoreni tekst)

Na prijemnoj strani dešifrovanje se vrši prema formuli:

$$M = C^d \pmod{N} = (M^e)^d \pmod{N} = M^{ed} \pmod{N}$$

Pri čemu vrednosti N i e poznate stranama u komunikaciji, a vrednost d je poznata samo prijemnoj strani. Na osnovu toga može se primeniti sledeće:

- Javni ključ: (N, e)
- Privatni ključ: d

3.9.1.2 RSA digitalni potpis

Digitalno potpisivanje poruke M vrši se na osnovu sledeće formule:

$$S = M^d \pmod{N} \quad \text{gde je } S \text{ je digitalni potpis}$$

Kod RSA: dešifrovanje i potpisivanje su iste operacije

Iz formule se zaključuje da je za digitalno potpisivanje neophodno poznavanje tajnog ključa d . Potpisivanje poruke vrši predajna strana odnosno pošiljalac.

Potvrda ispravnosti digitalnog potpisa na poruci M se vrši na prijemnoj strani, a prema sledećoj formuli:

$$S^e \pmod{N} = (M^d)^e \pmod{N} = M$$

Uočljivo je da je operacija ista kao i kod šifrovanja, prema tome svako ko zna javni ključ (N, e) može da potvrdi ispravnost digitalnog potpisa.

3.9.2 Difi-Helman

Difi i Helman (DH) algoritam nastao krajem '70. godina, kao rezultat istraživanja Vitfilda Difi (*Whitfield Diffie*) i Martina Helman (*Martin Hellman*) sa MIT, a koristi se za razmenu zajedničkog simetričnog ključa i nije namenjen za šifrovanje ili digitalno potpisivanje. Sigurnost ovog algoritma se zasniva na računskoj složenosti izračunavanja (jednosmerne funkcije) diskretnog logaritma.

Za zadate vrednosti g , p , i $g^n \pmod{p}$ potrebno je naći n , tako, ako je poznato g i x , gde je $x = g^n$, može da se odredi n na osnovu formule:

$$n = \log_g(x)$$

Ako je

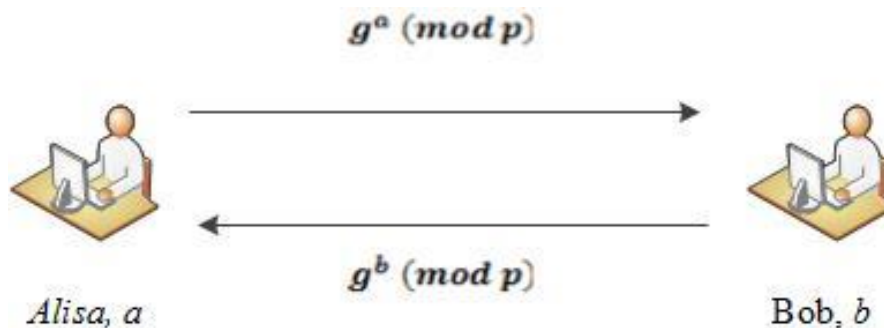
$x = g^n \pmod{p}$, n se takođe određuje preko diskretnog logaritma.

Neka je p veliki prost broj i g takvo da se za svako $x \in \{1, 2, 3, \dots, p-1\}$ može naći n tako da je:

$$x = g^n \pmod{p}$$

Neka su vrednosti p i g javne, a a i b tajne.

Alisa bira tajnu vrednost a , a Bob b kao velike slučajne cele brojeve, te na osnovu njih javno razmenjuju izračunate vrednosti $g^a \pmod{p}$ i $g^b \pmod{p}$ respektivno. Zatim, računaju zajedničku tajnu vrednost $g^{ab} \pmod{p}$ i koriste je kao simetrični ključ $K = g^{ab} \pmod{p}$. Na slici 3.9 je dat šematski prikaz razmene.



Slika 3.9: Šema DH algoritma

DH algoritam je slab na napad tipa MITM (man in the middle) te su autori algoritma predložili korišćenje DH u asimetričnim šifarskim sistemima, pri čemu su ključevi za šifrovanje i dešifrovanje različiti. Sa javnim ključem se vrši šifrovanje poruke, a sa tajnim dešifrovanje.

3.10 Režimi rada blokovskih šifara

U radu sa blokovskim šiframa kao što je DES otvoreni tekst se deli na blokove, te ukoliko je dužina poruke tolika da nije umnožak dužine bloka tada se mora dopunjavati do veličine bloka. Ovde ćemo pomenuti dva od pet najčešće korišćena režime rada i to:

elektronske kodne knjige (*engl. Electronic Codebook – ECB mode*) i ulančavanje bloka šifrata (*engl. Cipher Block Chaining - CBC mode*).

3.10.1 ECB

Kod režima ECB jedan blok otvorenog teksta šifruje se u jedan blok šifrata. Svaki blok otvorenog teksta šifruje se nezavisno.

Režim rada se odlikuje jednom ozbiljnom slabošću da za isti blok otvorenog teksta daje isti blok šifrata, pri čemu se svaki blok šifruje nezavisno.

