Digitalni potpis: Načela i primjena

Bastašić, Suzana

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

SUZANA BASTAŠIĆ

DIGITALNI POTPIS: NAČELA I PRIMJENA

Završni rad

Pula, rujan 2019. godine

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

SUZANA BASTAŠIĆ

DIGITALNI POTPIS: NAČELA I PRIMJENA

Završni rad

JMBAG: 0303007697, izvanredni student

Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijsko-komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Mentor: prof. dr. sc. Mario Radovan

Pula, rujan 2019. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA
o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____
_____
koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.
Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SADRŽAJ

1. Uvod 1

2. Povijest i pojam kriptografije 2

3. Algoritmi za kriptiranje 5

3.1. Enkripcija sa privatnim ključem – simetrični algoritmi 5

3.2. Enkripcija s javnim ključem – asimetrični algoritmi 6

3.2.1. RSA algoritam 9

3.2.2. DSA (Digital Signature Algorithm) 10

4. Izdavanje i vrste certifikata 12

4.1. Certifikat za udaljeni e-Potpis (ePotpis u oblaku) 13

4.2. Soft certifikat 15

4.3. Certifikati na uređaju 15

5. Primjena digitalnog potpisa 17

5.1. Potpisivanje dokumenata 17

5.2. Slijepi potpis 18

5.3. Potpis u web aplikacijama 19

5.4. Multimedijski sadržaji 20

6. Zakoni 21

6.1. Zakoni u Hrvatskoj 21

6.2. Zakoni u Europskoj Uniji 24

7. Zaključak 27

Literatura 28

1. Uvod

Pojam digitalni potpis (engl. *digital signature, DS*) odnosi se na tehnologiju koja omogućuje brzo i jednostavno poslovanje. Prema definiciji Hrvatskog enciklopedijskog rječnika, digitalni potpis je „šifriranje kojim se dokazuje autorstvo, tj. izvor elektroničkog dokumenta“. Digitalni potpis je zamjena za tradicionalno potpisivanje dokumenata koja zakonski jednako vrijedi kao vlastoručan potpis te se njime utvrđuje autentičnost (engl. *authentication*) nekog elektroničkog dokumenta. Autentičnost znači da je autor dokumenta poznat te da dokument nije ni na koji način mijenjan nakon što ga je ta osoba izradila. Osim autentičnosti, digitalni potpis osigurava i integritet (engl. *integrity*) i nepobitnost (engl. *non-repudiation*).

Rad obuhvaća pregled povijesti kriptografije gdje se opisuje razvoj upotrebe i načina šifriranja od svojih početaka do danas te se spominju najbitniji znanstvenici i inženjeri koji su doprinijeli razvoju digitalnog potpisivanja. Rad također opisuje vrste algoritama za kriptiranje, principe na kojima su temeljeni te njihovu sigurnost. Nadalje, u radu su opisani certifikati korišteni za digitalne potpise te kako se oni izdaju u Republici Hrvatskoj. U radu je navedeno i opisano nekoliko područja primjene digitalnog potpisa te zakone u Republici Hrvatskoj i Europskoj Uniji koji se trenutno primjenjuju.

2. Povijest i pojam kriptografije

Tijekom povijesti uspješnost neke vojske ovisila je o djelotvornoj komunikaciji. Iz tog razloga, poruke su se morale držati tajnima, kako neprijatelj ne bi došao do korisnih informacija. Ova tajnost dovela je do stvaranja posebnih odjela koji su bili zaduženi za šifriranje bitnih informacija.

Kako bi objasnili povijest digitalnog potpisa, moramo prvo istražiti povijest kriptografije. Riječ kriptografija je kombinacija grčkih riječi *krypto* koja znači skriveni i *graphene* koja znači pisati. Neki elementi kriptografije su se već pojavili kod starih Grka koji su koristili napravu za šifriranje nazvanu *skital* (Duajella, 2007.). Iako se poruke mogu prenositi skrivene, postoji rizik od pronalaženja skrivene poruke te se sadržaj može odmah pročitati. No kriptografija ima za cilj prikriti značenje poruke, a ne sakriti samu poruku. Prednost kriptografije je što ju treća strane ne može dešifrirati bez odgovarajućeg ključa.

