UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Sanja Popović

Primjena digitalnog potpisa u praksi

SPECIJALISTIČKI RAD

Podgorica, 2019.

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Primjena digitalnog potpisa u praksi

SPECIJALISTIČKI RAD

Kriptografija

Mentor: prof. dr. Vladimir Božović

Sanja Popović

Studijski program: Matematika i računarske nauke

Podgorica, Jul 2019.

Posveta

Zahvaljujem se porodici, prijateljima i mentoru

Apstrakt

Zbog sve češće upotrebe Interneta u poslovnim primjenama javlja se potreba za sigurnim i pouzdanim utvrđivanjem autentičnosti dokumenata. U tome nam pomaže digitalni potpis. Digitalni potpis predstavlja metodu za potpisivanje poruka u digitalnom obliku. Digitalni potpis omogućava autentifikaciju (osoba B može provjeriti je li poruku koju je primila zaista poslala osoba A) i nepobitnost (osoba A ne može poreći da je ona poslala poruku ako osoba B posjeduje poruku s njenim potpisom).

Abstract

Due to the increasing use of the Internetin business applications there is a need for secure and reliable authentication of documents. For that, we use digital signature. Digital signature is a method for signing messages in digital form. Digital signature enables authentication (person B can check wheter the received message was actually sent by person A) and non-repudiation(person A can not deny that she sent the message if the person B has the message with her signature).

Sadržaj

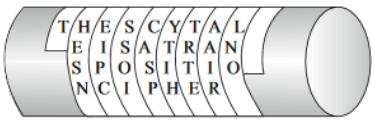
Glava 1

Uvod

Kada čujemo riječ kriptografija, prve asocijacije mogu biti šifrovanje e- mail- ova, siguran pristup web sajtu, pametne kartice za bankarske aplikacije ili razbijanje koda tokom Drugog svjetskog rata na Njemačkoj Enigmi (Slika 1.1).

Slika 1.1: Njemačka Enigma

Primjena kriptografije datira još od oko 2000 godina prije nove ere, kada su nestandardni "tajni" hijeroglifi korišćeni u drevnom Egiptu. Na primjer, postoje dokumentovani slučajevi tajnog pisanja u drevnoj Grčkoj, skita iz Sparte (Slika 1.2).



Slika 1.2: Skita iz Sparte

Kriptoragrafija je naučna disciplina koja se bavi proučavanjem metoda za slanje poruka u određenom obliku u kojem su čitljive samo onome kome su i namijenjene. Sama riječ krpitografija je grčkog porijekla i doslovno u prevodu znači "tajno pisanje". Osnovni cilj kriptografije je omogućiti dvijema osobama komunikaciju preko nesigurnog komunikacionog kanala, tako da ih treća osoba ne razumije. Osoba koja šalje poruku naziva se pošiljalac (Alisa), a osoba koja prima poruku naziva se primalac (Bob), dok treću osobu koja želi da presretne poruku nazivamo napadač (Eva). Srž kriptografije jeste sigurna komunikacija, a ona se postiže uz pomoć četiri osnovna načela kriptografije:

- Povjerljivost (privatnost ili tajnost) poruke – predstavlja činjenicu da samo autorizovane osobe mogu da pristupe datoj informaciji. To se postiže na razne načine- od fizičke zaštite sadržaja sve do matematičko kriptografskih algoritama koji čine da podaci na prvi pogled izgledaju neupotrebljivo.

- Integritet poruke – ovo svojstvo bavi se ispitivanjem "originalnosti" poruke, u smislu provjere da li je prije prijema i dekripcije poruke došlo do neautorizovanih promjena (brisanja, izmjene, umetanja teksta) na samom šifratu, a samim tim i otvorenom tekstu nakon dekripcije.

- Autentifikacija pošiljaoca- sposobnost primaoca poruke da iz iste utvrdi identitet pošiljaoca, porijeklo poruke, te njen put komunikacijskim kanalom.

- Neporicanje pošiljaoca- ovom osobinom kriptografija sprečava korisnika da "poriče" izvršavanje odnosno neizvršavanje određene akcije u prošlosti. Za ovu i prošlu osobinu blisko je vezan pojam digitalnog potpisa koji predstavlja neku vrstu dokaza identiteta pošiljaoca i njegovih radnji pri izvjesnim elektronskim akcijama.

Pošijalac najprije, pomoću već unaprijed dogovorenog ključa mora transformisati poruku koju šalje. Tu poruku nazivamo otvoreni tekst, postupak transformacije šifrovanje (kriptovanje), a dobijeni rezultat šifrat (šifrovana poruka). Nakon toga, pošiljalac šalje poruku preko nesigurnog komunikacionog kanala. Ako napadač presretne poruku i sazna sadržaj šifrata, on zbog nepoznavanja ključa, za razliku od primaoca ne može dešifrovati poruku i razumjeti je. Šifra predstavlja matematičku funkciju koju koristimo za šifrovanje i dešifrovanje. Sve moguće poruke, šifrati i ključevi zajedno sa funckijom za šifrovanje i dešifrovanje čine kriptosistem.

Definicija 1.1. *Kriptosistem je uređena petorka (P, C, K, E, D) za koju važi:*

1. *P je konačan skup svih mogućih otvorenih tekstova;*

2. *C je konačan skup svih mogućih šifrata;*

3. *K je prostor ključeva, tj. Skup svih mogućih ključeva;*

4. *za svaki ključ $k \in K$ postoji algoritam šifrovanja $e_k \in E$ i odgovarajući algoritam dešifrovanja $d_k \in D$, gdje su e_k: $P \mapsto C$ i d_k: $C \mapsto P$ funkcije sa svojstvom da je*

$$d_k(e_k(x)) = x,$$

za svaki otvoreni tekst $x \in P$.

Sigurnost igra veliku ulogu u doba Interneta. Dok je klasična kriptografija uglavnom korišćena od strane vojnih i obavještajnih organizacija, savremena kriptografija nalazi svoju primjenu u našem svakodnevnom životu.

1.1 Asimetrična kriptografija

Izum asimetrične kriptografije postao je revolucionaran u kriptografiji. Ovo novo polje uključuje tehnike javnog ključa. Kriptografski sistem sa javnim ključem koristi dva ključa, od kojih se jedan koristi kao javni ključ, a drugi kao tajni. Javni je poznat svima koji žele da učestvuju u kriptografskom procesu. Funkcionalnost javnog ključa u šemi šifrovanja sa javnim ključem je da se šifruje poruka za prijemnik tako da prijemnik može dešifrovati šifrovani tekst koristeći svoj tajni ključ. Primjer asimetrične kriptošeme uključuje digitalni potpis. U slučaju digitalnog potpisa javni ključ se koristi za provjeru validnosti potpisa u poruci, uz pretpostavku da je potpis dešifrovan korišćenjem tajnog ključa potpisnika. Tajni ključ je poznat samo jednom korisniku.