Šifrovanje se vrši primenom formule:

$$C_i = E(P_i, K) \quad \text{za } i = 0, 1, 2$$

a dešifrovanje

$$P_i = D(C_i, K) \quad \text{za } i = 0, 1, 2$$

Zbog eventualne velike redudanse poruke, postoji mogućnost da se iz ECB šifrata vidi originalna poruka i bez upotrebe ključa, odnosno delimično rekonstruiše kodna knjiga. Razlog za to je sledeći:

Ako pretpostavimo da je $P_i = P_j$, na osnovu formule sledi da je $C_i = C_j$. Napadač može zaključiti da je $P_i = P_j$ čak i ako ne zna P_i ili P_j .

3.10.2 CBC

Slabost ECB režima rada ovde je izbegnuta jer se za svaki sledeći blok otvorenog teksta šifrata koristi prethodni blok, odnosno vrši se takozvano ulančavanje blokova. Ulančavanje dodaje blokovskoj šifri mehanizam povratne sprege. Svaki blok se koristi za promenu šifrovanja sledećeg bloka. Tako, za ovaj režim rada je postignuto da identični blokovi otvorenog teksta daju različite blokove šifrata.

Za početak rada režima neophodno je obezbediti inicijalni vektor koji je generisan na čisto slučajan način. Dužina inicijalnog vektora jednaka je dužini bloka date šifre.

U režimu CBC, pre šifrovanja se obavlja operacija XOR nad blokom otvorenog teksta i prethodnim blokom šifrata.

Šifrovanje u CBC režimu je:

$$C_i = E(P_i \oplus C_{i-1}, K) \quad \text{za } i = 0, 1, 2$$

$$C_0 = E(IV \oplus P_0, K)$$

$$C_1 = E(C_0 \oplus P_1, K)$$

$$C_2 = E(C_1 \oplus P_2, K)$$

a za dešifrovanje:

