UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Miloš Milić

Digitalni potpis u elektronskom poslovanju

SPECIJALISTIČKI RAD

Podgorica, 2016.

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Digitalni potpis u elektronskom poslovanju

SPECIJALISTIČKI RAD

Kriptografija

Mentor: Vladimir Božović

Miloš Milić

Studijski program Računarske nauke

Podgorica, Oktobar 2016.

Apstrakt

Tajnovitost je srž, srce kriptografije. Enkripcija u praktičnom smislu znači očuvati tajnost informacija. Sve češća potreba za bezbjednom komunikacijom dvije strane kao i očuvanjem povjerljivosti informacija, dovela je do inovacija u digitalnom svijetu. Upravo zbog toga, digitalni potpis je postao jedan od najvažnijih kriptografskih alata koji se koristi danas. Njegova osnovna uloga je da utvrdimo identitet pošiljaoca poruke ili potpisnika dokumenta, kao i da se obezbjedi dokaz da originalni sadržaj poruke ili dokumenta koji je poslat nije mijenjan tokom slanja. U ovom radu opisaćemo princip funkcionisanja digitalnog potpisa, algoritme koji se koriste prilikom potpisa, kao i njegovu primjenu, konkretno u elektronskom poslovanju. Takođe osvrnućemo se i na samu bezbjednost korišćenja samog potpisa, kao i na njegovu dalju upotrebu u budućnosti.

Abstract

Secrecy is the heart of cryptography. Encryption in a practical way means to achieve information secrecy. Increasingly often need for safe communication between two sides as well as the preservation of confidentiality of information has led to innovations in the digital world. Therefore, the digital signature has become one of the most important cryptographic tool that is used today. Its primary role is to determine the identity of the sender of the message or the signer of the document, as well as to provide evidence that the original content of the message or document that has been sent has not been altered during the sending. In this paper we will describe the functions of a digital signature algorithms used in signatures, as well as its implementation, particularly in electronic business. Also we will look back to the safety of the use of signatures, as well as its further use.

Sadržaj

Glava 1

Uvod

Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacije. Kada se lične, finansijske, vojne ili informacije državne bezbjednosti prenose sa mjesta na mjesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi mogu se izbjeći sifrovanjem informacija koje želimo bezbjedno da pošaljemo i učinimo ih nedostupnim neželjenoj strani. Hronološki gledano, upravo su potpisi oduvijek bili najbolje prihvaćeni način autentifikacije. Potpisi se danas nalaze na različitim dokumentima (ugovori,pisma,transkacije i slično). Korištenje Morzeove azbuke za prenos poruka telegrafom započinje oko 1860. godine, a već 1869. godine presudom New Hampshire Supreme Court suda potpisi prenešeni na ovaj način proglašavaju se punomoćnim. Digitalni potpisi predstavljaju podskup elektronskih potpisa koji koriste različite kriptografske metode. Upravo zbog toga je razvoj digitalnih potpisa usko povezan sa razvojem i istorijom kriptografije. Whitfield Diffie i Martin Hellman 1976. godine, pod uticajem radova Ralpha Merkela na temu distribucije 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. Ovo ustvari i predstavlja temelj za pouzdanu provjeru porijekla informacija, tj. digitalni potpis. Zanimljivo je napomenuti da je ovaj način kriptovanja

podataka, prema nekim informacijama bio poznat britanskoj tajnoj službi nekoliko godina ranije nego spomenutoj dvojici istraživača. Spomenuti RSA algoritam prvi put javno su opisali Ron Rivest, Adi Shamir i Leonard 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 kao i aktuelnih ,ažurnih rješenja. Neal Koblitz i Victor S. Miller 1985. godine predlažu korištenje 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 Signature Algorithm) algoritma, koji pomoću manjeg ključa i sa približno jednakim vremenom izvođenja daje sigurniji digitalni potpis jednake veličine. Sredinom 1990-ih godina započinje standardizacija DS (eng. Digital Signature) algoritama u Sjedinjenim Američkim Državama: 1994. godine National Institute of Standards and Technology institut izdaje standard s oznakom FIBS PUBS 186 (eng. Federal Information Processing Standards Publications), a godinu dana kasnije American National Standards Institute institut izdaje ANSI X9.30 standard. Standardizacija na području Evrope započinje krajem 1990-ih i početkom 2000-ih godina, počevši od Evropske Unije, a kasnije i u ostalim zemljama. U Crnoj Gori, digitalni potpis i sigurna razmjena dokumenata aktuelna je od 2003. godine. Digitalni potpis služi da obezbijedi dokaz da je elektronski dokument autentičan. Autentičan znači da nam je poznato ko je kreirao dokument i da znamo da dokument nije izmjenjen na bilo koji način od trenutka kada nam je poslat. Digitalni potpisi se obično koriste za distribuciju softvera, multimedijalnih sadržaja, sigurnu korespodenciju povjerljivih podataka u elektronskom poslovanju, finansijske transakcije, kao i u drugim slučajevima u kojima je važno da se otkrije falsifikat ili manipulacija.

Glava 2

Šta je digitalni potpis?

Digitalni potpis je jedan od najvažnijih kriptografskih alata koji je danas u širokoj upotrebi. Digitalni potpis omogućuje utvrđivanje autentičnosti elektronskog dokumenta, npr. elektronskog pisma, veb stranice ili neke slike. Digitalni potpisi su zasnovani na asimetričnoj kriptografiji. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije izmijenjen bez dozvole autora. Provjera vjerodostojnosti (eng. authentication) potpisanih dokumenata omogućena je korištenjem enkripcije, pri čemu enkripcija predstavlja postupak kodiranja podataka prije slanja, i samo ih ovlašćeni primalac može prihvatiti i dekriptovati a samim tim i pročitati sadržaj.

Uz to što osigurava autentičnost (identitet pošiljaoca utvrđuje se dekripcijom sadržaja poruke), digitalni potpis osigurava i očuvanost poruke (provjerom sadržaja poruke utvrđuje se da li se poruka mijenjala na putu do primaoca) te nemogućnost negacije slanja (pošiljalac ne može poreći učestvovanje u transakciji jer jedino on ima pristup do svog privatnog ključa kojim je potpisao poruku). Digitalni potpisi su lako prenosivi, ne mogu biti imitirani, i mogu se automatski označiti vremenskom markom. Korišćenjem algoritma digitalnog potpisa potpisnik stvara par ključeva, privatni i javni, ali moguće je i da se za potpisivanje svih poruka koristi isti par. Osnova

sigurnosti digitalnog potpisa je u tajnosti privatnog ključa dok je javni ključ svima dostupan, a omogućuje provjeru autentičnosti poruke.
Digitalni potpisi se mogu koristiti za sve vrste poruka, bilo da su one kodirane ili ne, i jednostavno primalac poruke može biti siguran kada je u pitanju identitiet pošiljaoca, kao i u to da je poruka stigla nepromijenjena.