Glava 2

Digitalni potpis

Digitalni potpis (eng. Digital signature- DS) omogućava utvrđivanje autentičnosti elektronskog dokumenta, npr. Elektornskog pisma, web stranice ili slikovne datoteke. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije neovlašćeno izmijenjen. Provjera vjerodostojnosti (eng. Authentication) potpisanih dokumenata omogućava korišćenje enkripcije, pri čemu enkripcija predstavlja postupak kodiranja podataka prije slanja kako bi ih samo ovlašćeni primalac mogao dekodirati i razumjeti. Uz to što osigurava autentičnost (identitet pošiljaoca utvrđuje se dešifrovanjem sažetka poruke), digitalni potpis osigurava i integritet (provjerom sadržaja poruke utvrđuje se je li se poruka mijenjala na putu do primaoca) te neporečivost (pošiljalac ne može poreći sudjelovanje u transakciji jer jedino on ima pristup svom privatnom ključu kojim je potpisao poruku). Korišćenjem algoritma digitalnog potpisa potpisnik stvara par ključeva, privatni i javni, ali je moguće i da se za potpisivanje svih poruka koristi isti par. Poruka koja se potpisuje sažima se hash algoritmom- stvara se njen otisak. DS algoritam iz tako dobijenog sadržaja poruke i korisnikovog privatnog ključa stvara digitalni potpis koji se šalje ili objavljuje zajedno sa potpisanom porukom. Osnova sigurnosti digitalnog potpisa je u tajnosti privatnog ključa dok je javni ključ svima dostupan, a omogućava provjeru autentičnosti poruke.

Definicija 2.1. *Kriptosistem digitalnog potpisa je uređena petorka (P, A, K, S, V) gdje je:*

1. *P konačan skup svih mogućih poruka;*

2. *A konačan skup svih mogućih potpisa;*

3. *K je prostor ključeva, tj. konačan skup svih mogućih ključeva;*

4. *Za svaki $K \in K$ postoji algoritam za potpisivanje $sig_k \in S$ i odgovarajući algoritam za verifikovanje $ver_k \in V$, takvi da su za sve algoritme $sig_k : P \to A$ i $ver_k : P \times A \to \{0, 1\}$ gdje 0 predstavlja netačno, a 1 tačno, zadovoljene jednakosti*

$$ver_K(x, y) = \begin{cases} 1, & \text{ako je } y = sig_k(x) \\ 0, & \text{ako je } y \neq sig_k(x), \end{cases}$$

za svaku poruku $x \in P$ i svaki potpis $y \in A$. Par (x,y), gdje je $x \in P$ i $y \in A$, se naziva potpisana poruka.

2.1 Istorija digitalnog potpisa

Korišćenje Morseove abecede za prenos poruka telegrafom započinje oko 1860. godine, a već 1869. godine presudom New Hampshine Supreme Court suda potpisi preneseni na ovaj način proglašavaju se pravnomoćnim. Tokom 1980-ih godina mnoge firme i pojedinci koriste faks uređaje za hitan prenos papirnih dokumenata. Iako se kod takvog prenosa podataka potpis fizički nalazio na papiru, rukovanje i prenos podataka vršio se elektronski. Ovakvi potpisi nazivaju se elektronskim potpisima. Digitalni potpisi predstavljaju podskupinu elektronskih potpisa koji koriste

različite kriptografske metode. Razvoj kripografije sa javnim ključem (eng. public key cryptography) započinje 1874. godine opisom jednosmjernih enkripcijskih funkcija u knjizi " The Princioles of Science: A Treatise on Logic and Scientific Method" autora William Stanley Javonsa. Ranije 1970-ih godina James H. Ellis, Clifford Cocks i Malcolm Williamson osmišljaju prve algoritme temeljene na asimetričnom ključu, ali ne objavljuju svoja otkrića. Whitfield Diffie i Martin Hellman 1976. godine, pod uticajem radova Ralpha Merkela na temu distirbucije javnih ključeva, objavljuju prvu praktično upotrebljivu metodu razmjene ključeva, koja kasnije postaje poznata pod nazivom Diffie- Hellman razmjena ključeva i predstavlja poseban slučaj RSA algoritma. Spomenuti RSA algoritam prvi put javno su opisali Ron Rivest, Adi Shamir i Leonardno Adleman 1977. godine. Naziv algoritma stvoren je od početnih slova prezimena autora. To je prvi algoritam prikladan za potpisivanje i enkripciju podataka te se smatra sigurnim, pod pretpostavkom korišćenja dovoljno dugih ključeva i ažurnih implementacija. Neal Koblitz i Victor S. Miller 1985. godine predlažu korišćenje eliptičkih krivih nad konačnim poljima u kriptografskim algoritmima sa javnim ključem. Na temelju ovakve enkripcije razvijen je ECDSA (eng. Elliptic Curve DSA) algoritam, varijanta DSA (eng. Digital Signiture Algorithm) algoritam, koji pomoću manjeg ključa i sa približno jednakim vremenom izvođenja daje sigurniji digitalni potpis jednake veličine. Sredinom 1990-ih godina započinje standardizacija DS algoritma u Sjedinjenim Američkim državama: 1994. godine National Institute of Standards and Technology institute izdaje standard sa oznakom FIBS PUBS 186 (eng. Federal Information Processing Standards Publications), a godinu dana kasnije American National Standards Institute izdaje ANSI X9.30 standard, na nivou Evropske Unije i pojedinih zemalja.

