SIGURNOSNI PROTOKOLI U E-BANKARSTVU

Almedina Hatarić, MA, email: almedina_tr@hotmail.com,
Imran Kasumović-student, email: imran.kasumovic@gmail.com
Internacionalni univerzitet Travnik u Travniku, Bosna i Hercegovina

Sažetak: Sigurnost informacionog sistema obuhvata radnje, mjere i postupke u cilju zaštite podataka i informacionog sistema od nepredvidivih događaja sa neželjenim posljedicama. U tom smjeru je i sve veća potreba za onemogućavanjem svakog slučajnog ili namjernog narušavanja i sprječavanja funkcija računarskih sistema. Također, treba stvoriti i neophodne uslove za pravilno korištenje unaprijed definisanih funkcija informacionih sistema. Kao osnova za nalaženje zadovoljavajućeg odgovora na pitanje zaštite informacionih sistema, polazimo od klasifikacije prijetnji koje mogu ugroziti isti na: nesreće, greške i kriminal.
Na bazi navedene klasifikacije data su četiri odgovora na pitanja gdje se dobija djelimičan odgovor, a njihovom sintezom i potpuniji odgovor:

- vrijednost hardvera i softvera;
- raznovrsnost funkcija računarskih sistema;
- karaketristike računarskih sistema.

Najprije je potrebno definisati cilj zaštite sistema, da bi bilo koji sistem zaštite ima smisao samo ukoliko se nešto, od nečega i zbog nečega štiti, a da bi se isti postigao mora se na funkciju izvršavati sa nečim i na neki način. Rješenje ovako postavljenih ciljeva, odnosno pitanje je moguće uz logičke cjeline, a po principu "zlatnih pitanja" kriminalistike, kroz odgovarajuća "zlatna pitanja" informatičke zaštite i koja zahtjevaju potpune odgovore.
Ključne riječi: Protokol, sigurnost, informacioni sistem, bankarstvo, tehnologije

SAFETY PROTOCOLS IN E-BANKING

Abstract: Safety Information System includes actions, measures and procedures in order to protect data and information system from unforeseen events with undesirable consequences. In this direction is the increasing need for disabling any accidental or deliberate distortions and prevent the functions of computer systems. We should also create the necessary conditions for the proper use of predefined functions of information systems. As a basis for finding a satisfactory answer to the question of protection of information systems, we start from the classification of threats that can jeopardize the same accident, crime and error.
On the basis of this classification,there are given four answers to questions where a partial response is received, and by their synthesisis receiveda fuller response:

- the value of hardware and software;
- versatility of computer systems;
- characteriatics of computer systems.

First, it is necessary to define the purpose of the protection system, that any system of protection has meaning only if something, somewhere, and for some reason needs to be protected, and in order to achieve the goal, we need to execute something in some way on the function. The solution of these set goals is that question is possible with logical units, and according to the "golden questions" of criminology, the corresponding "golden questions" of information protection and which require full answers.
Keywords: Protocol, security, information systems, banking, technologies

1. UVOD

Elektronsko poslovanje je savremeni oblik organizacije poslovanja koji podrazumijeva intenzivnu primjenu informatičke i posebno internetske tehnologije.Elektronsko poslovanje je vođenje poslova na Internetu, što ne podrazumijeva samo kupovinu i prodaju, nego i brigu o klijentima i poslovnim partnerima, kao i organizaciju poslovanja u svojoj firmi online i organizaciju poslova prema klijentima.
lz navedene definicije se vidi da osnovu za elektronsko poslovanje čine informaciono komunikacione tehnologije koje se stapaju u Internet koji čini globalnu multimedijalnu infrastrukturu. Današni razvoj Interneta omogućio je nove dimenzije organizacionih i poslovnih procesa koji nastaju stvaranjem mogućnosti koje pružaju:

- Nov, interaktivan način za pristup tržištu i poslovnim partnerima, kako na lokalnom tako i na globalnom nivou.
- Mogućnost obavljanja odredenih poslovnih procesa van preduzeća.
- Dostupnost mnoštvu informacija, sa moćnim elementima pretraživanja i automatskom analizom.
- Novi modaliteti poslovnog udruživanja, finansijskih transakcija i obavljanja poslovnih procesa.

