Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-652-657

DIGITALNO POTPISIVANJE DOKUMENATA U LOKALNOJ MREŽI SA SOPSTVENIM CA

Branislav Kozma[1], Saša Adamović[2]
[1]Institut za virusologiju, vakcine i serume Torlak, Beograd
[2]Univerzitet Singidunum, Beograd

Abstract:
Rad se bavi dizajniranjem sopstvenog rešenja za digitalno potpisivanje dokumenata koji se razmenjuju u lokalnom okruženju. Na osnovu teorijskog pregleda tradicionalne šeme PKI infrastrukture, napraviće se nova generička šema 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 predstavljenog rešenja ukazaće se 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.

Key words:
digitalno potpisivanje,
CA,
lokalna mreža,
PKI.

UVOD

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* (engl. *Public Key Infrastructure, PKI u daljem tekstu*) 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, postoje primeri permanentnog narušavanja 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.

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 i literatura ([1], [3], [4], [5], [6], [7], [8], [9], [10]). 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 infrastrukturama, npr. ugradnja registra opozvanih sertifikata u digitalno potpisani dokument
- Problem razmene ključeva preko mreže je stalno aktuelan
- Vreme potrebno da se kriptoanalizom 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 certifikati kako bi se obezbedila autentifikacija korisnika, zaštita podataka i neporecivost poslatih informacija.
- *PKI* 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].

Validnost sertifikata može biti opozvana iz brojnih razloga, a osnovna uloga poverenja u sertifikaciona tela CA (engl. *Certificate Authority, CA u daljem tekstu*) kompromitovana. 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 [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.

Prednosti i nedostaci globalne i lokalne ingfrastrukture javnih ključeva

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 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.

Prednosti i nedostaci lokalne u odnosu na globalnu infrastrukturu javnih ključeva ogledaju se u sledećem:

- Upravljanje rizikom. Poznat je način i broj korisnika, jer je izdavalac sertifikata sopstveni *CA*. Postojanje tajnosti koda koji nije dostupan javnosti. Pretpostavka da je kod bezbedan. U ovom slučaju uvek će postojati nesigurnost u bezbednost koda i *PKI*.
- Certifikat se izdaje kome korisnik želi, a sa spoljnim korisnicima vrši se uzajamno sertifikovanje. Nedostatak je veliki teret na pojedinačnog korisnika u mreži.
- Direktna procena i prihvatanje gubitaka usled kompromitovanja.
- Metodologija lakog dodeljivanja *CA* sa kompromisom na dužu realizaciju u odnosu na eksternu *CA*.
- Troškovi implementacija sa finansijskog aspekta su relativno manji.

Razvoj tradicionalne ingfrastrukture javnih ključeva i kriptoloških mehanizama

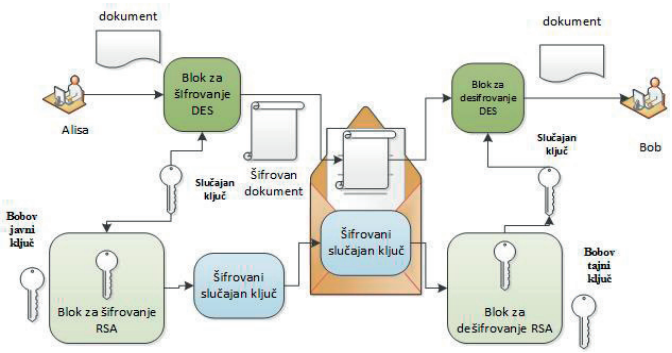
Simetrična kriptografija koristi isti ključ za šifrovanje i dešifrovanje. Jednostavna je za korišćenje i implementaciju, algoritmi su brzi, ali se pojavljuju dva osnovna problema: razmena podataka nije bezbedna, odnosno nema pouzdane autentifikacije korisnika, a drugo broj potrebnih ključeva, višestruko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

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.

Kombinacija asimetričnog *RSA* algoritma sa tajnim i javnim ključem i simetričnim algoritmom *DES* za šifrovanje poruke poznata je kao digitalni koverat [11].

Na primer, 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 Sl. 1 – Digitalni koverat je prikazan scenario.



Sl. 1 – Digitalni koverat

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 i dekompresija. Pri tom se podrazumeva da je bezbedna veza preko SSL protokola uspostavljena i da je sesijski ključ razmenjen (Sl.2.)

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

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 su postignute dve stvari, prvo smanjena je veličina dokumenta na očekivanu vrednost, a drugo postignute su izmene originalnog dokumenta tako da nije prepoznatljiv.