$$P_i = D(C_i, K) \oplus C_{i-1} \quad \text{za } i = 0, 1, 2$$

$$P_i = IV \oplus D(C_o, K)$$

$$P_1 = C_0 \oplus D(C_1, K)$$

$$P_2 = C_1 \oplus D(C_2, K)$$

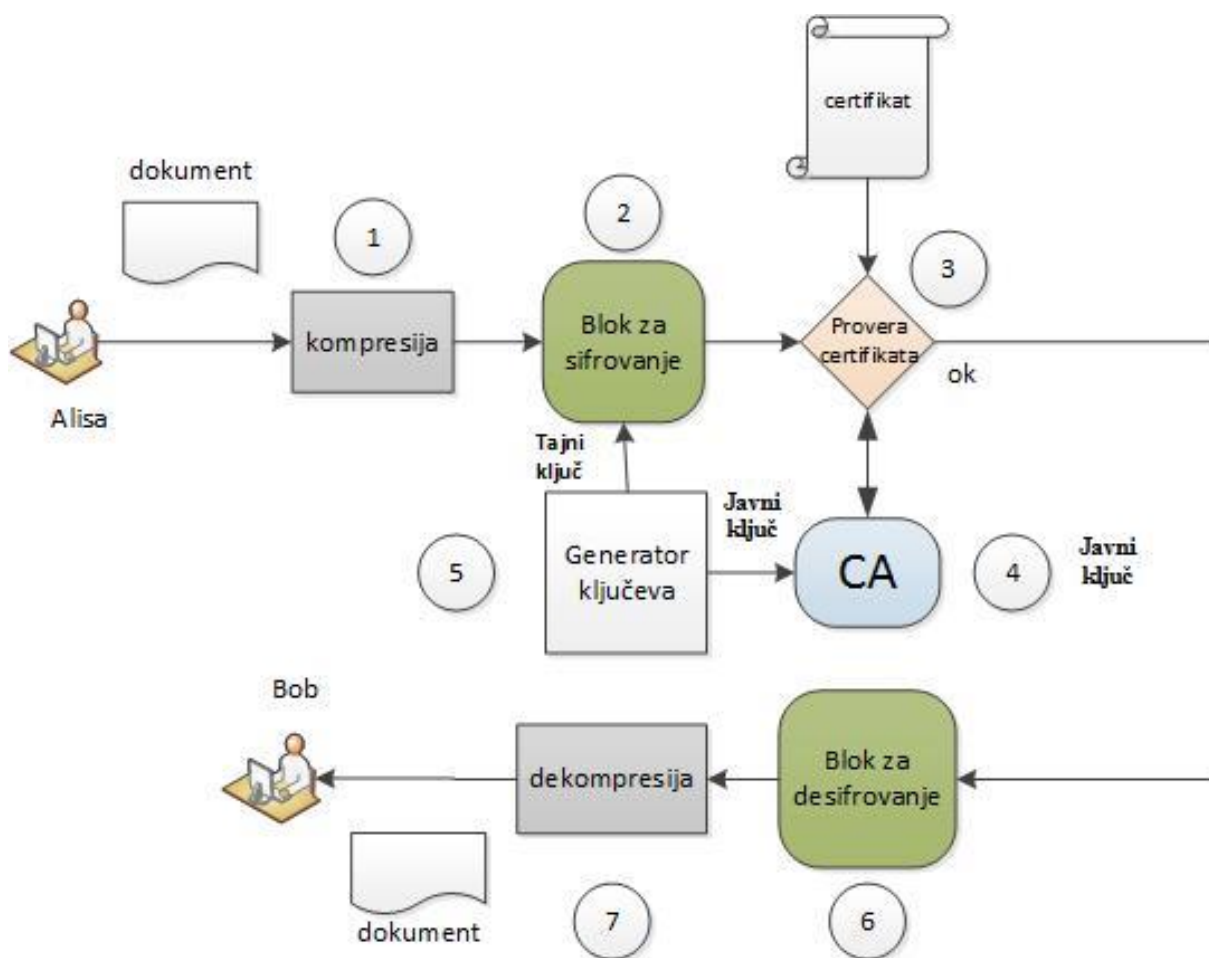
4 Pregled predloženog rešenja

Na osnovu generičkih šema, ekperimentalnog okruženja i analize u ovom poglavlju biće predstavljeno predloženo rešenje.

4.1 Generička šema predloženog rešenja

Predloženo rešenje za bezbednu razmenu dokumenata sačinjavaju nekoliko faza i to: na predajnoj strani, kompresija dokumenta, šifrovanje, potpisivanje, slanje dokumenta, dok na prijemnoj strani, dešifrovanje dokumenta, dekompresija. Pri tom se podrazumeva da je bezbedna veza preko SSL protokola uspostavljena i da je sesijski ključ razmenjen.

Kao podrška u proveru predloženog rešenja korišćeni su programi Matlab R2012b i CrypTool 2.0 (Nightly Build 5452.1).



Slika 4.1: Generička šema razmene dokumenata

Na slici 4.1 numerički su obeleženi elementi slike koji će biti detaljno opisani po koracima.

4.1.1 Kompresija

Na strani pošiljaoca (Alisa) originalni dokument koji može biti tekst, slika, pdf, audio mp3 ili video mp4 fajl se pretvara u binarni niz, a zatim se kompresuje *Huffman*-

ovom funkcijom **fhcode** na manju veličinu, u programskom okruženju Matlab. Kompresovanjem smo postigli dve stvari, prvo smanjili smo veličinu dokumenta na očekivanu vrednost, a drugo postignute su izmene originalnog dokumenta tako da nije prepoznatljiv.

4.1.2 Blok za šifrovanje

U narednom koraku kompresovani dokument se hešuje tako da ako bi došlo do najmanje promene u kompresovanom dokumentu odnosno poruci, promenio bi se i rezultujući heš poruke. Hešovana poruka se šifrjuje sa simetričnim algoritmom sa režimom.

4.1.3 Provera sertifikata

Na strani CA dodeljen javni ključ pošiljaoca (Alisa) se u slučaju ispravne verifikacije, prosleđuje primaocu (Bob) koji koristi isti za dešifrovanje poruke. Uz poruku je poslat i digitalni sertifikat pošiljaoca kako bi se primalac uverio u njegov identitet.

4.1.4 Dešifrovanje

Nakon provere identiteta primalac poruke dešifrjuje poruku algoritmom koji je dogovoren između korisnika, a koja u sebi sadrži kompresovan fajl.

Identitet pošiljaoca ne garantuje da poslata poruka nije izmenjena odnosno da nije narušen njen integritet. Iz tog razloga primalac poruke vrši upoređivanje primljene heš vrednosti sa vrednošću heša koji je dobijen primenom istog heš algoritma na samu primljenu poruku.