Poslovanje je oduvijek zavisilo od tehnologije, medutim to je danas izraženije više nego ikad. Moglo bi se reći da tehnologija danas upravlja cjelokupnim ljudskim životom i radom, a ne samo proizvodnim pogonima i uslužnim djelatnostima. Tehnologija je izmijenila način na koji danas obavljamo poslove, samu prirodu poslova i razloge zbog kojih ih obavljamo. Danas klijenti žele pristup proizvodima i uslugama u svako doba 0 - 24 sata na dan. Firme koje omoguće najfunkcionalniji, najpouzdaniji i korisniku najprilagodeniji proizvod ili uslugu imaju najveće izglede za uspjeh u dugom roku. Ulaganje u tehnologiju je neminovno kako bi se iznalazio način za stvaranje novih poslovnih mogućnosti, pariranju trendovima skraćivanja životnog ciklusa proizvoda, te bržem osvajanju novih tržišta. Poslovanje se kreće u nekad nezamislivim smjerovima i obavlja na načine koji se nisu mogli ni pretpostaviti u bližoj prošlosti. Najbolji primjer koji ovo potvrduje je upravo Internet koji danas odreduje poslovnu strategiju u najvećim svjetskim kompanijama, ali i u onim malim koje su svjesne kako njegovih prednosti u primjeni, tako i neminovnosti za tu primjenu, a sve u cilju održivosti u biznisu.

Područja u kojima se najčešće primjenjuje elektronsko poslovanje:

- online prodaja vlastitih dobara i usluga,
- elektronsko trgovanje,
- online zabava i rekreacija,
- elektronsko bankarstvo i online finansijske transakcije i
- elektronsko izdavaštvo.

2. INTERNET KAO PLATFORMA ELEKTRONSKOG POSLOVANJA

Intemet je globalna multimedijalna mreža koja povezuje računare širom svijeta. Sastoji se od

infrastrukture mrežnih servera i komunikacijskih kanala između njih koji se koriste za transport informacija između klijentskih PC-ja i WEB servera, kao i izradu samih servera.
Intemet je mreža svih mreža koje sve međusobno komaduju na dogovorenom jeziku koji se zove protokol. Taj protokol je poznat pod imenom TCP/IP (Transmission Control Protokol/Intemet Protokol). Postoji doslovno na milione mreža koje su povezane na Intemet, a on i dalje neprestano raste.

Temeljni koncept djelovanja intemeta je klijent/server arhitektura. Taj koncept je zasnovan na tome da bilo koji korisnik može da zahtijeva od mrežnog servera neku uslugu, a taj mu je server pruža, ukoliko on ima pravo pristupa toj usluzi. Svaki računar unutar mreže, koji ima u svojim memorijama neke podatke koje može "želi" pružiti drugim korisnicima na mreži, naziva se serverom.

Dok na drugoj strani svaki korisnički uređaj (npr. korisnički PC ili radna stanica u lokalnoj mreži) koji može zatražiti i prihvatiti podatke od nekog servera naziva se klijentom. Najznačajnije obilježje klijentsko/serverske arhitekture je to što korisnici ne moraju voditi brigu o tome gdje se u mrežnom sistemu tražena informacija nalazi, u kojem je obliku memorisana i kojim će komunikacionim putevima (telekomunikacionim linijama) doći do njega. Ono što klijent treba da zna je to da postoje mnogi standardni i nestandardni mrežni (intemet) servisi (usluge) pomoću kojih će inicirati traženje i dobijanje informacija, odnosno obavljanje nekog informacionog posla (prenosa i obrade podataka).

3. SIGURNOST U E-POSLOVANJU

Sigurnost podataka i prenos podataka je star problem. Najjednostavniji oblik bi mogao biti došaptavanje - infomiaciju dobiva samo jedna osoba i drugi ne znaju sadržaj poruke. Prednost je jednostavnost, a mana je kratka udaljenost na koju se takvim načinom poruka može prenijeti. Pojavom pisma otvorile su se nove mogućnosti, prije svega slanje poruka po glasniku na, za ono vrijeme, proizvoljne udaljenosti.