2.1 Motivacija za stvaranje digitalnog potpisa

Ovdje ćemo ukratko opisati jedan primjer koji dovodi do zaključka zašto su digitalni potpisi ustvari zaista potrebni. Koristićemo školski primjer u komunikaciji između Alise i Boba.
Pretpostavimo da je Alisa odlučila da proda Bobu svoj automobil za 15000 €. Kako bi bila sigurna da je Bob dobio zvaničnu ponudu ,ona mu je sačinila dokument sa ponudom koji je na dnu potpisala svojim potpisom. Sada kada Bob čita dokument sa ponudom od Alise, on zaista zna da je ona to napisala, jer se na dnu potpisala svojim imenom. Ovo sve pričamo pod pretpostavkom da neko nije krivotvorio Alisin potpis. Jer sada se postavlja pitanje, kako Bob zaista može biti siguran da mu je Alisa poslala pismo, i da nije u pitanju neka pronevjera?
Možda ona zaista želi da proda auto, ali za 25000 €, i cijeli dokument sa ponudom je krivotvoren od strane nekog trećeg lica. Pretpostavimo da je ipak dokument vjerodostojan. Šta ako treće lice, Malori, prilikom transfera dokumenta, otvori isti, i iskoristi Alisin potpis na način što ga falsifkuje na neki drugi dokument.
Uzmimo u obzir sledeći scenario:
Malori je iskopirala Alisin potpis dok je dostavljala dokument Bobu, i sačinila svoj dokument u kome kaže da prodaje svoju kuću po zaista povoljnoj cijeni. Na dnu dokumenta potpisala je Alisu falsifikovanim potpisom. Čarli je primio dokument i došao

kod Alise sa dostavljenom ponudom. Pri komunikaciji između Čarlija i Alise, Alisa demantuje da je poslala takav dokument Čarliju. Čarli postaje uvrijeđen, i zahtijeva od Alise da ispuni svoju ponudu, i usput prijeti zakonskim mjerama pozivajući se na potpisani dokument. Koristeći ovaj scenario, dolazimo do nekih zaključaka koji su nam potrebni da bi kreirali dobar potpis.

ŠTA TREBA DA SADRŽI JEDAN DOBAR DIGITALNI POTPIS?

1. **Autentičnost** - ubijediće primaoca poruke, da je zaista poruka od Alise ;
2. **Nemogućnost falsifikovanja** - niko osim Alise nije mogao potpisati tu poruku;
3. **Nemogućnost umnožavanja** - čak iako je poruka dospjela u ruke treće osobe, treća osoba nije u mogućnosti da iskoristi njene detalje ili potpis iz poruke;
4. **Nemogućnost promjene** - potpisani dokument ne može biti izmijenjen ni u kom smislu;
5. **Nemogućnost odbacivanja potpisa** - Alisa ne može naknadno tvrditi da ona nije potpisala taj dokument;

Sve nam ovo govori, da potpis u kombinaciji "olovka-papir", zaista nije zadovoljavajuće rješenje. Zamislimo samo situaciju da je Alisa došla kod Boba sa potpisanom ponudom da mu zaista proda auto za 15000 €. Dok je Bob kratko izašao, ona je izmijenila drugu cifru na dokumentu iz ”5” u "8". Kada se Bob vratio, zatekao je da auto više ne košta 15000 €. Automobil sada košta 18000 €. Bob ulaže prigovor na cijenu, međutim Alisa ga uvjerava da nije dovoljno dobro obratio pažnju na dokument sa ponudom. Isto tako Alisa je možda u međuvremenu odustala od prodaje svog automobila, i Bob je došao kod nje sa dostavljenom ponudom, ali ona sada tvrdi da ona nikada nije poslala Bobu dokument, i da je kompletna ponuda falsifikovana.

Korišćenjem kriptografije, zaista možemo zadovoljiti sve uslove koje smo gore naveli za kreiranje kvalitetnog potpisa.

Jedna od bitnijih razlika u odnosu na potpis "olovka-papir", je ta da se prilikom svake druge poruke, potpis mijenja, u stvari mijenja se funkcija koja ujedinjuje poruku sa potpisom pošiljaoca poruke. Na drugoj strani bez obzira od sadržaja poruke, potpis na papiru ostaje isti. Ovo u suštini i dovodi do krivotvorenja potpisa, lako ga je prenijeti na drugi dokument. Uvođenjem opisanog rješenja, svodimo ovu mogućnost na veoma malu vjerovatnoću.

Glava 3

Principi digitalnog potpisa

Mogućnost dokaza da je određena osoba generisala poruku je veoma važna kako u realnom tako i u digitalnom svijetu. U prethodnom poglavlju smo opisali kakve se sve situacije mogu desiti prilikom falsifikovanja čovjekovog potpisa načinjenog rukom i olovkom. Kao i kod ručnog potpisa, samo osoba koja je kreirala digitalnu poruku može generisati i validan digitalni potpis. Da bi ovo postigli koristićemo principe asimetrične kriptografije. Osnovna ideja je da osoba koja potpisuje poruku koristi privatni ključ, a osoba koja prima poruku koristi odgovarajući javni ključ. Pored asimetrične, postoji i simetrična kriptografija, koja koristi iste ključeve za enkripciju i dekripciju, i mnogo joj je lakše ući u trag i izvršiti napad na nju. Mi ćemo se dalje u radu uglavnom fokusirati na asimetričnu kriptografiju.

3.1 Enkripcija sa javnim i privatnim ključem

Prilikom kreiranja 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 omogućuju provjeru potpisa. Privatni ključevi dostupni su samo

svojim vlasnicima čime je onemogućeno lažno predstavljanje ili umnožavanje potpisa. Podaci koji se obilježavaju digitalnim potpisom skraćeno se nazivaju porukom. U postupku stvaranja digitalnog potpisa, da bi dobili sažeti otisak poruke (eng. message digest) koristi se sigurna jednosmjerna funkcija, tzv. SHA (eng. Secure Hash Algorithm) funkcija. 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 potpisom, šalje primaocu koji pomoću javnog ključa pošiljaoca utvrđuje vjerodostojnost poruke i samog čina digitalnog potpisa. U postupku provjere potrebno je koristi SHA algoritam jednak onom korišćenom prilikom stvaranja potpisa.