4.1.5 Dekompresija

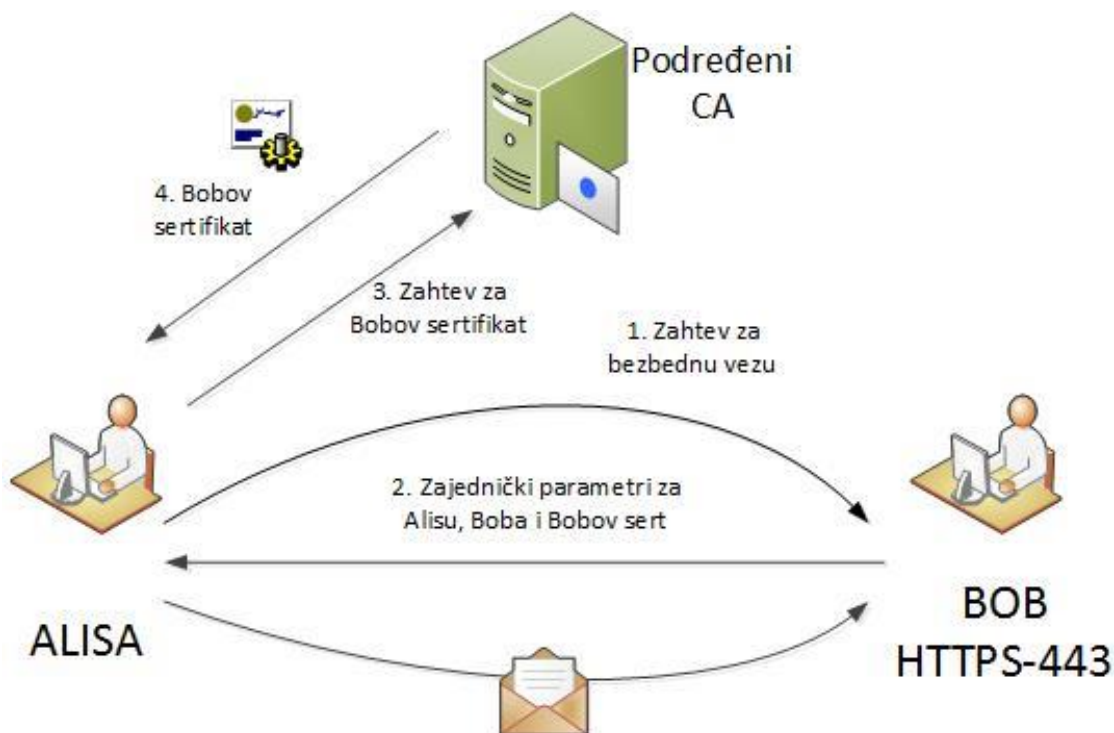
U ovom koraku dekompresijom poruke dobija se originalan dokument pošiljaoca. Ovde se podrazumeva da korisnik na prijemnoj strani ima adekvatni algoritam za dekompresiju kao na predajnoj strani.

4.1.6 Diskusija o generičkoj šemi predloženog rešenja

Detaljna analiza generičke šeme predstavljena je u narednim poglavljima gde su diskutovani scenariji komunikacije i primena u praksi:

1. Alisa traži zahtev za bezbednu komunikaciju – Cipher Suites
2. Dobija Cipher Suites zajednički za oboje i Bobov sertifikat
3. Alisin zahtev za Bobovim sertifikatom upućuje CA
4. CA šalje sertifikat
5. Alisa sifrjuje kompresovanu poruku sa DES, a sesijski ključ šifrjuje Bobovim javnim ključem.
6. Šifrovanu poruku i potpisani ključ salje zajedno kao digitalni koverat Bobu.

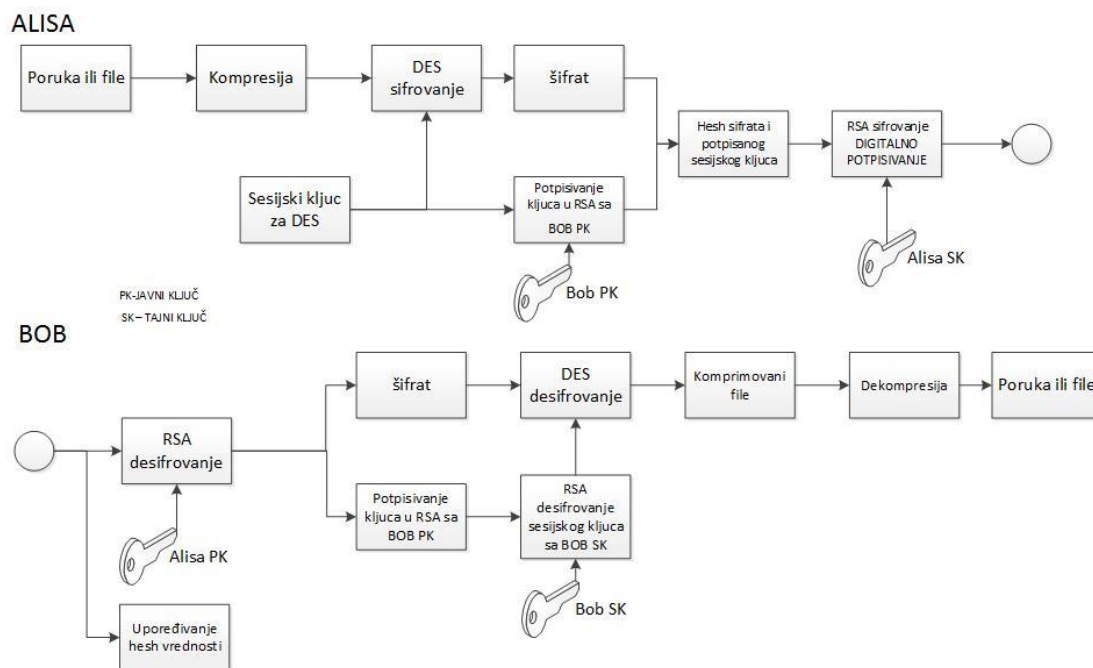
7. Bob proverava hesh vrednost poslatog koverta, dešifruje sa svojim tajnim ključem da bi uzeo sesijski ključ i proverava koverat na integritet.
8. Bob otvara poruku sa sesijskim ključem.