Najveća je primjena bila u vojne svrhe, a to je donijelo i veću opasnost za glasnika i za poruku. Glasnika je mogla spasiti velika brzina ili borbena vještina, ali kada je jednom savladan onda poruka dospijeva u ruke neprijatelju. Jednostavni trik Rimljana je bio da se poruka napiše na traci koja je omotana oko štapa tačno određenog promjera, pa su takvu poruku mogli razumjeti samo vlasnici takvog štapa. Neprijatelj je dobio samo traku s nerazumljivim redosljedom znakova, a poruku nije znao čak ni glasnik.

Kad se jednom sazna da je poruka zaštićena na taj način, isprobavanjem se relativno lako može doći do štapa odgovarajuće veličine. Drugi način je, na primjer, svako slovo zamjeniti nekim drugim. Primalac i pošiljalac poruke moraju imati istu tablicu zamjena kako bi poruku mogli napisati, odnosno pročitati. Ko nema tablicu može isprobavati, ali za trideset slova ima čak 30! (faktorijel) mogućih tablica.

Mana ovakvog načina zaštite je da se nekako mora poslati i tablica, pa ako neprijatelj ima sreću da je presreo glasnika s tablicom može ubuduće pročitati sve poruke. Štaviše, može sam

napisati šifrovanu poruku, pa poslati lažnog glasnika. Ako primalac poruke poznaje rukopis, barem potpis pošiljaoca, znaće da je poruka lažna. lsto tako može zatražiti od glasnika da se identifikuje, na primjer, posebnim prstenom medaljonom, a najbolje ličnom potvdom. Pojavom masovnihkomunikacija, posebno intemeta, potreba za zaštićenim prenosom je naglo porasla. Sada je potreban, ne samo generalima i vladarima, nego i poslovnim ljudima, i običnim građanima. Bilo da je riječ o vojnoj industrijskoj tajni, broju kreditne kartice ljubavnom pismu, zaštita podataka je postala svakodneva potreba. Kako uglavnom ne znamo kojim putem putuju naši podaci i kroz čije ruke prolaze, zaštićeni prenos podataka je neophodan za svaki posao gdje se traži tajnost privatnosti.

3.1. SSL protokol

Secure Sockets Layer (SSL) je protokol za sigumo slanje poruka (komuniciranje) putem Inteneta, koji omogućuje slanje povjerljivih podataka (npr. broj kreditne kartice) putem Inteneta u šifrovanom i sigumom obliku. SSL protokol ostvaruje poseban komunikacioni sloj, koji je smješten na pouzdan transportni sloj (npr. TCP/IP), dok se na SSL smješta aplikacijski sloj.

Od aplikacijskog sloja prima poruku koju treba poslati, rastavi je u manje dijelove prikladne za šifrovanje, dodaje kontrolni broj, šifruje, eventualno kompresuje, a zatim te dijelove pošalje. Primalac primi dijelove, dekompresuje, dešifruje, provjeri kontrolne brojeve, sastavi dijelove poruke, pa ih preda aplikacijskom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mrežu. Ukoliko su klijent i server neaktivni duže vrijeme ili razgovor sa istim atributima zaštite potraje predugo, atributi se mijenjaju.

SSL protokol je dizajniran i napravljen od Netscape Communications korporacije, da bi bio korišten sa Nescape Navigatorom. Prva verzija, 1.0, je razvijena 1994. godine, međutim, to je bila samo probna verzija korištenja unutar ove korporacije. Verzija 2.0 je bila prva koja je izdata u javnost i koja je isporučivana sa Netscape Navigatorom, verzijama 1 i 2.

SSL protokol je stvoren kao odgovor rastućim zahtjevima za zaštićeni prenos podataka na Internetu. Zbog pravovremenog nastanka, te zbog tržišne uloge preduzeća Netscape Communications, stvaraoca ovog protokola, SSL je postao vrlo rasprostanjen. SSL osim što je odobren kao standard od strane www consortiuma (www.w3.org) postao je de facto standardom.