3.2 Heš funkcija i njene osobine

Kriptografska heš funkcija je deterministički postupak koji uzima proizvoljan blok podataka i vraća niz bita fiksne dužine, tj. heš vrijednost. Ukoliko se podaci slučajno ili namjerno promijene, mijenja se i heš vrijednost. Podaci koji se kodiraju često nazivamo porukom, a heš vrijednost zovemo sažetak ili otisak poruke.

Idealna kriptografska heš funkcija ima četiri glavne karakteristike:

- Za bilo koju poruku lako je izračunati heš vrijednost;
- Za zadatu heš vrijednost nemoguće je pronaći originalnu poruku;
- Nemoguće je promijeniti sadržaj poruke, a da se njena heš vrijednost ne promijeni;
- Nemoguće je pronaći dvije poruke koje imaju istu heš vrijednost;

Naveščemo par razloga koji daju prednost potpisa heširane verzije poruke u odnosu na kompletnu poruku:

Efikasnost: potpis će biti značajno kraći i zbog toga dobijamo na uštedi vremena jer je heširanje u praksi brža operacija od samog potpisivanja.

Kompatibilnost: poruke su obično predstavljene kao nizovi bita, ali neke šeme potpisivanja funkcionišu na drugačiji način unutar različitih domena (npr. u slučaju RSA, računa se po modulu N). Korišćenjem heš funkcije možemo proizvoljnu poruku pretvoriti u odgovarajući format.

Integritet: bez korišćenja heš funkcija, tekst koji treba potpisati se mora podijeliti u blokove koji su dovoljno mali da bi se šema potpisivanja mogla direktno primijeniti na takve blokove. Štaviše, primalac potpisane poruke nije u stanju da prepozna potpis ukoliko svi blokovi nisu prisutni u odgovarajućem redosljedu.

3.3 Digitalni sertifikat

Digitalni sertifikati koriste se kod zahtjevnijih implementacija enkripcije s javnim ključem, npr. kod veb servera. Digitalni sertifikat može da se shvati kao digitalna lična karta, jer sadrži podatke o korisniku sertifikata i podatke o izdavaocu sertifikata, i putem njega možemo drugoj osobi dokazati svoj identitet. Radi se o sertifikatu kojeg izdaje jedno ili više ovlašćenih tijela (eng. Certificate Authority), a koja predstavljaju dio PKI (eng. public key infrastructure) sistema. 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., i time sprječavaju neovlašćen pristup podacima objavljivanjem lažnog javnog ključa. O ovome ćemo pričati detaljnije u poglavlju o elektronskom poslovanju.

Pored PKI sistema postoji i Mreža povjerenja (eng. web of trust), i koristi se kod PGP (eng. Pretty Good Privacy), GnuPGP i drugih sistema kompatibilnih sa

OpenPGP [1] standardom. PGP je neka vrsta hibridnog sistema jer kombinuje i simetričnu i asimetričnnu enkripciju. Podaci se prije šifrovanja pakuju, ukoliko je to moguće. Ovo nam daje dvije prednosti:

Prva je ta što je manja količina podataka za prenos. Druga prednost je dodatna sigurnost, jer se pakovanjem poruke u djelove eliminiše mogućnost sličnosti između djelova. Mnoge tehnike kriptoanalize upravo koriste te slične djelove unutar izvornog fajla koji se šalje kako bi probili zaštitu. Ovdje se vodi računa o veličini djelova fajla, pa fajlovi koji su prekratki neće biti podijeljeni već se šalju u svom izvornom obliku. Nakon što se fajl podijeli i upakuje u djelove, PGP pravi privremeni ključ, i to na način generisanja slučajnog broja koji se dobija na osnovu pokreta korisnika mišem kao i tastature, koji su u tom trenutku takođe nasumični.

Ovaj ključ ima samo jednokratnu upotrebu jer se u PGP algoritmu podaci inače šifruju simetričnom enkripcijom. Međutim sami privremeni ključ šifruje se asimetričnom enkripcijom i pridružuje se već šifrovanim podacima.

Kod dešifrovanja koristi se inverzan proces. Prvo PGP pomoću tajnog ključa dešifruje privremeni ključ, a zatim se dešifruju i podaci.

[1] OpenPGP predstavlja protokol koji se koristi za kriptovanje komunikacije putem e-maila,a zasniva se na kriptografiji javnog ključa

Glava 4

Algoritmi digitalnog potpisa

DS algoritmi uopšteno se sastoje od tri osnovna koraka:
Stvaranja javnog i privatnog ključa, stvaranja digitalnog potpisa na osnovu sažetka poruke (korišćenje već opisane heš funkcije) i privatnog ključa, i na kraju utvrđivanja vjerodostojnosti potpisane poruke korištenjem javnog ključa pošiljaoca. U nastavku teksta opisaćemo tri najčešća algoritma za stvaranje i provjeru digitalnog potpisa: RSA, DSA i ECDSA.

4.1 RSA

RSA (Rivest, Shamir, Adleman) algoritam moguće je koristiti pored potpisivanja i za kriptovanje zadate poruke. Pošiljalac poruku potpisuje pomoću vlastitog privatnog ključa, a kriptuje korišćenjem javnog ključa primaoca. Nakon što poruka stigne, primalac dekriptuje poruku pomoću vlastitog privatnog ključa, a provjera vjerodostojnosti potpisa vrši se uz korišćenje potpisnikovog javnog ključa. RSA šema digitalnog potpisa je bazirana na RSA sistemu enkripcije. Njena sigurnost počiva na težini problema faktorisanja proizvoda dva velika prosta broja. Algoritam se sastoji od sljedećih koraka:

1. Generisanje RSA ključeva

2. Generisanje RSA potpisa i kriptovanje poruke

3. Dekriptovanje poruke i utvrđivanje vjerodostojnosti potpisa

Da bi najbolje pokazali primjer algoritma koristićemo primjer iz udžbenika u komunikaciji između Boba i Alise.

4.1.1 Generisanje RSA ključeva

Pretpostavimo da Bob želi da pošalje Alisi potpisanu poruku x. Da bi kreirao par ključeva (javni i privatni) koristiće RSA enkripciju. Postupak biranja ključeva vrši se na sledeći način:

Bob vrši generisanje RSA ključeva

1. Nasumično bira dva velika prosta broja p i q

2 .Računa modul $n_1 = pq$

3. Zatim računa količnik $\phi(n_1) = (p-1)(q-1)$

4. Bira cijeli broj e_1 takav da vrijedi $1 < e_1 < \phi(n_1)$, i da e_1 i $\phi(n_1)$

nemaju zajedničkih djelitelja osim broja 1

5. Računa d_1 , tako da zadovoljava kongruenciju $d_1 e_1 \equiv 1(\mod \phi(n_1))$,

odnosno da vrijedi $d_1 e_1 = 1 + k\phi(n_1)$, za neki cijeli broj k

6. Javni ključ se sastoji od modula n_1 i javnog eksponenta e_1,

a privatni ključ se sastoji od modula n_1 i privatnog eksponenta d_1.