Slika 4.2: Šema razmene na bezbednom nivou

Na ovaj način smo obezbedili da se tajni ključevi korisnika ne prenose preko mreže, a da u slučaju obstrukcije razmene od strane napadača, nije moguće doći do sesijskog ključa za dešifrovanje poruke, što je prikazano na slici 4.2.

S obzirom da je komunikacija zaštićena preko SSL protokola, a distribucija sertifikata nije deo ovog protokola, na slici 4.3 je dat princip razmene dokumenata sa korišćenjem ključeva iz sertifikata.



Slika 4.3: Detaljna šema algoritma digitalnog potpisivanja dokumenta

4.2 Postavka i objašnjenje eksperimentalnog okruženja

4.2.1 Razvojno okruženje

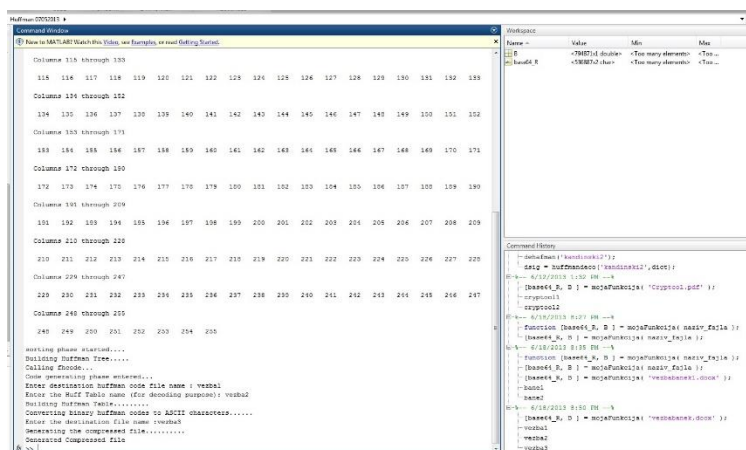
Za potrebe pretvaranja u binarni niz i kompresovanja dokumentata kao razvojno okruženje korišćen je program Matlab R2012b. Za proveru kriptoloških mehanizama na kompresovanim fajlovima korišćen je program CrypTool 2.0 (Nightly Build 5452.1).

4.2.2 Matlab, Cryptool

U programskom okruženju MatlabR2012b rađena je kompresija fajlova sa programom "moja funkcija" koja u sebi sadrži funkciju **fhcode**. U toku kompresije generisana su tri fajla:

- binarni fajl originalnog fajla
- huffmanova tabela za svrhu dekodovanja i na kraju,
- kompresovan fajl.

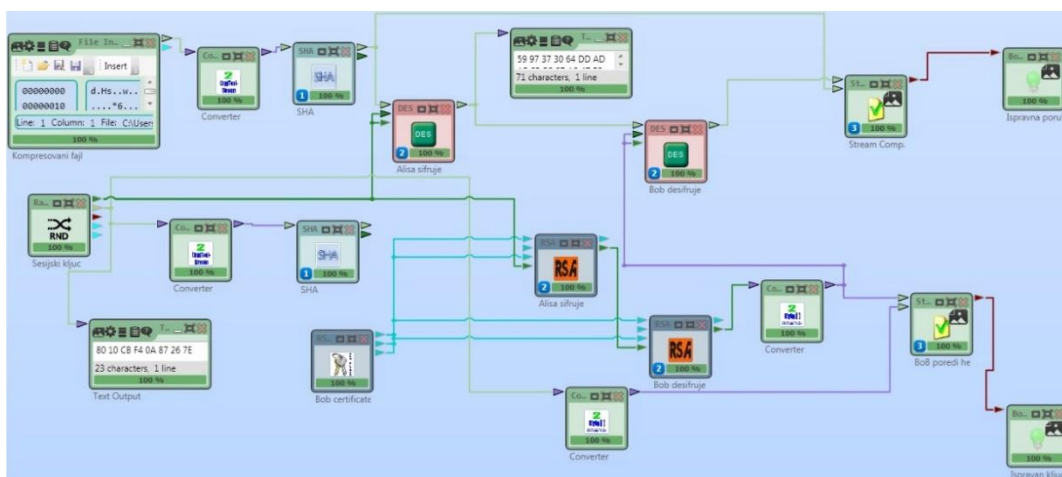
Na slici 4.4 je prikazan primer kompresije tekstualnog fajla od 777kb.



Slika 4.4: Generisanje kompresovanog fajla u programu Matlab

Evaluacija dobijenih rezultata kompresije data je u narednim poglavljima. Dobijeni fajl je zatim korišćen kao kompresovana poruka odnosno ulazni podatak u programskom okruženju Criptool 2.0 (Nightly Build 5452.1) za šifrovanje i dešifrovanje poruke simetričnim DES algoritmom.

Criptool 2.0 (Nightly Build 5452.1) je besplatno programsko okruženje za edukaciju u kome se mogu realizovati osmišljeni kriptografski koncepti. Korišćenjem ovog programa provereni su zamišljeni kriptografski algoritmi za šifrovanje, dešifrovanje i digitalno potpisivanje kompresovanih dokumenata. Za digitalno potpisivanje dokumenata korišćen je standardno korišćeni u svetu RSA algoritam, a za simulaciju asimetričnih ključeva upotrebljen je generisani sertifikat korisnika.