2.2 Princip digitalnog potpisa

Provjeru vjerodostojnosti autora ili podataka moguće je sprovesti korišćenjem:

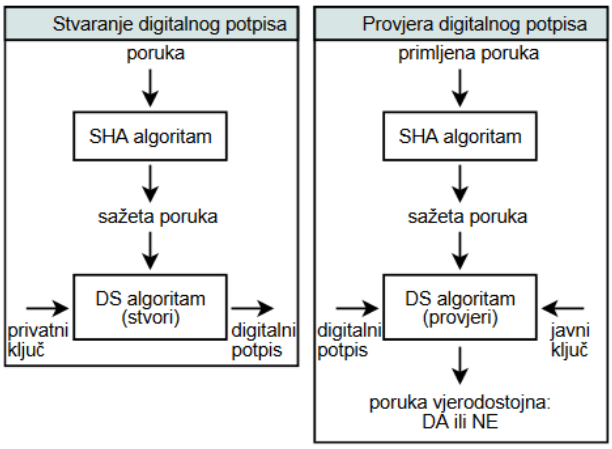
- Lozinki- najčešći način dokazivanja vjerodostojnosti je upotrebom korisničkog imena i sa njim vezane lozinke
- Checksum- koristi se prvenstveno za provjeru ispravnosti primljenih podataka, ali može poslužiti i za provjeru autentičnosti istih jer neispravni testni zbir ukazuje na neovlašćenu izmjenu podataka
- CRC provjere (eng. Cyclic Rendundancy Check) – konceptualno slično testnom zbiru, ali koristi dijeljenje polinoma kako bi se utvrdila ispravnost podataka
- Enkripcije sa privatnim ključem
- Enkripcije sa javnim ključem
- Digitalnim sertifikatima

2.2.1 Enkripcija privatnim ključem

Kod enkripcije sa privatnim ključem svaki računar ili korisnik posjeduje tajni ključ pomoću kojeg se podaci, prije slanja računarskom mrežom, kriptuju. Primalac treba da zna pošiljaocev tajni ključ kako bi mogao dekriptovati tako primljene podatke. Zbog toga je prije uspostavljanja komunikacije potrebno znati koji računari (tj. korisnici) će razumjeti poruku, pa na svaki računar instalirati privatne ključeve računara sa kojih se očekuju poruke.

2.2.2 Enkripcija javnim ključem

Prilikom stvaranja digitalnog potpisa koristi se privatni ključ dok se za njegovu provjeru koristi javni ključ koji odgovara, ali nije jednak, privatnom ključu. Svaki korisnik posjeduje vlastiti privatni i javni ključ. Javni ključevi su javno dostupni i svakom korisniku omogućavaju provjeru potpisa. Privatni ključevi dostupni su samo svojim vlasnicima čime je onemogućeno kriptovanje potpisa. Podaci koji se obilježavaju digitalnim potpisom skraćeno se nazivaju porukom. U postupku stvaranja digitalnog potpisa za dobijanje sažetog pregleda poruke (eng. message digest) koristi se sigurna jednosmjerna funckija, tzv. SHA (eng.Secure Hash Algorithm) algoritam. To su funkcije koje se matematički vrlo jednostavno izračunavaju, ali im je vrlo teško pronaći inverznu funkciju. Iz tako dobijene sažete poruke DS algoritmom stvara se digitalni potpis. Poruka se, zajedno sa pripadnim potpisom, šalje primaocu koji pomoću pošiljaocevog javnog ključa utvrđuje vjerodostojnost poruke i samog digitalnog potpisa. U postupku provjere potrebno je koristiti SHA algoritam jednak onom korišćenom prilikom stvaranja potpisa. Na slici 2.1 shematski su prikazani opisani postupci stvaranja i provjere digitalnog potpisa.



Slika 2.1: Shematski prikaz postupka stvaranja i provjere digitalnog potpisa

U opisanom postpku potpisuje se samo sažeta poruka, a ne cijela poruka, iz sljedećih razloga:

- Efikasnost: potpis će biti puno kraći pa će i cjelokupno postupak biti brži jer je u praksi stvaranje sažetka poruke puno brže od stvaranja potpisa.

- Javna dostupnost dokumenta: npr. razne diplome, potvrde, dozvole, ugovori i sl. trebaju biti javno dostupni pa se spremaju i prenose bez enkripcije, a priloženi potpis garantuje vjerodostojnost pojedinih dokumenata.

- Vjerodostojnost: tekst koji se potpisuje treba da bude kraći od dužine privatnog ključa. Kako to poruka koja se potpisuje najčešće nije, potrebno ju je u slučaju potpisivanja bez sažimanja, razložiti na djelove, pojedinačno potpisati svaki dio i poslati. Primalac za tako razlomljene poruke ne bi mogao znati je li koji njen dio izgubljen ili izbrisan tokom prenosa.

2.3 Digitalni sertifikat

Digitalni sertifikat koristi se kod zahtjevnijih implementacija s javnim ključem, npr. kod web korisnika. Radi se o sertifikatu kojeg izdaje javno ili više ovlašćenih tijela (eng. Certificate Authority), a koja predstavljaju dio PKI (eg. Public key infrastructure) sastava. Spomenuto tijelo djeluje kao posrednik između dva računara ili korisnika, ono potvrđuje njihove identitete i razmjenjuje njihove javne ključeve. Sertifikati koriste digitalne potpise za povezivanje javnih ključeva sa podacima o identitetu vlasnika, kao što su ime osobe ili organizacije, adresa i sl. Time sprečavaju neovlašćen pristup podacima objavljivanjem lažnog javnog ključa. Mreža povjerenja (eng. Web of trust) predstavlja alternative centralizovanim PKI sastavima, a koristi se kod PGP (eng. Pretty GOOD Privacy), GnuPGP i drugih sastava kompatibilnih sa OpenPGP

standardom. Djeluje tako da korisnici, koristeći vlastite privatne ključeve, potpisuju identifikacijske sertifikate drugih korisnika. Spomenuti identifikacijski sertifikati mogu sadržati informacije kao što su javni ključevi i podaci o njihovim vlasnicima. Na primjer, korisnik može prihvatiti vjerodostojnost sertifikata ako ga je potpisalo troje ili više korisnika u koje spomenuti korisnik ima djelimično povjerenja, ili jedan potvrđeno vjerodostojan korisnik.

Glava 3

Algoritmi digitalnog potpisa

3.1 Hash funkcije

Hash funkcija za ulaz uzima poruku koja je uglavnom fiksne dužine a kao izlaz daje šifrovanu poruku, poznatu kao hash-code, hash-rezultat. Preciznije rečeno. Hash funkcija h pridružuje nizovima znakova proizvoljne dužine nizove znakova fiksne dužine. Za domen D i kodomen R definišimo preslikavanje $h, h : D \to R$, gdje je $|D| > R$. Kako je $D > R$, može doći do "sudara", jer sa manjim brojem znakova trebamo reprezentovati veći broj znakova. Osnovna ideja hash funkcije je da hash služi kao kompaktna reprezentacija slike (digitanog potpisa) ulazne vrijednosti i da se ne može dobiti pomoću neke druge ulazne vrijednosti.