Konačno, Bob je kreirao parametre za ključeve:

a. Bobov privatni ključ: $k_{pr} = (n_1, d_1)$

b. Bobov javni ključ: $k_{pub} = (n_1, e_1)$

4.1.2 Generisanje RSA potpisa i kriptovanje poruke

Kao što ćemo vidjeti u protokolu ispod, Bob računa potpis s za poruku x na taj način što enkriptuje poruku x sa svojim privatnim ključem.Njegovo vlasništvo nad privatnim ključem ga identifikuje kao vlasnika potpisane poruke. Bob nadovezuje potpis s na poruku x i taj par šalje Alisi. Potpis računa na sledeći način:

Bob generiše RSA potpis i kriptuje poruku

1. Računa heš vrijednosti poruke $M : x = HASH(M)$, gdje je HASH kriptografska heš funkcija, kao npr. $SHA - 1$
2. Računa potpis $s = h^{(d_1 \mod n_1)}$
3. Nakon što je izračunao, dodaje potpis poruci. Nakon ovoga Bob kriptuje poruku:
4. Uzima javni ključ od primaoca poruke (n_2 i e_2)
5. Iz poruke M dobija se primjenom dogovorenog povratnog protokola (eng. padding scheme) broj m, tako da vrijedi $m < n$
6. Računa kriptovanu poruku $c = m^{e_2} \mod n_2$

4.1.3 Dekriptovanje poruke i utvrđivanje vjerodostojnosti potpisa

Nakon što je Bob poslao, Alisa prima potpisanu poruku i dekriptuje je pomoću Bobovog javnog ključa. Ako se x_1 i x poklapaju, Alisa zna dvije važne stvari: prvo, autor poruke posjeduje Bobov privatni ključ, i ako samo Bob ima pristup tom ključu, onda je samo Bob mogao biti taj koji je potpisao poruku.

Drugo, poruka nije izmjenjena prilikom prenosa, tako da je integritet poruke zagarantovan. Ovim su ispoštovana dva najveća kriterijuma bezbjednosti.

Alisa dekriptuje poruku i verifukuje RSA potpis

1. Alisa prvo dekriptuje poruku. Iz primljene poruke c izvlači m i to:

$m = c^{d_2} \mod n_2$

2. Koristeći inverzni protokol iz koraka enkrpicije iz prethodnog poglavlja (5.), iz m računa izvornu poruku M.

Nakon što je dekriptovala poruku, Alisa provjerava vjerodostojnost potpisa:

3. Računa heš vrijednost poruke $M : x = HASH(M)$, gdje je HASH funkcija jednaka onoj korištenoj prilikom stvaranja potpisa.

4. Računa $x_1 = s^{(e_1 \mod n_1)}$

5. Potpis je vjerodostojan ako vrijedi $x_1 = x$.

4.2 DSA

DSA (eng. Digital Signature Algorithm) algoritam propisan je DSS (eng. Digital Signature Standard) standardom savezne vlade Sjedinjenih Američkih Država i koriste ga sve civilne vladine organizacije te sve nevladine kompanije i organizacije koje sarađuju s vladom. Algoritam je 1991. godine patentirao David W. Kravitz, bivši zaposleni NSA (eng. National Security Agency) agencije. DSA algoritam se za razliku od RSA ne može koristiti za enkripciju iz razloga što to nije bilo poželjno, (sa tačke gledišta američke vlade) jer su u to vrijeme i dalje bila na snazi stroga ograničenja za izvoz kriptografskih alata iz SAD-a. Nasuprot tome, DSA implementacija se može koristiti samo za potpisivanje, i zbog toga je bilo lakše da se izvezu sistemi koji uključuju samo funkcionalnost potpisa.

DSA algoritam se kao i RSA sastoji iz tri koraka:

1. Generisanje DSA ključeva
2. Potpisivanje DSA poruke
3. Utvrđivanje vjerodostojnosti poruke

4.2.1 Generisanje DSA ključeva

Prvo je neophodno odlučiti se za dužinu ključeva koje ćemo koristiti za potpisivanje. Ovo je primarni kriterijum jačine tj. sigurnosti samog potpisa. Mi ćemo koristiti parametre za ključeve iz originalnog DSS-a, a oni mogu biti i drugačiji. Ostale kombinacije nalaze se u tabeli ispod.

p	q	potpis
1024	160	320
2048	224	448
3072	256	512

Tabela1. Dužina u bitima različitih parametara potpisa za DSA

Generisanje DSA ključeva

1. Biramo 160 - bitni prost broj q

2. Zatim biramo L-bitni prost broj p tako da vrijedi: $p = qz + 1$ za neki cijeli broj z, gdje je $512 \leq L \leq 1024$, $L|64$

3. Nakon toga biramo h tako da vrijedi: $1 < h < p - 1$, $\alpha = h^z \mod p > 1$

4. Generišemo nasumični broj d, tako da vrijedi: $0 < d < q$

5. Računamo $\beta = \alpha^d \mod p$

6.Dobijeni ključevi su :

$K_{pub} = (p, q, \alpha, \beta)$ je javni ključ,

$K_{pr} = (d)$ je privatni ključ

4.2.2 Generisanje DSA potpisa

DSA potpis se sastoji od para cijelih brojeva (r, s). Pošto je svaki od parametara dugačak samo 160 bita, ukupna dužina potpisa je 320 bita. Korišćenjem privatnog i javnog ključa, potpis za poruku x se računa na sljedeći način:

Generisanje DSA potpisa

1. Generišemo nasumični broj k, tako da vrijedi: $0 < k < q$
2. Računamo $r = (\alpha^k \mod p) \mod q$
3. Nakon toga računamo $s = (k^{-1}(SHA-1(m) + dr)) \mod q$, gdje je $SHA-1(m)$ tzv. heš funkcija primijenjena na poruci m koja računa 160-bitni sažetak poruke m, što u stvari predstavlja njen „otisak“.
4. Ponavljamo postupak ako je $r = 0$ ili $s = 0$
5. Dobijamo potpis (r, s)

Otisak koji smo dobili možemo koristiti kao zamjenu za poruku m.