Uz SSL razvijala su se i druga rješenja koja ostvaruju zaštićeni prenos podataka kroz mrežu. Uspješnost SSL-a dodatno je naglašena nedostatkom drugih dovoljno dobrih rješenja koja bi ga zamjenili. S-MIME je jedno od drugih rješenja.

3.1.1. S-MIME

Secure-MIME protokol je razvila RSA i dodatak je već postojećem MIME protokolu. Koristi sistem javnih ključeva kao osnovu za provjeru ispravnosti i šifrovanje. Algoritmi za šifrovanje i rad sa potvrdama identični su onima korištenim u SSL-u, tako da se iste potvrde mogu koristiti i u ovom protokolu. Korisnicima MIME-a, SMIME omogućava zaštitu

identičnu u ovom radu opisanoj zaštiti koju pruža SSL.

4. SISTEM JAVNIH KLJUČEVA

Kroz računare koji se nalaze na Intemetu, kontinuirano prolaze brojni podaci, i u normalnim situacijama vlasnici tih računara ne provjeravaju njihov sadržaj. Ali mnogo je podataka koji zahtjevaju zaštitu od opasnosti koje vrebaju sa globalne mreže. Sa zadatkom zaštite podataka u takvim uslovima, uspostavljena je tehnika zvana sistem javnih ključeva (*Public Key Criptography*), koja ostvaruje sljedeće zadatke zaštite: **Šifrovanje** i **dešifrovanje** (*encryption and decryption*) dozvoljavajuda dva učesnika u komunikaciji sakriju sadržaj koji šalju jedan drugome. Pošiljaoc šifruje podatke, prije nego ih pošalje, dok ih primalac dešifruje, nakon što ih primi.

Šifrovanje predstavlja proces transformacije podataka u oblik nerazumljiv svima osim predviđenim primaocima. **Dešifrovanje** je obrnut proces, transformacijašifrovanih podataka u razumljiv oblik. Algoritam za šifrovanje određen je prikladnom matematičkom metodom. Često se koriste dvije povezane metode, jedna za šifrovanje, a druga za dešifrovanje. U najnovijm metodama za šifrovanje koristi se niz alfanumeričkih znakova, koji se nazivaju ključ, koji koriste algoritam kako bi se podaci šifrovali. Dešifrovanje sa odgovarajućim ključem je jednostavno, dok je bez njega vrlo složeno, odnosno, najčešće nemoguće za sve praktične primjene. Odvajanjem algoritma od ključa, omogućuje da svi budu upoznati sa algoritmom, ali bez ključa podaci su i dalje nerazumljivi.

4.1. Dužina ključa i snaga zaštite

Snaga zaštite zavisi od složenosti otkrivanja ključa. Najjednostavnije je ključ direktno nabaviti od vlasnika, krađom ili nekim načinom prisile uvjeriti ga da nam ga da. Takvim tehnikama dolazimo u opasnost da budemo identifikovani i ugrožavamo sebe. Drugi način je izračunati ključ na osnovu šifrovanih podataka, koji slobodno prolaze kroz mrežu. Složenost tog zadatka zavisi od dužine ključa i algoritma za šifrovanje. Snaga zaštite je često opisana dužinom ključa koji se koristi, pa uopšte vrijedi sljedeće: duži ključ - bolja zaštita.

Dužina ključa se mjeri u bitovima. Tako kod upotrebe SSL protokola se može naći i korištenje 40- bitnog ključa, ali i 128-bitnog, koji daje znatno bolju zaštitu šifrovanja sa istim algoritmom. Algoritmi koji se koriste su zasnovani na matematičkim metodama čija je karakteristika da otežavaju, gotovo onemogućuju, dešifrovanje bez poznavanja ključa. Različiti algoritrni za šifrovanje mogu zahtjevati različite dužine ključeva.

4.2. Potvrde

Potvrda (certificate) je elektronski dokument koji identifikuje pojedinca, računar, preduzeće ili neki drugi entitet koji posjeduje privatni ključ. Potvrda uz ime entiteta sadrži i njegov javni ključ. Kao što se lična karta, vozačka dozvola ili neki drugi dokument koriste za identifikaciju, tako i potvrde u računarski komunikacijama pružaju dokaz o identitetu odgovarajućeg entiteta.