Slika 4.5: Šifrovanje kompresovanog dokumenta

4.2.3 Specifikacija hardverske platforme

U procesu razvoja rešenja za kompresiju fajlova, kriptoloških mehanizama, analize dobijenih vrednosti i rezultata korišćen je personalni računar sledećih performansi prikazanih u tabeli 4.1:

Tabela 4.1: Karakteristike računara korišćenog za kompresiju

Komponente	Opis
Procesor	Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz
Memorija (RAM)	8.00 GB
Grafička kartica	AMD Radeon HD 7700 Series
Hard disk	1 TB
Primary monitor resolution	1920x1080
OS	Windows 7 Professional 64bit

4.3 Sprovedene analize koje su prethodile projektovanju celokupnog rešenja

Na osnovu analize minimalnih zahteva bezbednosti i detaljnog uvida u TPKE definisanih u poglavlju 2. utvrđeno je da korisnici u lokalnom okruženju imaju najviše potrebu za sigurnom e-mail komunikacijom, sigurnom autentikacijom i digitalnim potpisivanjem podataka koji se razmenjuju.

S obzirom da se komunikacija odvija u lokalnom okruženju potreba za implementacijom sertifikata koji će biti prihvaćeni od strane svih korisnika na Internetu je suvišna iz dva razloga.

Prvi je finansijske prirode, jer takvi sertifikati iziskuju velika finansijska izdvajanja i utiču na finansijsku sposobnost korisnika.

Drugi razlog je od strateškog značaja da li je korisniku potrebno visokoarbitražno certifikaciono telo prihvaćeno od celog sveta u svrhu bezbedne komunikacije sa zaposlenima ili klijentima. Komunikacija sa spoljnim klijentima izvan lokalnog okruženja moguća je međusobnom sertifikacijom između dva domena.

Iz tog razloga, prihvatljivo rešenje arhitekture CA za lokalno okruženje je kombinacija internog root CA i podređenih CA u hijerarhijskom modelu. IT zaštita vrhovnog ili root CA pored fizičke zaštite, podrazumevala bi *offline* mod rada ili bi fizički bio odvojen sa mreže. Na slici 4.6 je predstavljena predložena arhitektura PKI.

S obzirom da se u lokalnom okruženju vrši autentifikacija zaposlenih prilikom zapošljavanja na osnovu ličnih dokumenata izdatih od treće strane u koju se ima poverenja (npr. MUP RS ili druga državna ustanova), potreba za CRL je suvišna. Zahtev za izradu i izradu korisničkog sertifikata može biti automatizovana procedura.

U samoj strukturi PKI predloženog rešenja upotrebljeni su kriptološki mehanizmi koji zahtevaju korišćenje simetričnih i asimetričnih ključeva, odnosno korišćena je kombinacija šifrovanja kriptološkim simetričnim ključem i digitalnog potpisivanja kriptološkim asimetričnim ključevima. Ova kombinacija je omogućila maksimalno

iskorišćenje prednosti šifrovanja simetričnim ključevima i načina autentifikacije asimetričnim kriptološkim ključevima.

Za šifrovanje je korišćen DES algoritam jer je nekoliko desetina puta brži od 3DES ili AES algoritma, zahvaljujući maloj dužini ključa (56 bita). Primenom DES algoritma je kompenzovano vreme šifrovanja u odnosu na veličinu kompresovanih fajlova koji su reda veličine od nekoliko kb pa do nekoliko Mb.

Sa predloženom novom PKI na lokalnom nivou postigli smo sledeće benefite:

- jednostavnost i društvenu prihvatljivost

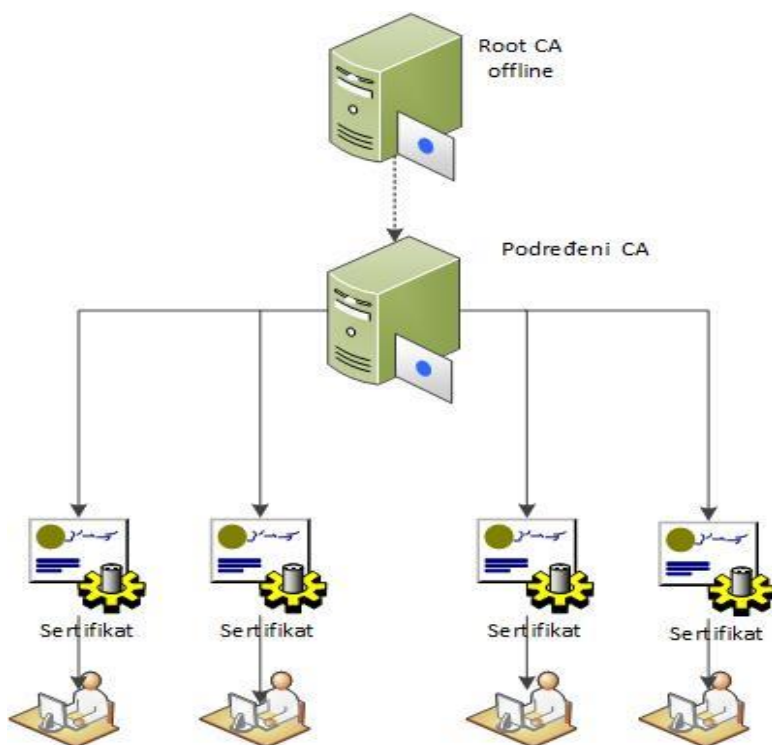
Predloženi PKI je jednostavniji za implementaciju u postojeće lokalno okruženje, a sa boljim performansama zaštite podataka i upravljanja. Postoji mogućnost implementacije na sva lokalna okruženja definisana u radu, te je iz tog razloga i društveno prihvatljiv.