4.2.3 Verifikacija poruke

Proces verifikacije poruke sastoji se iz sledećih koraka:

Verifikacija poruke sa DSA potpisom

1. Ako je $0 < r < q$ ili $0 < s < q$ potpis se smara neispravnim,jer početni uslov nije zadovoljen.
2. Računamo pomoćnu vrijednost $w = s^{-1} \mod q$
3. Računamo $u1 = (SHA-1(m)w) \mod q$
4. Računamo $u2 = (rw) \mod q$
5. Na kraju računamo $v \equiv (\alpha^{u1}\beta^{u2} \mod p) \mod q$

Verifikaciju potpisa određujemo na sledeći način:

Ukoliko je $v \equiv r \mod q$, potpis je validan, u suprotnom potpis je nevalidan.

Potpis (r,s) se prihvata samo ako važi $v \equiv r \mod q$. U suprotnom, verifikacija nije uspjela. U slučaju da verifikacija nije uspjela, zaključujemo da su ili poruka ili potpis izmjenjeni prilikom prenosa ili javni ključ pošiljaoca nije ispravan.

4.2.4 Primjer slanja poruke kroz DSA

Prikazaćemo teorijski dio algoritma na praktičnom primjeru razmjene poruke:

Bob šalje poruku x Alis potpisanu DSA algoritmom. Uzećemo da je heš vrijednost poruke x :$h(x) = 26$. Potpis i verifikacija poruke vrše se na sledeći način:

Bob kreira ključeve

1. Bob bira $p = 59$.
2. Bob bira $q = 29$
3. Zatim bira $\alpha = 3$
4. Bira privatni ključ $d = 7$
5. $\beta = \alpha^d \equiv 4 \mod 59$ Ovim je Bob kreirarao parametre $(p, q, \alpha, \beta) = (59, 29, 3, 4)$.

Zatim potpisuje poruku:

Bob potpisuje poruku

6. Koristi već izračunatu heš vrijednost poruke: $h(x) = 26$
7. Zatim bira efemeralni ključ $k = 10$
8. Računa $r = (3^{10} \mod 59) \equiv 20 \mod 29$
9. Računa $s = (26 + 7 \times 20) \times 3 \equiv 5 \mod 29$ Bob je generisao potpis: $(x, (r, s)) = (x, (20, 5))$.

Šalje ga Alisi. Sada Alisa treba da verifikuje poruku. Ona računa sledeće parametre:

Alisa verifikuje poruku

10. $w = 5^{-1} \equiv 6 \mod 29$
11. $u1 = 6 \times 26 \equiv 11 \mod 29$
12. $u2 = 6 \times 20 \equiv 4 \mod 29$
13. $v = (3^{11} \times 4^4 \mod 59) \mod 29 = 20$
14. Na kraju provjerava da li je $v \equiv r \mod 29$, dobija da jeste$\rightarrow$ potpis je validan.

4.3 ECDSA

ECDSA (eng. Elliptic Curve DSA) algoritam je varijanta DSA algoritma koja u radu koristi skupove eliptičnih krivih. Uz istu mjeru zaštite ovaj algoritam rezultira manjom veličinom ključeva (u bitima) od DSA algoritma, pa samim tim i kraćim potpisom, uz približno jednako vrijeme izvođenja. Takođe treba napomenuti da na ovakvim kriptosistemima nema jakih napada pa je to i razlog uzimanja manjih veličina. Iz ovih razloga, algoritam digitalnog potpisa zasnovan na eliptičnim krivim (ECDSA) standardizovan je 1998. godine od strane Američkog nacionalnog instituta za standardizaciju (ANSI). Algoritam se kao i prethodna dva opisana (RSA,DSA) sastoji iz sledećih koraka:

1. Generisanje ECDSA ključeva
2. Generisanje ECDSA potpisa
3. Verifikacija poruke i utvrđivanje indentiteta pošiljaoca

4.3.1 Generisanje ECDSA ključeva

Eliptička kriva određena je skupom od šest parametara $T = (p, a, b, q, A, B)$, gdje je p cijeli broj koji određuje konačno polje ϕ_p, a dva elementa a, b iz ϕ_p određuju eliptičku krivu $E(\phi_p)$: $E : y^2 \equiv x^3 + ax + b \mod p$. Proces odabira ključeva je sledeći:

Generisanje ECDSA ključeva

1. Biramo slučajni cijeli broj d za koji važi $0 < d < q$.
2. Računamo $B = dA$.
3. Ključevi koje dobijamo su:

a. javni ključ: $k_{pub} = (p, a, b, q, A, B)$,

b. privatni ključ $k_{pr} = (d)$

4.3.2 Generisanje ECDSA potpisa

Postupak potpisivanja poruke sastoji se od sljedećih koraka:

Generisanje ECDSA potpisa

1. Biramo slučajan efemeralni ključ k_E za koji važi $0 < k_E < q$.
2. Računamo $R = k_E A$.
3. Računamo $r = x \mod A$, gdje je x- koordinata tačke $(x, y) = k_E q$
4. Računamo $s \equiv (h(x) + d \cdot r)k_E^{-1} \mod q$.
5. Dobijeni potpis je (r, s)

4.3.3 Verifikacija ECDSA potpisa

Proces verifikacije potpisa kroz ECDSA algoritam funkcioniše po sljedećem principu:

Validacija ECDSA potpisa

1. Računamo pomoćnu vrijednost $w \equiv s^{-1} \mod q$.
2. Računamo pomoćnu vrijednost $u_1 \equiv w \cdot h(x) \mod q$.
3. Računamo pomoćnu vrijednost $u_2 \equiv w \cdot r \mod q$.
4. Računamo $P = u_1 A + u_2 B$.
5. Verifikaciju potpisa $(x_P, (r, s))$ vršimo na sledeći način:

Ukoliko je $x_P \equiv q \mod r \rightarrow$ potpis je validan, u suprotnom potpis nije validan.

U posljednjem (5.) koraku, oznaka x_P označava x-koordinatu tačke P. Osoba koji vrši verifikaciju, potpis (r,s) prihvata kao validan samo ako x_P ima istu vrijednost kao i parametar r po modulu q. U suprotnom, potpis se smatra nevalidnim.

Glava 5

Digitalni potpis u elektronskom poslovanju

Brz razvoj informacione i telekomunikacione tehnologije dovodi do rasta i širenja poslovanja na globalnom nivou. Uvođenjem i sve većom primjenom kompjuterske obrade podataka i korišćenjem savremenih sistema i komunikacije, došlo je do promjena u poslovanju pravnih lica i razvoja elektronskog poslovanja. Poslovanje koje je zasnovano na savremenoj digitalnoj tehnologiji i koje omogućava da se transakcije prevashodno ostvaruju elektronskim putem, poznato je pod imenom Elektronsko poslovanje (eng. e-business).