Potvrde se koriste sa ciljem zaštite od imitiranja, predstavljanja kao neko ko taj entitet zapravo nije. Dobijanje potvrde zasnovano je na istom konceptu kao i potvrde u realnom svjetu - moraju se zadovoljiti određeni uslovi. Za dobijanje lične karte se moramo prijaviti policiji da utvrde naš identitet, uzmu otisak prsta, adresu stanovanja i odrede vrijeme važenja lične karte.Ako se želi dobiti vozačka dozvola, mora se prvo položiti vozački ispit kako bi se dokazala sposobnost vožnje vozila odgovarajuče kategorije.

Rad sa digitalnim potvrdama kakve koristi SSL protokol organizovan je na vrlo sličan način. Kao što svaka osoba u svom novčaniku ima različite isprave (potvrde) za različite namjene (lična, zdravstvena, vozačka...), tako i za identifikaciju preko mreže, u skladu s namjenom, koriste se odgovarajuće potvrde. lzdavaoci potvrde su institucije, koji provjeravaju identitet drugih entiteta i izdaju potvrde o tome.

To mogu biti ili nezavisni subjekti u komunikaciji dva entiteta, dakle treća osoba, ili sam subjekat u komunikaciji koji ujedno i izdaje potvrde (npr. banka provjerava identitet svojih klijenata vlastitim potvrdama). Metoda kojom će se provjeravati identitet zavisi od politike poslovanja određenog izdavaoca potvrde, baš kao što je i različit način u realnom svijetu - zavisi od njene upotrebe. U svakom slučaju, prije izdavanja potvrde, njen izdavalac mora provesti svoju proceduru provjere identiteta onoga kome je izdaje. Ta se procedura objavljuje kako bi svako ko takvu potvrdu primi mogao ustanoviti, da li je to dovoljno siguma metoda za njegove potrebe.

Značaj digitalnog potpisa uporediv je sa značajem svojeručnog potpisa koji se koristi za potpisivanje papimih dokumenata. U nekim situacijama digitalni potpis može bitiispravan kao i svojeručni potpis. Uz javni ključ i ime identiteta, potvrda sadrži datum do kojeg je potvrda važeća, ime izdavaoca potvrde, serijski broj i još neke podatke. I sama potvrda koja putuje po mreži može biti objekat napada. Zato je i sama digitalno potpisana. Kako izdavalac potvrde uživa naše povjerenje, svim ponudama potvrdakoje izdaje se može vjerovati.

4.3. Metode provjere identiteta

U komunikaciji podacima provjera identiteta uključuje pouzdanu međusobnu identifikaciju dva subjekta u komunikaciji. To je moguće učiniti na više načina, gde je upotreba potvrda jedna od njih. U mrežnom okruženju komuniciraju najčešče klijent (npr. neki komunikacioni softver na personalnom računaru) i server (npr. softver i hardver koji sadrže web stranice). Identifikacija klijenta se odnosi na potvrđivanje identiteta klijenta od strane servera, odnosno provjeravanje osobe za koju se pretpostavlja da koristi softver klijenta. Identifikacija servera odnosi se na potvrđivanje identiteta servera od strane klijenta, odnosno identifikaciju organizacije za koju se pretpostavlja da je odgovorna za server (na odgovarajućoj mrežnoj adresi).

Identifikacija klijenta jedan je od osnovnih elemenata sigumosti u komunikacijskojmreži. Postoje dva tipa identifikacije klijenta:

4.3.1. Identitikacija pomoću lozinke (password)

Vrlo je česta identifikacija klijenta od strane servera pomoću imena i šifre. Time korisnik dobija pristup serveru. Server održava listu imena i šifri, te ako je neko ime na listi i korisnik upiše ispravnu šifru, odobrava se pristup serveru. Identifikacija pomoću potvrde. Ova identifikacija je dio SSL protokola. Klijent digitalno potpiše slučajno odabrane podatke, te pošalje potvrdu i potpisane podatke kroz mrežu. Server koristi spomenute tehnike da potvrdi identitet klijenta.