- jeftinije rešenje

Posmatrano sa finansijskog aspekta potrebna su minimalna ulaganja u postojeće infrastrukturu jer se predviđa iskorišćenje postojećih resursa.

- vrhovni CA je ekvivalentno predstavljen na lokalnom nivou, a nad kojim imamo potpunu kontrolu
- bezbednosne performanse su uvećane
- uvedena je kompresija podataka koja pozitivno utiče na bezbednost, ali i negativno na vremenske performanse

Obzirom da se osnovna verifikacija izvršava na lokalnom nivou napravljen je vremenski kompromis, te na ovaj način dobijamo bezbedniju, jeftiniju PKI šemu sa približno istim vremenskim performansama.



Slika 4.6: Predložena arhitektura PKI

4.4 Evaluacija predloženog okruženja sa prikazom softverskog rešenja

Korišćenjem kompresije podataka pre algoritma za šifrovanje postižu se značajne prednosti iz dva razloga:

- Kriptoanaliza se oslanja na redudanse u otvorenom tekstu, a kompresija dokumenata pre šifrovanja umanjuje te redudanse, drugo
- Šifrovanje je proces koji traje, a kompresijom dokumenata pre šifrovanja ubrzava se ceo postupak

Prilikom utvrđivanja valjanosti metode predloženog rešenja kompresije u programskom okruženju MatlabR2012b, ideja vodilja je bila da se kao uzorci za kompresovanje fajlova odnosno dokumenata upotrebe najčešće korišćeni formati. Pri tome se vodilo računa o njihovim prosečnim veličinama u bajtovima. U poslovnom okruženju najviše cirkulišu dokumenta tekstualnog (Microsoft office aplikacije, notepad) i pdf formata. Cilj je bio prikazati da pomenuta funkcija za kompresiju podržava sve formate dokumenata bez obzira na vreme potrebno za izvršenje. Takođe, nisu se analizirali fajlovi različitih formata, a istih veličina, jer rezultati ne bi predstavljali realne potrebe kao ni približno zadovoljavajuću veličinu fajla koji bi bilo svrsishodno kompresovati.

Rezultati kompresije prikazani su u tabeli 4.2. Na primer, originalni video fajl u mp4 formatu veličine 8,747MB kompresovan je na veličinu 5,182MB što predstavlja očekivanu vrednost od oko 59% za video fajlove. Najbolje kompresovani fajlovi po veličini i vremenu kompresije su tekstualni i pdf fajlovi.

Tabela 4.2: Kompresovani fajlovi različitih formata

Format fajla	Originalna veličina	Veličina nakon kompresije	Vrednost kompresije u %	Vreme kompresije (00:00:00)
mp4	8,747 Mb	5,182 Mb	59,24	02:12:00
mp3	4,75 Mb	2,796 Mb	58,86	01:16:00
docx	777 kb	9 kb	98,84	00:05:00
pdf	1Mb	450 kb	45,00	00:43:00

4.5 Oblast primene predloženog rešenja

Predloženo rešenje PKI primenljivo je u lokalnim okruženjima sa već postojećim infrastrukturama lokalnih mreža, iako se može primeniti i u lokalnim okruženjima u izgradnji koja imaju potrebu za zaštitom dokumenata i autentifikacijom korisnika u svom poslovanju. Pri tome je neophodno prethodno osmisliti i definisati potrebu i politiku korišćenja digitalnih sertifikata, aplikacije i korisnike koji će ih koristiti, konfiguraciju CA, konfiguracije i planove upravljanja sertifikatima.

U lokalnim strukturama kao što su prosvetne ustanove, zdravstvene ustanove, kompanije, državne institucije i ostale institucije od značaja, postoji potreba za proverom autentičnosti korisnika i integriteta dokumenata koja se razmenjuju putem IT mreže.

Posebno je interesantna primena predloženog rešenja na male poslovne sisteme koja poseduju dokumenta sa strateški poverljivim informacijama. Svim poslovnim

sistemima ovakva PKI struktura pruža IT bezbednost sa minimalnim ulaganjima i mogućom studijom izvodljivosti.