Elektronsko poslovanje u Crnoj Gori najviše je zaživjelo upravo u bankama. Trenutno je u Crnoj Gori 13 banaka koje rade sa pravnim i fizičkim licama, i sve banke u svojoj ponudi imaju usluge elektronskog poslovanja, koje uključuje elektronsko bankarstvo na prvom mjestu.

5.1 Komunikacija i digitalno potpisivanje dokumenata u e-poslovanju

Svaka banka u Crnoj Gori ima svog provajdera koji joj nudi usluge elektronskog bankarstva, kao i svog ovlašćenog CA (eng. Certificate Authority) koji joj izdaje digitalne ceritikate za sigurnu komunikaciju.

5.1.1 Sertifikaciona tijela za izdavanje digitalnih sertifikata (CA)

Izdavanje digitalnih sertifikata vrše posebne firme (CA Certification Authority), koje imaju ulogu da provjere i utvrde nečiji identitet i nakon toga mu izdaju digitalni sertifikat , kojim se potvrđuje da određeni javni ključ zaista pripada toj osobi. Digitalni sertifikat mora da sadrži sledeće:

- Naziv organizacije;
- Dodatne podatke za identifikaciju (JMBG, BRLK, adresa, broj telefona);
- Javni ključ;
- E-mail adresa koja se vezuje kao digitalni potpis za mejl pošiljaoca;
- Datum do koga važi javni ključ;
- Naziv CA firme koja izdaje digitalni sertifikat;
- Jedinstveni serijski broj;

Od ovih podataka se formira sertifikat koji se na kraju šifruje koristeći tajni ključ CA. Za provjeru validnosti digitalno potpisanih poruka, Outlook Express zahtijeva informaciju za određeni digital ID, od odgovarajuće CA firme, koja šalje natrag informaciju o statusu digitalnog sertifikata. Kvalifikovani digitalni potpis se formira u skladu sa preporukom PKCS1 (Public Key Cryptographic Standard), a dužina modula u asimetričnom kriptografskom algoritmu mora biti minimalno 1024 bita.

PKCS1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog potpisa. Najčešće korišćeni standard za digitalne sertifikate je X.509.

5.1.2 Digitalno potpisivanje e-maila

Unutar svake banke postoji lokalno registraciono tijelo (LRA). To je jedno ili više pravnih lica koje je odgovorno za identifikaciju i autentikaciju budućih korisnika elektronskog bankarstva i koje raspolaže svom zvaničnom dokumentacijom klijenata. Ova osoba koristi svoj digitalni sertifikat kao sredstvo komunikacije, kako unutar banke, tako i eksterno sa raznim drugim kompanijama, bankama i sl. Na taj način ova osoba utvrđuje svoju autentičnost kao zaposlenog banke i zadužena je za svu zvaničnu komunikaciju između banke i drugih strana. U praksi, osoba koja predstavlja LRA podnosi zahtjev za izdavanje digitalnog sertifikata, sa svojim ličnim dokumentima, kao i email adresom za koju želi da veže potpis ka CA. CA provjerava identitet LRA osobe na osnovu ličnih dokumenata. Ako je sve u redu, CA kreira digitalni sertifikat sa digitalnim potpisom za zadatu email adresu koju je LRA poslao u svom zahtjevu. Sada LRA ima svoj digitalni ID, i želi sa nekim da komunicira. Uzećemo za primjer da zaposleni u banci kao e-mail servis koriste Microsoft-ovo rješenje Microsoft Outlook.

U MS Outlook-u, digitalni sertifikat je implementiran kao digital ID i sastoji se od javnog ključa (public key), privatnog ključa (private key) i digitalnog potpisa (digital signature). Pri svojoj prvoj komunikaciji, LRA šalje uz svoji digitalni potpis i svoj javni ključ ka osobi X. Da bi konačno potpisao svoju poruku koju je spremio, LRA mora unijeti odgovarajuću lozinku koja je vezana za digitalni sertifikat. Digitalni potpis se kreira na osnovu sadržaja same poruke koju LRA u banci kreira. Po

prijemu elektronskog dokumenta i digitalnog potpisa, primalac X prvo dešifruje digitalni potpis javnim ključem koji je dobio od pošiljaoca. Pošto većina komunikacionih softvera (među njima i MS Outlook kao vodeći) u sebi ima već sadržane javne ključeve odgovarajućih CA tijela kojima se vjeruje, osoba X će po prijemu poruke lako utvrditi validnost sertifikata osobe LRA. Dodatno, osoba X možda takođe posjeduje svoj digitalni sertifikat. Tada će osoba X, pri prijemu poruke, da bi pročitala sadržaj poruke od LRA, morati unijeti svoju lozinku (koja ovdje predstavlja privatni ključ). U ovom konkretnom slučaju, pri sledećoj komunikaciji između LRA i osobe X, osoba X neće morati više koristiti svoj privatni ključ kako bi pročitala sadržaj od LRA, jer su ključevi već razmijenjeni, i oni sada "vjeruju jedno drugom". LRA i osoba X takođe imaju mogućnost i da enkriptuju sadržaj koji šalju jedno drugom, ukoliko šalju izuzetno povjerljive podatke, a u komunikaciji se nalazi još osoba koji ne bi trebali da vide sadržaj poruke. MS Outlook koristi određenu vrstu DES algoritma za enkripciju, i u ovom slučaju poruka je dodatno zaštićena i niko treći je ne može pročitati, ali može vidjeti da je poslata.

Ovim je opisan samo mali dio primjene digitalnih sertifikata. Oni se danas u Crnoj Gori, osim u bankama, koriste i u Poreskoj Upravi, MUP-u i na raznim drugim instancama.

5.2 Digitalni potpis u e-bankingu i u e-trgovini

U poglavlju 5.1. opisali smo kako ovlašćena lica koriste digitalne sertifikate izdate od strane CA za komunikaciju. Na sličan način i pravna i fizička lica, kao klijenti različitih banaka, apliciraju za svoje digitalnih sertifikate. Za razliku od LRA predstavnika u bankama, njihova prvenstvena namjena je rad sa elektronskom bankom, autorizacija različitih transakcija i mogućnost plaćanja kroz razne e-banking softvere.

Ovlašćeno pravno ili fizičko lice, koristeći svoj digitalni sertifikat u komunikaciji između servera banke i svog računara kroz sigurni komunikacioni kanal, vrši transakcije novcem, povlači povjerljive podatke, radi sa računima banaka za koje je ovlašćeno. Ovlašćeni korisnik uz svaku transakciju kači svoj digitalni potpis, koji se na serveru banke oslikava imenom i prezimenom osobe koja je autorizovala određenu transakciju, i na taj način se u bilo kom momentu lako utvrđuje njegov identitet.