Ukoliko je potvrda ispravna to je serveru dokaz o identitetu klijenta, pa time i korisnika. Kao i kod identifikacije pomoču šifre, u ovom prikazu pretpostavlja se da korisnik vjeruje serveru, da server ima pristup traženom resursu i da je server zatražio identifikaciju klijenta prihkom odobravanja pristupa zatraženom resursu. Također, se pretpostavlja da klijent ima važeću potvrdu.

4.3.2. Identifikacija pomoću potvrda

Identifikadja pomoću potvrda smatra se prikladnijom od identifikacije na osnovu lozinke jer se bazira na:

- nečemu što korisnik poseduje (privatni ključ);
- nečemu što korisnik zna (šifru kojom čuva svoj privatni ključ);

Vrlo je slično identifikaciji osoba na bankomatu, gdje korisnik mora imati karticu i znati tajni broj. Međutim, potrebno je naglasiti kako su te dvije pretpostavke istinite samo ako su korisnikov računar i šifra zaštićeni od neautorizovanogpristupa. Šifra je potrebna za pristup privatnom ključu koji čuva klijentski softver.

4.4. Vrste potvrda

Postoji više vrsta potvrda. Potvrde je moguće koristiti i u drugim situacijama, ne samo u okviru SSL protokola, ali njihova upotreba izlazi izvan okvira ovog rada.

4.4.1. Klijentske SSL potvrde

Koriste se za identifikaciju klijenta putem SSL protokola. Uobičajeno je poistovjećivanje identiteta klijenta sa osobom. Osim za identifikaciju osoba kod pristupa serveru, klijentska potvrda se može koristiti i u druge svrhe, npr. za digitalno potpisivanje digitalnih formulara.

Primjeri:

1. Banka daje korisniku klijentsku SSL potvrdu koja omogućuje serveru banke identifikaciju korisnika i dozvoljava korištenje bankovnog računa.
2. Preduzeće može dati svakom novom zaposlenom klijentsku SSL potvrdu, kojom je moguće dobiti pristup serveru preduzeća.

4.4.2. Serverske SSL potvrde

Koriste se za identifikaciju servera od strane klijenta putem SSL protokola. Identifikacija servera je obavezna u SSL protokolu za ostvarivanje zaštićenog prenosa podataka dok identifikacija klijenta nije. Primjer: Intemet poslovanje, npr. on-line prodavnice, najčešće koriste identifikaciju servera preko serverskih SSL potvrda kako bi uspostavili zaštićenu SSL vezu i ubijedilikorisnika da je to odgovarajuće preduzeće sa kojim korisnik želi poslovati. Šifrovana SSL veza osigurava da osjetljivi podaci koji se šalju kroz mrežu, kao što su brojevi kreditih kartica, budu zaštićeni.

4.4.3. Potvrde izdavaoca potvrda

Koriste se za identifikaciju izdavaoca potvrda. Klijentski i serverski softver koristi potvrde izdavaoca potvrda da ustanovi kojim drugim potvrdama se može vjerovati. To pojednostavljuje rad i klijentu i serveru, jer dovoljno je administrirati rad sa samo jednim izdavaocem potvrda, a može se pristupati serverma čije su potvrde u sklopu sistema tog jednog izdavaoca potvrde. Primjer potvrde izdavaoca potvrda koje čuva klijent odlučuju kome će klijent vjerovati. Administrator informacionog sistema unutar preduzeća može organizovati sigunosnu politku u komunikaciji na osnovu potvrda kod svakog korisnika u preduzeću. Primjeri drugih vrsta potvrda su S/MIME potvrde koje služe za digitalno potpisivanje i šifrovanje elektronske pošte, zatim potvrde za potpisivanje objekata koje mogu poslužiti kao potvrda da je softver poslan preko Intemeta stvamo proizvod odgovarajućeg preduzeća.