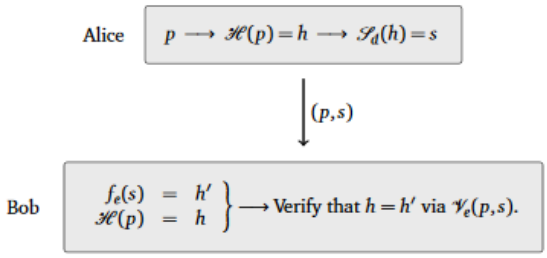
3.1.1 Definicija i osnovna svojstva

Hash funkcije možemo podijeliti u dvije klase: hash funkcije bez ključa koje za ulazni parametar imaju samo poruku i hash funkcije sa ključem koje za ulaz imaju poruku i tajni ključ.

Definicija 3.1. *1. Hash funkcija je funckija $X : \{0,1\} \to \{0,1\}^l$, za neko fiksirano $l \in N$, dato polinomijanim algoritmom.*

2. *X je "otporna na sudar" ako je neizvodljivo naći različite* x_1, x_2 *za koje važi* $X(x_1) = X(x_2)$.

Na Slici 3.1 prikazan je proces digitalnog potpisivanja korišćenjem hash funkcije i javnog kriptosistema za potpisivanje i verifikaciju.



Slika 3.1: Proces digitalnog potpisivanja korišćenjem hash funkcije

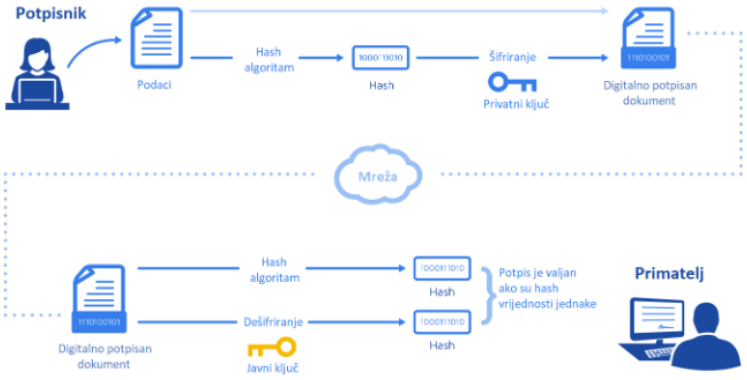
Osnovno svojstvo hash funkcije je zahtjev da za bilo koja dva izračunata različita hash-a i ulazi iz kojih su oni izračunati moraju biti različiti. Drugo svojstvo efikasnih hash funckija je da za dva izračunata ista hash ulaza iz kojih su izračunati ne moraju biti isti. Ako izračunamo hash vrijednost za jedan ulaz, a nakon toga ulazu promijenimo samo jedan bit, tada bi novi izračunati hash trebao da bude potpuno različit od prethodnog.

3.2 Algoritmi za digitalno potpisivanje

Sistem digitalnog potpisivanja se sastoji od tri različita algoritma:

- Algoritam za generisanje javnog i privatnog ključa- izlaz iz algoritma su privatni ključevi i odgovarajući javni ključ. Pomoću privatnog ključa će poruka biti potpisana, a pomoću javnog verifikovana..
- Algoritam za izradu potpisa- generiše se digitalni potpis na osnovu sažetka poruke i privatnog ključa.

- Algoritam za provjeru potpisa- koristeći poruku, javni ključ ili potvrđuje ili opovrgava autentičnost poruke
- Shematski prikaz međusobnog djelovanja ova tri algoritma je prikazan na Slici 3.2.



Slika 3.2: Shematski prikaz algoritma za stvaranje i provjeru digitalno potpisane poruke

Dva najčešća i najpouzdanija algoritma koji se koriste za digitalno potpisivanje su:

1. DSA (Digital Signature Algorithm).
2. RSA (Rivest- Shamir- Adleman).

3.2.1 DSA

DSA je algoritam baziran na matematičkom konceptu modularnog eksponenta i problemu diskretnog logaritma. The National Institute of Stndards and Technology (NIST) predložio je DSA za korišćenje u Digital Signature Standard (DSS) 1991. godine. DSA algoritam funkcioniše u okviru kriptosistema javnog ključa i zasniva se na algebarskim svojstvima modularnog eksponenta, zajedno sa problemom diskretnog

logaritma, koji se smatra računski nepopravljivim. Algoritam koristi par ključeva koji se sastoji od javnog i privatnog ključa. Privatni ključ se koristi za generisanje digitalnog potpisa za poruku, a takav potpis se može provjeriti pomoću odgovarajućeg javnog ključa potpisnika. Digitalni potpis osigurava provjeru autentičnosti poruke (primalac može provjeriti porijeklo poruke), validnost (primalac može provjeriti da poruka nije izmijenjena od trenutka potpisivanja) i nepovjerenje (pošiljalac ne može lažno da tvrdi da nije potpisao poruku). DSA algoritam obuhvata četiri operacije: generisanje ključa (kreira se par ključeva), distribuciju, potpisivanje i verifikovanje potpisa.

3.2.1.1 Generisanje ključa

Generisanje ključa ima dvije faze. Prva faza je izbor parametara algoritma koji se mogu dijeliti između različitih korisnika sistema, dok druga faza izračunava jedan par ključeva za jednog korisnika.

Generisanje parametara :

- Izabrati odobrenu kriptografsku hash funkciju H izlazne dužine $|H|$ bita. Ako je H veća od dužine modula N, koristi se samo zadnji lijevi bajt hash izlaza.
- Izabrati dužinu hash-a L. DSS ograničio je da L bude umnožak 64 između 512 i 1024 uključujući i njih.
- Izabrati dužinu modula N, tako da je $N < L$ i $N \leqslant |H|$.
- Izabrati N- bitni q.
- Izabrati L- bitni p tako da je $(p-1)$ umnožak od q.
- Izabrati cijeli broj h proizvoljno iz $\{2, \ldots, p-2\}$.

- Izračunati $g := h^{(p-1)/q} \mod p$. U rijetkim slučajevima, ako je $g = 1$ probati ponovo sa drugim brojem h. Obično se koristi $h = 2$.

Parametri algoritma su (p, q, g). Oni mogu biti podijeljeni između različitih korisnika sistema.

Ključevi za pojedinačnog porisnika

Neka je dat skup parametara. Druga faza izračunava par ključeva za jednog korisnika:

- Izabrati cijeli broj x, proizvoljno iz $\{1, \ldots, q-1\}$.
- Izračunati $y := g^x \mod p$.

3.2.1.2 Distribucija ključa

Potpisnik treba da objavi javni ključ y. Zapravo, on bi trebao poslati ključ primaocu preko pouzdanog, ali ne i obavezno tajnog mehanizma. Potpisnik treba da drži privatni ključ x tajnim.