Ako recimo, određeni poslodavac otvara svoju veb prodavnicu, kojoj će klijenti pristupati putem određene veb stranice, i želi da svojim klijentima omogući plaćanje kreditnim karticama, kao i pristup povjerljivim informacijama, tada veb server na kojem je poslodavac 'postavio' veb prodavnicu treba da ima mogućnost da radi kao siguran veb server. (eng. Secure Web Server)

Prvi preduslov za to je taj veb server dobije svoj digitalni sertifikat od odgovarajućeg CA. Poslodavac tada mora popuniti zahtjev za izdavanje sertifikata ka CA, na način na koji smo već opisali, i nakon što ga dobije on je spreman za rad. Postavlja svoj sertifikat na svoj server, i sada čeka klijente da pokupe njegov sertifikat po prvi put i učine transakciju povjerljivom.

5.2.1 Kako učiniti elektronske transakcije putem digitalnog potpisa bezbjednim?

SSL (eng. Secure Socket Layer) protokol koji je razvila firma Netscape, je trenutno najcešće korišćen metod za obavljanje sigurnih transakcija na mreži. Podržava ga većina veb servera kao i klijenata uključujući Microsoft Internet Explorer i Netscape Navigator. SSL obezbjeđuje privatnost, integritet podataka i autentičnost pošiljalaca korišćenjem kombinacije šifrovanja javnim ključem, simetričnog šifrovanja, i digitalnih sertifikata. Transakcija korišćenjem SSL protokola uključuje sledeće aktivnosti:

• server šalje svoj digitalni sertifikat klijentu;

• klijent provjerava da li je sertifikat izdat od strane CA;

• klijent i server razmjenjuju javne ključeve;

• klijent generiše tajni ključ koji se koristi samo u započetoj transakciji (najčešće unosi odgovarajući pin kod ili lozinku);

• klijent šifruje generisani tajni ključ, korišćenjem serverovog javnog ključa i šalje ga serveru;

• u daljem toku transakcije server i klijent koriste isti tajni ključ metodom simetričnog kriptovanja;

Glava 6

Sigurnosni rizici prilikom primjene digitalnog potpisa i mjere zaštite

Korišćenje digitalnog potpisa sa sobom nosi određene rizike o kojima smo pričali u samom uvodu u ovu tematiku. Potpis može biti falsifikovan, presretnut, povjerljivi sadržaj može biti pročitan a da toga nisu svjesni ni pošiljalac ni primalac poruke.
Nauka koja se bavi razbijanjem šifri, dekodiranjem, zaobilaženjem sistema autentifikacije ,uopšteno provaljivanjem kriptografskih pravila i protokola naziva se **k**riptoanaliza. Dakle, kriptoanaliza je naučna disciplina koja proučava postupke otkrivanja otvorenog teksta bez poznavanja ključa ,ili obratno postupke otrkivanja ključa uz poznavanje otvorenog ili kriptovanog teksta. Različite tehnike kriptoanalize nama su poznatiji kao napadi.
Najveća prijetnja podacima koji se prenose putem računarske mreže javlja se usled slabosti komunikacione opreme pomoću koje se vrši prenos podataka. Ugrožavanje podataka u računarskim mrežama se odnosi na prisluškivanje, analizu, mijenjanje, uklanjanje informacija kao i lažno predstavljanje. Treba napomenuti da do ovih napada može doći na bilo kom mjestu prenosa informacija od izvora do odredišta.
Napade na sigurnost možemo razdvojiti na pasivne i aktivne napade.

Pasivni napadi se odnose na sva prisluškivanja i nadgledanja informacija tokom prenosa, bez ikakvih izmjena. Ovom vrstom napada napadač na relativno jednostavan način dolazi do informacija. Pasivni napadi se teško otkrivaju. Kao najčešće korišćeni mehanizam zaštite od pasivnih napada primjenjuje se kriptovanje podataka koji se prenose putem komunikacionih linija. Kao algoritme za kriptovanje, koristimo već ugrađene algoritme koji nude e-mail ili drugi komunikacioni servisi, koji u kombinaciji sa našim privatnim ključem dodatno otežavanju čitanje ili tumačenje poruke osobama kojima nisu namenjeni.

Aktivni napadi, na drugoj strani su svi napadi koji vrše promjenu sadržaja ili toka informacija. Ova vrsta napada je daleko komplikovanija i teža za otkrivanje nego što su pasivni napadi. U aktivne napade se ubrajaju modifikacije paketa informacija koji se kreću putem mreže, slanje lažnih paketa, prekidi toka informacija kao i razne vrste preusmjeravanja paketa na mreži. Zbog raznovrsnosti ove vrste napada, mehanizmi zaštite moraju biti daleko komplikovaniji i napredniji nego kod pasivnih napada.

Navešćemo nekoliko napada koji su danas najprisutniji u svakodnevnoj korespodenciji i komunikaciji putem Interneta:

- *napad poznatim šifrovanim tekstom* : ovaj napad je i najteže izvesti, jer napadač poznaje samo šifrovani tekst i ništa više;

- *napad poznatim otvorenim tekstom* : napadač ima pristup i otvorenom tekstu i njemu odgovarajućem šifrovanom, i sprovodi analizu datih podataka sa ciljem pronalaženja ključa koji se koristi za šifrovanje;

- *napad odabranim otvorenim tekstom* : napadač može sam da bira otvorene tekstove i može da vidi njima odgovarajuće šifrovane tekstove. Ovaj tip napada se najčešće koristi za napade na asimetrične šifre kod kojih napadač, pošto zna javni ključ, može da šifruje otvorene tekstove po svom izboru;

- *napad adaptivnim odabranim otvorenim tekstom*: napadač ima pristup šifri tako

da može da zada jedan otvoren tekst, dobije šifrovani rezultat, a zatim bira sledeći otvoreni tekst koji će šifrovati ali tako da postoji veza između dva otvorena teksta sa ciljem nalaženja veze između dva rezultujuća šifrovana teksta ;

- *napad odabrani šifrovanim tekstom* : Napad je isti kao odabrani otvoreni tekst samo što sada umjesto funkcije šifrovanja posmatramo dešifrovanje;

- *standardni ASCII napad* : pripada grupi napada „samo šifrovani tekst“, i primjenjuje se na šifre kod kojih se otvoreni tekst predstavlja standardnim ASCII kodom;

- *meet in the middle napad* : osmislili su ga Diffie i Hellman, i spada u grupu napada „poznat otvoren tekst“. To je napad na blok šifre kod kojih se šifrovanje vrši dva puta sa dva različita ključa, sa ciljem povećanja sigurnosti šifre;

6.1 Kako korisnik može povećati svoju sigurnost?

Skoro svi programi za enkripciju umjesto brojeva kao ključa, koriste niz slova i brojeva odnosno lozinku. Svi algoritmi ovog tipa su generalno sigurni, bez obzira da li su simetričnog ili asimetričnog tipa, međutim lozinci se uvijek može ući u trag ukoliko se korisnik ne pridržava nekih osnovnih pravila. Idealna kombinacija zaštite je kada korisnik posjeduje varijantu "hardver - softver".