4.5. Sadržaj potvrde

Sadržaj potvrde koja se koristi u SSL protokolu organizovan je prema X.509 v3 specifikaciji za potvrde izrađene od strane ITU. Korisnici se ne moraju previše opterećivati sadržajem potvrde, jer baratanje njima najčešće ide automatski. Osnovni zadatak potvrde je da potvrdi vezu između javnog ključa i određenog entiteta (*npr. osobe ili preduzeća*) određenog sopstvenim imenom. Tako je jedan od važnijih podataka naziv nosioca potvrde (*distinguishedname*). Naziv nosioca potvrde je struktuirani niz atributa koji jedinstveno opisuje entitet koji potvrda identifikuje.

Tipična potvrda: Svaka X.509 potvrda se sastoji od dva dijela: s podacima i s potpisom.

Dio sa podacima sadrži:

- Serijski broj potvrde koji je jedinstven za svaku potvrdu izdanu od tog izdavaoca potvrde.
- Podaci o korisnikovom javnom ključu, koristeći algoritam i sam ključ.
- Ime izdavaoca potvrde (struktuiran kao i ime nosioca potvrde).
- Period važenja potvrde (npr. između 1:00, 15.11.1998 i 1:00, 15.11.1999.).
- Ime entiteta, nosioca potvrde.
- Dodatni, neobavezni, podaci mogu pružiti korisne podatke bilo klijentu bilo serveru.

Dio sa potpisom potvrde sadrži:

- Algoritam za šifrovanje, koji koristi izdavaoc potvrde za svoj digitalni potpis.

- Digitalni potpis, napravljen na osnovu kontrolnog broja dobijenog iz svih podataka u potvrdi, šifrovan privatnim kijučem izdavaoca potvrde.

5. ZAKLJUČAK

Informacione tehnologije predstavljaju veoma važan faktor (resurs) u procesu strateškog pozicioniranja preduzeća. Proces tranzicije koji u sebi sadrži i procese globalizacije i integracije tržišta obezbjeđuje preduzećima sa našeg područja da izlaze na inostrano tržište, ali istovremeno i otvara granice naše zemlje za priliv stranog kapitala, investicija i proizvoda. U takvom okruženju preduzeća se, kao i sama zemlja i privreda, moraju transformisati. Veliki broj informacija mora se obezbjediti menadžment timu preduzeća da bi se procesi u preduzeću odvijali na optimalnom nivou.

Poznavanje problema zaštite infonnacionih sistema kroz objekte zaštite, prijetnje, posljedice, mjere i rizike su preduslov za uspješnu organizaciju sigurnosti samog infonnacionog sistema od strane lica koja se bave ovom problematikom.

Uglavnom se do sada na svim većim konvencijama povodom sigumosti na intemet mreži kao najveći problem izdvaja čovjek kao korisnik, koji je nedovoljno upućen u mogućnostima korištenja servisa sigurnosti, neophodna je kvalitetnija edukacija korisnika infommcionih sistema, a kroz organizacione mjere (primjer da svaki zaposleni ima položen ECDL i slično) i edukacija u osnovama sigurnosti, a što ovaj rad sadrži u sebi.

Pored navedenog, cilj ovog rada je bio da ukaže na obavezu zaštite podataka koji se prenose putem računarske mreže i prikaže osnovne mehanizme za njihovu zaštitu. Ovim radom su dati samo okviri kriptografije, korištenje i sigumost primjenjenih algoritama bez konkretinh primjera matematičkih operacija. Kao nauka koja se razvija brzo, sa razvojem računara, za očekivati je i njenu nadogradnju i implementaciju u sigumosnim mjerama savremenih informacionih sistema.

6. LITERATURA

[1] Wirtz, J., Lwin, M.O., Williams, J.D.: Causes and consequences of consumer online privacy concern, International Journal of Service Industry Management, Vol. 18, No. 4, 2007, pp. 327.
[2] SSL protocol, http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt (novembar 2016)
[3] McRobb, S., Rogerson, S.: Are they really listening?: An investigation into published online privacy policies at the beginning of the third millennium, Information Technology & People, Vol. 17, No. 4, 2004, pp. 443
[4] http://www.slideshare.net/majatodorovic980/zatita-i-sigurnost-u-elektronskom-poslovanju, (novembar 2016)