3.2.1.3 Verifikovanje potpisa

Poruka m se potpisuje na sljedeći način:

- Izabrati cijeli broj k proizvoljno iz $\{1, \ldots, q-1\}$,
- Izračunati $r := (g^k \mod p) \mod q$. U rijetkim slučajevima kada je $r = 0$, ponoviti postupak sa drugim proizvoljnim brojem k.
- Izračunati $s := (k^{-1}(H(m) + xr)) \mod q$. U rijetkim slučajevima kada je $s = 0$ ponoviti proces sa drugim proizvoljnim brojem k.. Izračunavanjem k i r stvara se novi ključ.

3.2.1.4 Verifikovanje potpisa

Provjera da li je potpis (r, s) validan za poruku m vrši se na sljedeći način:

- Provjeriti da li je $0 < r < q$ i$0 < s < q$.
- Izračunati $w := s^{-1} \mod q$.
- Izračunati $u_1 := H(m)w \mod q$.
- Izračunati $u_1 := rw \mod q$
- Izračunati $v := (g^{u_1}y^{u_2} \mod p) \mod q$.
- Potpis je validan ako i samo ako je $v = r$.

3.2.2 RSA

RSA je algoritam za asimetričnu kriptografiju, prvenstveno namijenjen šifrovanju podataka ali se danas koristi i u sistemima elektronskog potpisa. RSA danas predstavlja industrijski standard u oblasti asimetrične kriptografije i zaštiti podataka, tako da je široko primijenjen u mnogim sigurnosnim protokolima i sistemima elektronskog poslovanja. RSA je algoritam za simetričnu kriptogafiju nastao 1977. godine. Tvorci ovog algoritma su Ronald Rivest, Leonard Ejdlman i Adi Šamir, gdje RSA predstavlja akronim njihovih prezimena. U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi. Sigurnost RSA zasniva se na složenosti faktorizacije velikih brojeva. Smatra se da je određivanje originalne poruke na osnovu šifrata i ključa za šifrovanje ekvivalentno faktorizaciji proivoda dva velika prosta broja.

3.2.2.1 Postupak generisanja ključa za RSA algoritam

Osoba A formira javni i tajni ključ:

1. Bira porste brojeve p i q,.

2. Izračunava broj n=pq.

3. Izračunava broj $t = (p-1)(q-1)$

4. Bira slučajno broj e (dio javnog ključa).

5. Odgovarajućim (prošireni Euklidov) alogirtmom računa d, tj. Tajni ključ

6. Javni ključ je par (n, e) .

Vlasnik privatnog ključa d, slobodno može da objavi brojeve n i e tako da svako ko želi da mu uputi tajnu poruku može to i učiniti, a njen sadržaj može čitati samo vlasnik privatnog ključa, dok ostali dobijaju besmislen tekst.

3.2.2.2 Šifrovanje poruke

Da bi osoba B koja posjeduje javni ključ šifrovala poruku m osobi A mora da:

1. Računa $c = m^e \mod n$.

2. Taj broj c (šifrat originalne poruke m) osoba B, šalje osobi A, koja pristupa dešifrovanju, odnosno koristeći broj d- tajni ključ računa..

3.2.2.3 Dešifrovanje poruke

Koristeći broj d- tajni ključ osoba A računa: $c^d \mod n$, a taj broj je i originalna poruka m.

Glava 4

Primjena digitalnog potpisa

Informatičko poslovanje je veoma važan i nezamjenljiv način komunikacije u današnje doba. Stoga, bez napredne zaštite i osiguranja, uprkos svim prednostima koje donosi, može biti izvor brojnih rizika. Zato digitalni potpis predstavlja sigurnost i povjerenje na širokom spektru djelatnosti i usluga, a najviše se koristi u područjima potpisivanja dokumenata, slijepog potpisa, potpisa u internetskim aplikacijama i kao zaštita multimedijalnih sadržaja.

4.1 Digitalno potpisivanje dokumenata

U mnogim zemljama digitalno potpisivanje je po pravnoj važnosti izjednačeno sa ručnim potpisom. To znači digitalno potpisani dokument pravno obavezuje potpisnika, u skladu sa uslovima navedenim u dokumentu. Zbog toga se preporučuje korišćenje različitih parova ključeva za enkripciju i za potpisivanje. Korišćenjem para ključeva namijenjenih enkripciji, korisnik moše učestvovati u kriptovanoj komunikaciji (npr. Pregovorima o kupovini nekretnine), ali ne potpisuje svaku poruku pravno važećim potpiom. Jednom kada zainteresovana strana postigne dogovor, ugovor se digitalno potpisuje i tek tada su potpisnici pravno vezani potpisanim dokumentom.

Tako potpisani ugovor moguće je zatim, zbog dodatne zaštite, slati kriptovanog. DS algoritni i protokoli ne pružaju, sami po sebi, informaciju o tome kada je dokument potpisan. Potpisnik može, ali i ne mora, uključiti vremensku oznaku (eng. time stamp) unutar digitalnog potpisa ili se u samom dokumentu može spomenuti datum i vrijeme potpisivanja. Ovakvo označavanje vremena omogućava navođenje netačnog, npr. ranijeg datuma ili vremena potpisivanja. Korišćenjem sigurnih vremenskih oznaka (eng. trusted time stamp) sprječava se ovakva zloupotreba digitalnog potpisa. Sigurne vremenske oznake osigurava pouzdana treća strana, tzv. TSA (eng. Time Stamping Authority), koja time potvrđuje postojanje određenih podataka prije nekog vremena. Ranjivost takvog korišćenja vremenskih oznaka moguće je umanjiti ubacivanjem više oznaka različitih TSA organizacija u potpisu. Jedna od osnovnih prednosti korišenja digitalnog potpisa, uz osiguranje autentičnosti i integriteta dokumenta, je onemogućavanje nepriznavanja dokumenta od strane potpisanika (eng. non- repudiation). Ako sporna poruka nije potpisana, njen navodni pošiljalac je uvijek može poreći tvrdnju da je neko drugi napisao i poslao. To se ne može dogoditi sa potpisanim porukama osim u slučaju otkrivanja korisnikovog privatnog ključa, kojeg zbog toga treba čuvati u strogoj tajnosti. Spremanje privatnog ključa na tzv. Pametnoj kartici (eng. smart card) jedan je od načina osiguravanja njegove tajnosti. Alternativa je čuvanje privatnog ključa na privatnom računaru korisnika, ali takav pristup ima dva ozbiljna nedostatka:

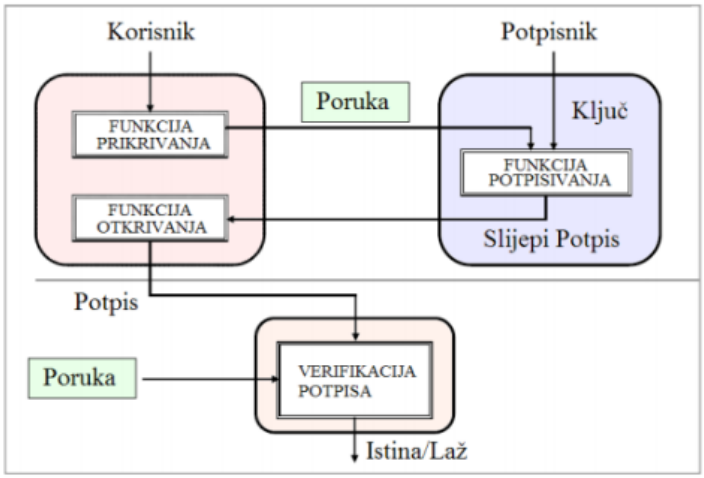
- Korisnik može potpisivati dokumente samo na sopstvenom računaru.
- Tajnost privatnog ključa zavisi od sigurnosti računara na kojem je postavljen.

Karticu je potrebno povezati na računar i proslijediti joj hash vrijednost poruke, ugrađeni procesor zatim iz sačuvanog privatnog ključa i primljenog otiska poruke proračunava potpis koji se potom šalje računaru. Na taj način privatni ključ nikada ne

napušta karticu. Većinu kartica potrebno je prije upotrebe aktivirati ličnim identifikacionim brojem (eng. Personal Identification Number- PIN), a napravljene su tako da onemogućavaju, ili barem otežavaju, neovlašćen pristup sačuvanim podacima.

4.2 Slijepi potpisi

Slijepi potpis (eng. blind signature) oblik je digitalnog potpisa kod kojeg je sadržaj poruke skriven (eng. blinded) od potpisanika. Takvim potpisom moguće je provjeriti vjerodostojnost originalne otkrivene (eng. unblended) poruke jednako kao što se to čini običnim digitalnim potpisom. Ovakvi potpisi najčešće se koriste u primjenama gdje je jedna strana autor poruke, a neka druga njen potpisanik, npr. u kriptografskim sistemima za glasanje ili kod sigurnih elektornskih platežnih sistema. Druga moguća primjena slijepih potpisa je sprečavanje potpisanika da poveže potpisanu skrivenu poruku s kasnije otvorenom porukom tokom njenog eventualnog ocjenjivanja (eng. unlunkability). Slijepi potpisi ovako se koriste u primjerima kod kojih je nužna anonimnost pojedinih saradnika. Slijepo potpisivanje moguće je implementirati pomoću raznih DS algoritama s javnim ključem, npr. RSA ili DSA algoritmom. Poruka se prije potpisivanja skriva, najčešće kombinovanjem s nasumično odabranim ključem (eng. blinding factor) i zatim se potpisuje nekim od uobičajnih DS algoitama. Vjerodostojnost potpisane skrivene poruke, zajedno sa ključem korišćenim za njeno skrivanje, moguće je utvrditi pomoću potpisnikovog javnog ključa. Kriptosistem slijepog potpisa sastoji se od tri funkcije: funkcija prekrivanja, funkcija potpisivanja i funckija otkrivanja (Slika 4.1).



Slika 4.1: Protokol slijepog potpisa

4.3 Digitalni potpisi u web aplikacijama

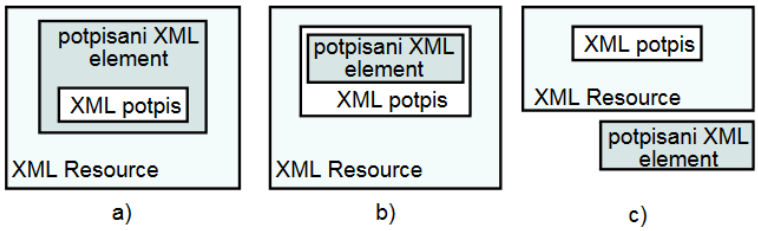
Različite sadržaje web stranica moguće je potpisati XML digitalnim potpisom koji je regulisan W3C XML Signature standardom krovne međunarodne standardizacijske organizacije na području web tehnologija World Wide Web Consortium. XML potpisom moguće je potpisati sljedeće tipove podataka:

- XML elemente, skupove XML čvorova (eng. Nodes) i njihov sadržaj,
- Spoljne URI oznake,
- Spoljne binarne datoteke,
- Binarne podatke ugrađene u XML dokumente u obliku znakovnih nizova kodiranih u bazi 64.

Na pojedinoj web stranici moguće je potpisati bilo koji njen programski dostupan element (djelove HTML i XML programskog koda, pa skrivena i vidljiva polja formulara kao i njihove sadržaje), datoteke prisutne na klijentskom računaru, mrežne

resurse koji su dostupni s klijentovog računara ili posebno preko servera. Postoje tri tipa XML potpisa (Slika 4.2):

- Omotani (eng. enveloped)– potpis je ugrađen u podatke koji se potpisuju
- Omotavajući (eng- enveloping)- potpisani podaci su ugrađeni u XML potpis
- Odvojeni (eng. detached) XML potpis i potpisani podaci su razdvojeni.



Slika 4.2: a) omotani; b) omotavajući; c) odvojeni

Opšta struktura XML digitalnog potpisa je(Slika 8):

```
<Signature ID?>
   <SignedInfo>
     <CanonicalizationMethod/>
     <SignatureMethod/>
     (<Reference URI? >
       (<Transforms>)?
       <DigestMethod>
       <DigestValue>
     </Reference>)+
   </SignedInfo>
   <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
 </Signature>
```

Slika 4.3: Opšta struktura digitalnog potpisa

gdje "?" označava jedno ili nijedno pojavljivanje, "+" označava jedno ili više pojavljivanja, a "*" označava nula ili više pojavljivanja odgovarajuće oznake. Potpisi su sa potpisanim podacima povezani URI oznakama, ako se ti podaci nalaze izvan XML datoteke, ili fragmentalnim oznakama (eng. fragment identifier), ako su podaci i potpis unutar iste datoteke.