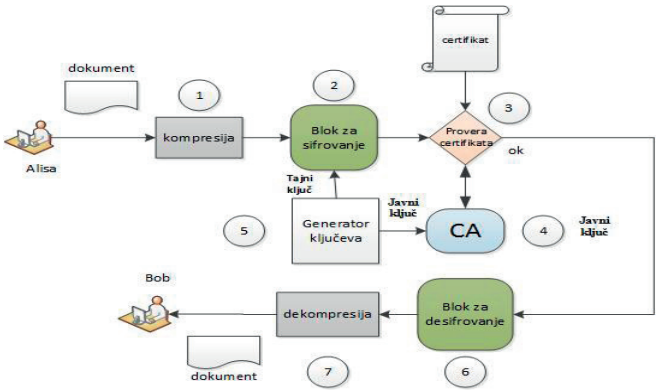
U narednom koraku kompresovani dokument se hešuje tako da ako bi došlo do najmanje promene u kompresovanom dokumentu odnosno poruci, promenio bi se i rezultujući heš poruke. Hešovana poruka se šifruje sa simetričnim algoritmom sa režimom.

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.

Nakon provere identiteta primalac poruke dešifruje 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.

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.



Sl.2 – Generička šema razmene dokumenata

Detaljna analiza generičke šeme sa diskusijom scenarija komunikacije i primene u praksi predstavljena su na Sl.3 i Sl. 4.

Alisa traži zahtev za bezbednu komunikaciju – Cipher Suites

Dobija Cipher Suites zajednički za oboje i Bobov sertifikat

Alisin zahtev za Bobovim sertifikatom upućuje *CA*

CA šalje sertifikat

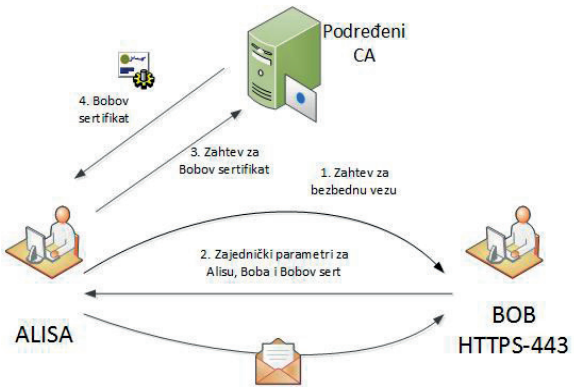
Alisa šifruje kompresovanu poruku sa *DES*, a sesijski ključ šifruje Bobovim javnim ključem.

Šifrovanu poruku i potpisani ključ šalje zajedno kao digitalni koverat Bobu.

Bob proverava *hesh* vrednost poslatog koverta, dešifruje sa svojim tajnim ključem da bi uzeo sesijski ključ i proverava koverat na integritet.

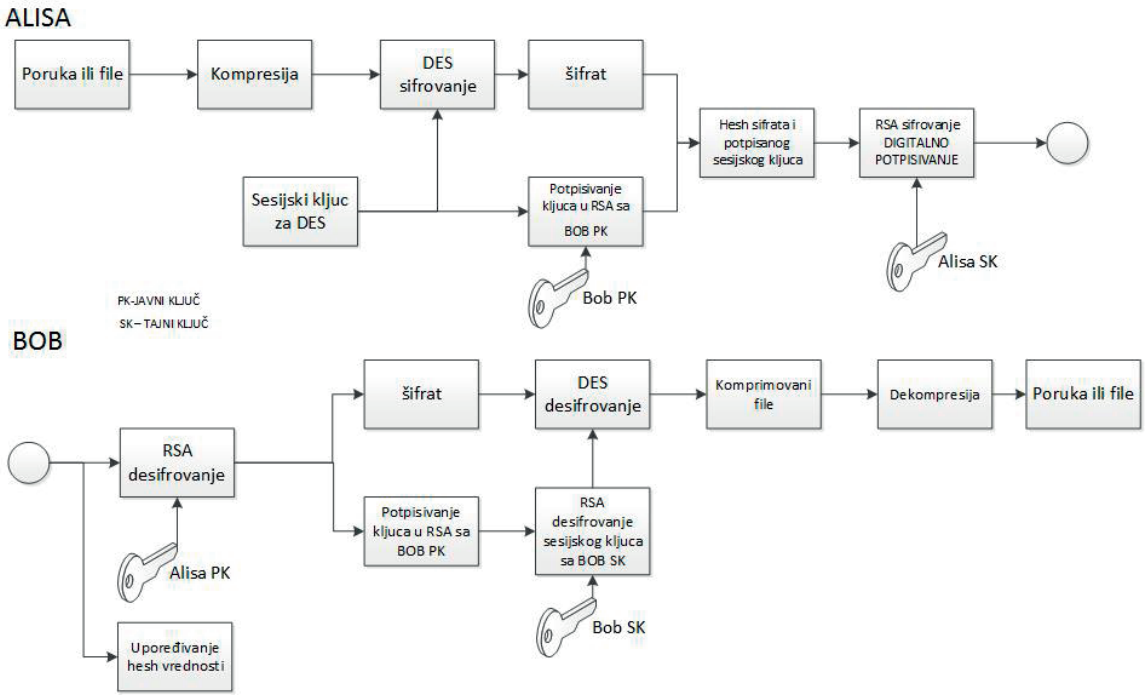
Bob otvara poruku sa sesijskim ključem.

Na ovaj način je obezbeđeno da se tajni ključevi korisnika ne prenose preko mreže, a da u slučaju opstrukcije razmene od strane napadača, nije moguće doći do sesijskog ključa za dešifrovanje poruke, što je prikazano na Sl.3.