5 Zaključak

5.1 Sumarni ciljevi rada i ostvareni rezultati

Cilj ovog rada je bio da se konfigurira PKI infrastruktura koja će obezbediti digitalno potpisivanje dokumenata sa sopstvenim CA i dodatna zaštita dokumenata za prenos u lokalnom okruženju.

Dopirinos ovog rada predstavljen je sa specifično konfigurisanom PKI infrastrukturuom na lokalnom nivou ili za primenu u manjim poslovnim okruženjima. Specifičnosti naše šeme se ogledaju u primeni dodatnih mehanizama koji poboljšavaju bezbednosne performanse sistema. Ova vrsta poboljšanja nije jednostavno primenjiva na globalnom nivou zbog svoje kompleksnosti koja prvenstveno zahteva neograničene hardverske reurse.

Prikazana PKI infrastruktura po konfiguraciji je manja od tradicionalne na globalnom nivou, a zahvaljujući primeni kriptoloških mehanizama poboljšana je zaštita dokumenata. Korišćenjem predložene infrastrukture postignuta je kontrola nad izdavanjem sertifikata bez zavisnosti poverenja od treće strane. Dodatna zaštita postignuta je korišćenjem mehanizma kompresije Hafmanovim kodovanjem koji je razvijen u programskom okruženju Matlab. Kompresovanje dokumenata je u globalnoj infrastrukturi opcionog karaktera i u skoro 98% slučajeva se ne koristi.

Postigli smo sledeće benefite:

1. kontrolu izdavanja sertifikata i broja korisnika,
2. tajnost koda koji nije dostupan javnosti,
3. pojednostavili metodologiju izdavanja sertifikata sa svesnim prihvatanjem rizika koji ovakvo rešenje donosi.

Način implementacije i aplikacije za generisanje sertifikata, serverske aplikacije kao što su Windows server 2008, aplikacije za elektronsku poštu, pdf dokumenta i kreiranje dokumenata, zatim način digitalnog potpisivanja dokumenata (Microsoft office paketi, Adobe Acrobat i Acrobat Reader) nisu razmatrane u ovom radu jer su to standardni paketi proizvođača koji podržavaju navedeni korisnički servis i za njih postoje detaljna korisnička uputstva.

5.2 Predlog za budući rad

Predloženo rešenje se odnosi na lokalno okruženje sa manjim brojem korisnika na osnovu koga je određena arhitektura i struktura PKI. Digitalno potpisivanje dokumenata sa sopstvenim CA za lokalna okruženja može se poboljšati primenom još jače autentifikacije korisnika kao i poboljšanjem performansi kompresije podataka.

Takođe, predmet budućeg rada podrazumeva uvođenje dvofaktorske autentifikacije korisnika i čuvanje tajnih ključeva na smart karticama, USB flash memorijama ili upotrebu token uređaja.

Razvoj tehnologije, okruženja na globalnom nivou i zahtevi poslovanja sve češće nameću kompanijama potrebu za izmeštanjem podataka, aplikacija pa čak i infrastrukture izvan njihovih lokalnih okruženja.

U zavisnosti od tehnološkog razvoja hardverskih komponenti, aplikacija i softvera nameće se razmatranje primene drugačije hardverske infrastrukture za serverske uređaje, kao i dodatno obezbeđenje poverenja u treću stranu ukoliko se pojavi potreba.

Literatura

- [1] Milica Kovinić (RCUB), „Uvod u kriptografiju i infrastrukturu javnih ključeva (PKI)“, © Copyright AMRES, 2010
- [2] FOX IT, Black Tulip, „Report of the investigation into the DigiNotar Certificate Authority breach“, Project no./Ref. no. PR-110202, Date 13 August 2012, Version 1.0
- [3] L. Kohnfelder, „Toward a Practical Public Key Cryptosystem“, Bachelor's thesis, MIT Department of Electrical Engineering, Maj 1978
- [4] S. Mrdović, „Izgradnja infrastukture javkih ključeva (PKI)“, magistarski rad 2004, Univerzitet u Sarajevu 2004.
- [5] M. Milosavljević / G. Grubor, *Osnove zaštite informacija*, Beograd: Univerzitet Singidunum, 2010.
- [6] Miloš Milenković, Saša Adamović, Marko Šarac, Dalibor Radovanović, „Upravljanje X.509 sertifikatima u PKI sistemu“, Naučno stručno savetovanje "ZITEH 2010", Beograd, Srbija, 2010.
- [7] M. Stamp, *Information security: principles and practice*, 2nd ur., New Jersey: John Wiley & Soons, 2011.
- [8] B. Schneier, *Primenjena kriptografija: Protokoli, Algoritmis i izvorni kod na jeziku C*, 2go izdanje., prevod Mikro knjiga 2007.
- [9] M. Veinović / S. Adamović, *Kriptologija 1*, Beograd: Univerzitet Singidunum, 2013.
- [10] S.R. SUBRAMANYA AND BYUNG K. YI, „Digital Signatures“, na internetu dostupno na: <http://www.cse.unr.edu/~bebis/CS477/Papers/DigitalSignatures.pdf>