4.4 Zaštita multimedijalnog sadržaja digitalnim potpisom

Zaštita multimedijanog sadržaja razlikuje se od ostalih vrsta digitalnih podataka po tome što ih je moguće mijenjati bez narušavanja sadržaja koji se prenose pa je prilikom provjere autentičnosti potrebno razlikovati obradu od zlonamjernih promjena sadržaja-napada. S druge strane, bilo kakva izmjena nekog elektronskog pisma ili pravnog dokumenta predstavlja napad i treba biti uočena u postupku provjere vjerodostojnosti. Multimedijalne sadržaje moguće je štititi ugrađivanjem tzv. Vodenih žigova (eng. watermark) ili njihovim digitalnim potpisivanjem. Vodeni žig je skup informacija, namijenjenih npr. zaštita autorskih prava, ugrađen u multimedijalni sadržaj pri čemu sam žig može biti vidljiv ili skriven od krajnjeg korisnika. Vidljivi žigovi koriste se za ograničavnje upotrebe označenog sadržaja dok se skirveni žigovi koriste za utvrđivanje njegovog porijekla. Neobrađeni i nesažeti sadržaji naročito su pogodni za zaštitu vodenim žigovima zbog:

- Vodeni žig je direktno povezan sa podacima na koje se odnosi, pa ga je moguće jednostavno provjeriti.
- Unutar takvih podataka postoji dovoljno prostora za ugrađivanje žiga bez narušavanja vidljivog sadržaja.

Pojedini vodeni žigovi najčešće su krhki, tako da ne mogu preživjeti obradu sadržaja koji obilježavaju (npr. sažimanje), ali mogu biti vrlo robusni, što znači da su otporni na obradu sadržaja, pa i na različite zlonamjerne izmjene. Kako se multimedijalni sadržaj rijetko distribuira i koristi bez sažimanja mnogo je prikladnija njihova zaštita digitalnim potpisom. Mnogi standardi za sažimanje podataka, npr.

JPEG i MPEG omogućavaju unos korisničkih podataka u poseban odjeljak unutar sažetka datoteke, gdje je moguće ugraditi digitalni potpis. Tokom izmjene sadržaja izvorni korisnički podaci, u ovom slučaju digitalni potpis, najčešće se odbacuju. Čak i ako napadač uspije zadržati potpis unutar izmijenjene datoteke, napad je lako moguće otkriti zbog nepodudaranja hash vrijednosti napadnute datoteke i vrijednosti iz potpisa. Digitalni potpis je moguće uskladištiti u posebnu datoteku koju je onda potrebno distribuirati sa sadržajem na koji se odnosi. Postupak potpisivanja multimedijalnih sadržaja u načelu se ne razlikuje od potpisivanja ostalih vrsta podataka, a glavna razlika je u informacijama koje se koriste za stvaranje potpisa. Kod tekstualnih dokumenata ili djelova programskog koda potpisuje se niz bitova tako da promjena barem jednog znaka biva uočena tokom provjere vjerodostojnosti. Multimedijalni dokumenti se potpisuju tako da se zaštiti njihov sadržaj, vizuelne i zvučne informacije koje krajnji korisnik percipira tokom pregledanja. Te informacije se ne gube legalnom obradom dokumenta, npr. sažimanjem ili promjenom veličine slike, pa se ne gubi ni vjerodostojnost potpisane datoteke. U slučaju napada na potpisani multimedijalni dokument, najčešće u obliku zamjene pojedinih elemenata zlonamjerno oblikovanim sadržajem, dolazi do izmjene potpisanih informacija koje je moguće otkriti provjerom vjerodostojnosti.

Glava 5

Digitalni potpis u Crnoj Gori

Elektronski potpis i elektronska identifikacija predstavljaju važan segment elektronskog poslovanja. Njegovom primjenom omogućava se provjera autentičnosti potpisnika, zaštita integriteta podataka koji se prenose i neporecivost elektronskog potpisivanja dokumenta. Primjena je omogućena korišćenjem digitalnog sertifikata kojim se elektronskim putem potvrđuje veza između podataka za provjeru elektronskog potpisa i identiteta potpisnika. Digitalni sertifikat može da se shvati kao digitalni identifikacioni dokument, odnosno "elektronska lična karta“ jer sadrži podatke o korisniku sertifikata kao i podatke o njegovom izdavaocu. U Crnoj Gori postoje dva sertifikaciona tijela za izdavanje kvalifikovanih digitalnih sertifikata. To su Ministarstvo javne uprave, koje je preuzelo poslove Ministarstva za informaciono društvo i telekomunikacije i koje izdaje digitalne sertifikate za potrebe ministarstava i drugih organa državne uprave i Pošta Crne Gore kao javno sertifikaciono tijelo za građane i pravna lica u Crnoj Gori. Pošta Crne Gore izabrana je za nacionalno sertifikaciono tijelo za javne potrebe.

Ovim aktivnostima prethodilo je donošenje Uredbe o djelokrugu, sadržaju i davaocu usluga sertifikovanja elektronskih potpisa za organe uprave (Službeni list Crne

Gore, broj 84/2009") kojom je utvrđeno da poslove sertifikovanja elektronskih potpisa za potrebe organa uprave vrši Ministarstvo nadležno za poslove informacionog društva. Na osnovu člana 9 Uredbe usvojen je Pravilnik o postupcima izdavanja sertifikata. Pravilnik definiše infrastrukturu javnih ključeva, koja predstavlja kompleksan sistem koji se sastoji od kriptografskih tehnologija, protokola, standarda, politika, procedura, servisa i aplikacija za zaštitu podataka i mrežnih resursa. Korisnik nakon izdavanja digitalnog certifikata dobija:

- **Digitalni identitet** (kriptovanje/digitalni potpis dokumenta, kriptovanje/digitalni potpis e-mail poruka, prijava na Windows sa certifikatom (SmartCard Logon))
- **Uređaj za čuvanje digitalnog identiteta** (USB eTokon)
- **Koverat sa passwordom** za token
- **Korisničko i tehničko uputstvo** za instalaciju pripadajućih softvera.

Pošta CG CA izdaje slijedeće tipove digitalnih certifikata:

- kvalifikovani digitalni certifikat izdat na pametnoj kartici;
- kvalifikovani digitalni certifikati;
- kvalifikovani digitalni certifikat za povjerljivost izdat na pametnoj kartici;
- kvalifikovani digitalni certifikat za povjerljivost;
- digitalni certifikat za SSL server.