Pod ovim podrazumijevamo da korisnik posjeduje digitalni sertifikat u kombinaciji sa jakom lozinkom koju je kreirao i koja je vezana za taj sertifikat.

Mi ćemo navesti nekoliko osnovnih principa kojih se korisnik treba pridržavati prilikom kreiranja lozinke:

• Idealno je za lozinku izabrati nasumični niz slova i brojeva, gdje bi neka minimalna dužina lozinke bila makar 8 karaktera. Međutim korisnici izbjegavaju ovakve lozinke jer ih teško pamte, pa upotrebljavaju riječi iz svakodnevnog govora.

• Nipošto ne treba koristiti riječi koji se lako mogu pogoditi na osnovu poznavanja vlasnika potpisa kao što su: godina rođenja, ime roditelja ili ljubimca, djeteta i slično.

• Ako već koristi neku smislenu lozinku, korisnik bi trebao povesti računa da ona sadrži više od jedne riječi, spojene nekim znakom interpunkcije.

Treba imati u vidu da ako neko dođe do vaše lozinke i učini malverzaciju, npr. prebaci novac sa vašeg računa na neki drugi račun ili izvrši internet kupovinu, banke su tada nemoćne da previše pomognu, jer zakon ne prepoznaje ovakav vid prevare, pogotovo ako se radi o manjim sumama. Zato je uvijek potrebno naglasiti budućim korisnicima usluga elektronskog poslovanja da povedu računa o svojoj bezbjednosti, u ovom slučaju o lozinci koju kreiraju za svoj elektronski nalog.

Glava 7

Zaključak

Digitalizacija i sve češća upotreba Interneta u poslovnim primjenama dovele su do potrebe sigurne i pouzdane komunikacije kao i utvrđivanja autentičnosti dokumenata. Digitalni potpisi se sve više, zavisno od toga koliko se često koriste i koliko su važni dokumenti koji se potpisuju, približavaju klasičnim potpisima i polako ih isključuju iz upotrebe. Kada to kažemo mislimo na povećanje današnjih trendova u korištenju digitalnog potpisa. Oni će sa vremenom potpuno zamijeniti pisane potpise u primjenama od dugoročnih korporativnih ugovora do ličnih pisama i dnevnika. Mnogi informativni analatičari i stručnjaci slažu se kako će, kroz određeno vrijeme, za pokretanje svih programskih paketa i pristup svim datotekama biti potreban odgovarajući digitalni potpis.

Sve češća upotreba digitalnih potpisa dovodi do veće učestalosti napada – pokušaja lažnog predstavljanja, i ostalih malverzacija. Zbog toga je važno definisati politiku upravljanja digitalnim potpisima koja detaljno propisuje dozvoljene i sigurne načine korišćenja digitalnih potpisa, propisuje korišćenje infrastrukture digitalnih potpisa i korišćenje sigurnosnih normi. Iz tog razloga neohphodno je standardizovati algoritme koji implementiraju digitalne potpise na nivou države, i na nivou samog Interneta, npr. od strana organizacija kao što su IEEE (eng. Institute of Electrical Electronics

Engineers) ili ANSI (eng. American National Standards Institute).

Oko primjene digitalnog potpisa u praksi postoje još brojna otvorena pitanja. Brojni analitičari ukazuju nam na nedovoljnu provjerenost i kvalitet tehnoloških rješenja koja bi se konkretno trebala primjenjivati u praksi, prije svega u smislu sigurnosti i pouzdanosti. Vjerovatno takav stav proizilazi i iz činjenice da zakonska regulativa ne propisuje koja tehnološka rješenja valja primjenjivati, odnosno barem koje standarde ona moraju zadovoljavati.

Budućnost digitalnog potpisa je u svakom slučaju svijetla. Koja god tehnologija ili algoritam bili korišteni, teško je već danas zamisliti svijet računarskih mreža bez odgovarajućih algoritama autentifikacije. Uprkos tome što je digitalni potpis dio digitalnog svijeta koji se vrlo brzo mijenja i prihvata novitete, pri oslanjanju na jedan od algoritama za digitalni potpis važno je razmišljati ne samo o današnjoj snazi i moći računara, već i o nadolazećim računarima koji će eventualno biti dovoljno snažni za krivotvorenje potpisa pukom silom (engl. „brute force attack“). Druga, uvijek prisutna neugodna mogućnost je da već danas postoji način „razbijanja“ digitalnih potpisa pomoću nekih brzih metoda faktorizovanja (velikih) brojeva, koje bi tad ugrozile ne samo kripto zaštitu algoritama poput danas najrasprostranjenijeg RSA, već bi vrlo lako osporile i digitalne potpise (načinjene sa RSA ili sličnim algoritmom). Međutim, današnje analize i teorije nam govore da se ovo ne može dogoditi u skorijoj mogućnosti, te se služimo činjenicama da je digitalni potpis danas skoro neprobojan, i kao takav, najsigurnije rješenje kao sredstvo pouzdane komunikacije.

Bibliografija

[1] William Stallings, Cryptography and Network Security Principles and Practices, 2005

[2] Wenbo Mao, Modern Cryptography: Theory and Practice.
Prentice Hall PTR, 2003

[3] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978.

[4] Hrvatska Akademska i istraživačka mreža,Digitalni Potpis,2007
`http://www.cis.hr/www.edicija/LinkedDocuments/`
`CCERT-PUBDOC-2007-02-182.pdf`

[5] Alasdair McAndre, Introduction to Cryptography with
Open-Source Software,2012

[6] Darinka Vučinić, Univerzitet Crne Gore, Prirodno-matematički fakutlet, Digitalni Potpis, 2010

[7] Pretty Good Privacy , Wikipedia (Pretty Good Privacy)
`https://sr.wikipedia.org/sr/Pretty_Good_Privacy`

[8] James Price, Cryptanalysis and Brute Force Attacks