Sl.3 – Šema razmene na bezbednom nivou

S obzirom da je komunikacija zaštićena preko *SSL* protokola, a distribucija sertifikata nije deo ovog protokola, na sledećoj šemi je dat princip razmene dokumenata sa korišćenjem ključeva iz sertifikata (Sl. 4).



Sl. 4 – Detaljna šema algoritma digitalnog potpisivanja dokumenta

Postavka i objašnjenje eksperimentalnog okruženja

Za potrebe pretvaranja u binarni niz i kompresovanja dokumenata 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*).

U programskom okruženju Matlab R2012b 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
- hafmanova tabela za svrhu dekodovanja i na kraju,
- kompresovan fajl.

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. Za digitalno potpisivanje dokumenata korišćen je standardno korišćeni u svetu *RSA* algoritam, a za simulaciju asimetričnih ključeva upotrebljen je generisani sertifikat korisnika.

Na osnovu analize minimalnih zahteva bezbednosti i detaljnog uvida u *TPKI* definisanih u poglavlju II. utvrđeno je da korisnici u lokalnom okruženju imaju najviše potrebu za sigurnom e-mail komunikacijom, bezbednom autentifikacijom 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.

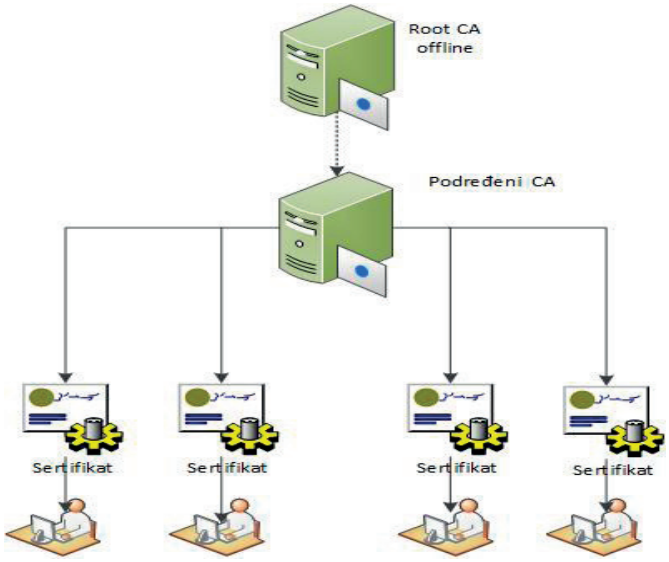
Drugi razlog je od strateškog značaja da li je korisniku potrebno visoko arbitražno sertifikaciono telo prihvaćeno od celog sveta u svrhu bezbedne komunikacije sa zaposlenima ili klijentima. Komunikacija sa spoljnim klijentima izvan lokalnog okruženja moguća je međusobnom sertifikacijom između dva domena.

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 Sl. 5 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 izrada 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.



Sl. 5 – Predložena arhitektura PKI

Sa predloženom novom *PKI* na lokalnom nivou postižu se sledeći benefiti:

- jednostavnost i društvena 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 infrastrukture 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.

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 redundanse u otvorenom tekstu, a kompresija dokumenata pre šifrovanja umanjuje te redundanse, 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 analizirani fajlovi različitih formata, a istih veličina, jer rezultati ne bi predstavljali realne potrebe kao ni približno zadovoljavajuću veličinu fajla koje bi bilo svrsishodno kompresovati.

Rezultati kompresije prikazani su u Tabela III.1. 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 III.1 - 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

ZAKLJUČAK

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

Doprinos ovog rada predstavljen je sa specifično konfigurisanom *PKI* infrastrukturom na lokalnom nivou ili za primenu u manjim poslovnim okruženjima. Specifičnosti predstavljene 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 resurse.

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.

Postiti su sledeći benefiti:

1. kontrola izdavanja sertifikata i broj korisnika,
2. tajnost koda koji nije dostupan javnosti,
3. pojednostavljena metodologija 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.

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 dvo faktorske autentifikacije korisnika i čuvanje tajnih ključeva na *smart* karticama, *USB flash* memorijama ili upotrebu token uređaja.

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 javnih 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, Algoritmi i izvorni kod na jeziku C, drugo izdanje., prevod Mikro knjiga 2007.

[9] M. Veinović / S. Adamović, Kriptologija 1., Beograd: Univerzitet Singidunum, 2013.

[10] M. Milosavljević, S. Adamović, Kriptologija 2., Beograd, Univerzitet Singidunum, 2014.

[11] S.R. SUBRAMANYA AND BYUNG K. YI, „Digital Signatures“, na internetu dostupno na: http://www.cse.unr.edu/~bebis/CS477/Papers/DigitalSignatures.pdf

DIGITALLY SIGNING DOCUMENTS WITH OWN CA IN THE LOCAL NETWORK

Abstract:
In this paper, will be designed 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.

Key words:
digital signature,
CA,
local network,
PKI.