5.1 Postupak za izdavanje digitalnog sertifikata

Postupak izdavanja digitalnih sertifikata ministarstvima i drugim organima državne uprave je definisan Pravilnikom o postupcima izdavanja sertifikata. Zahtjeve za

izdavanje digitalnih sertifikata može podnijeti svaki službenik organa državne uprave odnosno organ državne uprave. [GOV.ME] CA izdaje sertifikate tek nakon provjere identiteta korisnika i uspešnog 12 završetka procesa registracije. Glavni koraci u procesu obrade zahtjeva za izdavanje sertifikata su:

- korisnik podnese potpisan obrazac za prijavu i priloži valjan dokument za identifikaciju
- korisnik prihvati uslove potpisivanjem sporazuma End-User Agreement
- Zahtjev za izdavanje sertifikata je prihvaćen i odobren od strane [GOV.ME] CA Registration Authority
- Registration Authority podnosi zahtjev za sertifikat [GOV.ME] CA operativnoj službi (enlg. Operations Authority, skraćeno OA)
- [GOV.ME] CA OA dodaje i aktivira korisnika u aplikaciji sertifikacionog tijela sa odgovarajućim sertifikatom profila. Aplikacija sertifikacionog tijela generiše kodove za aktiviranje , koji se sastoje od referentnog broj i autorizacijskog koda. Kodovi za aktiviranje trebaju korisniku u tehničkom postupku preuzimanja sertifikata.
- Kodove za aktiviranje je potrebno poslati korisniku koji je tražio izdavanje sertifikata: Referentni broj šalje OA elektronskim putem na e-mail adresu koju je korisnik naveo na obrascu zahtjeva za izdavanje sertifikata
- autorizacijski kod je odštampan i zatvoren u kovertu. OA isporučuje kovertu RA koju zatim, korisnik preuzima lično u RA kancelariji

5.2 Primjena digitalnog sertifikata

Važan zadatak javnih institucija je da, u sferi elektronskih komunikacija, primjenom informaciono-komunikacionih tehnologija obezbijede servise javne administracije gradjanima i biznisu. Sve veći broj aplikacija i web servisa elektronske uprave zahtjevaju/omogućavaju autentifikaciju i digitalno potpisivanje korišćenjem digitalnog identiteta.

5.2.1 Portal eUprave

Važan zadatak javnih institucija je da, u sferi elektronskih komunikacija, primjenom informaciono-komunikacionih tehnologija obezbijede servise javne administracije gradjanima i biznisu. Sve veći broj aplikacija i web servisa elektronske uprave zahtjevaju/omogućavaju autentifikaciju i digitalno potpisivanje korišćenjem digitalnog identiteta. Digitalni certifikati na portalu se koriste radi registrovanja korisnika (fizička lica i pravni subjekti) koji koriste web usluge, a koriste ga i službenici iz državnih institucija koji obavljaju poslove administriranja, kreiranja, obrade elektronskih usluga i moderaciju javnih rasprava.

5.2.2 Poreska Uprava Crne Gore

Portal Poreske Uprave Crne Gore (https://eprijava.tax.gov.me) namijenjen je unosu poreskih prijava, odnosno obračuna poreza i doprinosa. Za pristup portalu, u cilju elektronske dostave IOPPD obrazaca, potreban je certifikat izdat na lično ime ili na pravno lice i u oba slučaja, dodjeljivanje prava za podnošenje prijava je u nadležnosti Poreske Uprave. Portalu PU može se pristupiti samo certifikatom koji je izdala Pošta Crne Gore.

5.2.3 Službeni list Crne Gore I Pravno-informacioni system Crne Gore

Cilj je projekta elektronskog izdanja Službenog lista Crne Gore je povezanost svih pravnih dokumenata, zakona i podzakonskih akata od 1945. godine, kao i jednostavnost njihove pretrage na portalu. Zakon o objavljivanju propisa i drugih akata Crne Gore predviđa da se elektronsko izdanje Službenog lista potpisuje digitalnim potpisom i objavljuje na internet stranici Javne ustanove. Takodje, svaki propis ili drugi akt, koji treba da se objavi u Službenom listu i nalog, koji se dostavlja u elektronskom obliku, moraju biti potpisani digitalnim potpisom.

5.2.4 Centralni registar stanovništva

Važan cilj u razvoju informacionog društva je interoperabilnost koja će omogućiti različitim organima uprave da uskladjeno djeluju u smjeru zajedničkih ciljeva. Kako je Centralni registar stanovništva jedan od ključnih registara u državi, podaci iz CRS-a dostavljaju se korisniku koji za obradu tih podataka ima pravni osnov utvrdjen zakonom. Sve veći broj državnih institucija koristi informacione sisteme pa stoga ne čudi potreba za bezbjednim povezivanjem IS državnih institucija sa eCRS sistemom upotrebom digitalnih certifikata.

5.2.5 Sistem za upravljanje dokumentima u vladi i ministarstvima – eDMS

Sistem za upravljanje dokumentima je trenutno pokrenut u 12 ministarstava. eDMS je namijenjen vršenju kancelarijskog poslovanja elektronskim putem pa podrazumijeva da se poslovni procesi razmjene dokumenata obavljaju uz pomoć digitalnih

certifikata. Sa druge strane, povjerljiva dokumenta koja se nalaze na sistemu je potrebno kriptovati iz bezbjednosnih razloga. U svakom slučaju, eDMS nudi mogućnost digitalnog potpisa, enkripcije sadržaja i podrške za digitalno uništavanje.

Glava 6

Zaključak

Kako je danas rad bez računara i interneta u obavljanju bilo kakvog posla skoro nezamisliv, potreba za očuvanjem autentičnosti i sigurnosti dokumenata postaje sve veća. Iz navedenog razloga digitalni potpis poprima sve širu upotrebu i samo je pitanje vremena kada će u potpunosti zamijeniti klasično potpisivanje. Digitalni potpis je ključ sigurnosti i povjerenja u savremenom poslovanju. Omogućio je kvalitativni skok u razvoju mnogih aplikacija jer obezbjeđuje bržu i jednostavniju komunikaciju. Koncept online potpisivanja ugovora zasigurno će otvoriti vrata novim uslugama i oblicima poslovanja. Najširа primjena digitalnog potpisa vidi se kod Internet bankarstva (u kojem se koriste pametne kartice za sigurno pristupanje web aplikacijama) i u korišćenju (skeniranjem) digitalizovanog ručnog potpisa bankarskih transakcija. Budućnost digitalnog potpisa leži u njegovoj sigurnosti, a njegova sigurnost u algoritmima koji se koriste za šifrovanje podataka. Digitalni potpis će sigurno postati preovladavajući način utvrđivanja autentičnosti dokumenata.

Bibliografija

[1] Introduction to Cryptography, Johannes A.Buchmann,

[2] Digitalni potpis, Mario Zovkić i Tedo Vrbanec

[3] An Introduction to Cryptography, Mohamed Barakat, Christian Eder, Timo Hanke

[4] Cryptography Theory and Practice D.R.Stinson (2002)

[5] The Science of Secret Writting, L.D. Smith (1971)