Julije Cezar je često koristio kriptiranje poruka u vojne svrhe, te je po njemu nazvana supstitucija u kojoj je svako slovo zamijenjeno drugim, tri mjesta udaljenim slovom. U islamskoj kulturi su se kriptirali osjetljivi državni dokumenti, porezne knjige i upravni priručnici. Primjer je *Ada bal-Kuttaba*, priručnik iz 10. stoljeća u kojem se opisuje način kriptiranja. U 9. stoljeću, arapski znanstvenik al-Kindi opisao je svoju metodu kripto analize koja se temeljila na brojanju najčešćih slova u nekom jeziku te prebrojavanja znakova u kriptiranom dokumentu.

U Europi je u 15. stoljeću kriptografija već bila razvijena, no postoji mogućnost da je razvoj matematike i ostalih znanosti u arapskom svijetu imalo utjecaj i na razvoj kripto analize u Europi. Godine 1586. Blaise de Vigenère, francuski diplomat je objavio knjigu Rasprava o tajnom pisanju, u kojoj opisuje kriptiranje poruke pomoću 26 šifriranih abeceda. Nazvana prema njemu, Vigenèreova šifra koristila se tijekom čitavog 17. i 18. stoljeća, a nakon izuma telegrafa bila je često korištena za prijenos poslovnih tajni.

U 19. stoljeću, Charles Babbage projektirao je Diferencijalni stroj br. 1 te nešto kasnije Diferencijalni stroj br. 2, koji su u 20. stoljeću imali veliki utjecaj na kripto analizu. Babbage je također ostao poznati u povijesti jer je uspio razbiti Vigenèreovu šifru.

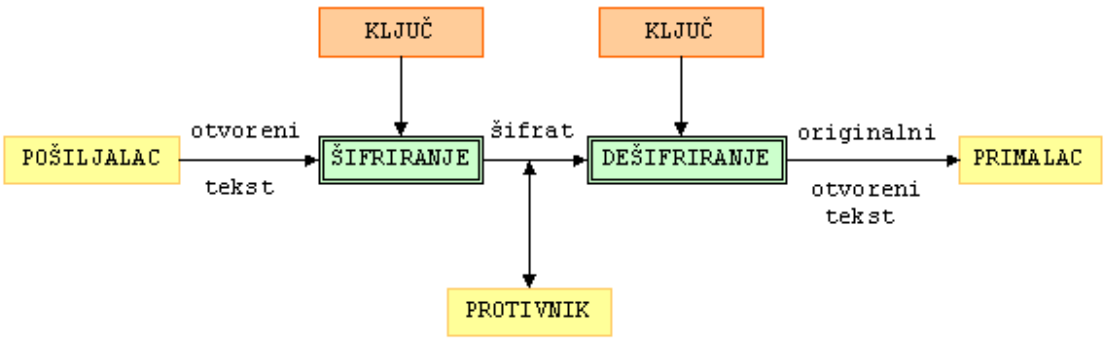
Kraj 19. stoljeća donio je izum radija, a skori početak Prvog svjetskog rata doveo je pitanje korištenja radija u vojne svrhe. Sa Babbageovim razbijanjem Vigenèreove šifre, kriptografija je trebala nove izume koji bi omogućili tajnost tijekom rata. Iako tijekom Prvog svjetskog rata nije došlo do značajnijih izuma, u poslijeratnim godinama kriptografi su se okrenuli tehnologiji. Njemački izumitelj Arthur Scherbius je 1918. godine patentirao svoj izum, uređaj Enigmu, koju je Njemačka prihvatila za vojnu uporabu te je 1925. godine započela masovna proizvodnja. Enigma je bila rotorska naprava kojom su pomacima rotora upravljali zupčanici koji su omogućavali nepravilan redoslijed, što je otežavalo dekripciju poruka. Sastojala se od tipkovnice, zaslona sa 26 žarulja koje su prikazivale šifrirani tekst, tri mehanička rotora te električne ploče. Prvi rotor se nakon šifriranog slova okretao za jedan kontakt, a kada bi napravio cijeli krug, okreti bi se nastavili na drugom rotoru. Kako bi povećao sigurnost Enigme bez dodavanja novih rotora, Scherbius je povećao broj početnih postavki (Duajella, 2007.). Prvi pomak u razbijanju šifri zapisanih koristeći Enigmu napravili su Poljaci, koji su nekoliko godina uspješno dešifrirali poruke, dok Nijemci nisu 1939. godine povećali broj mogućih ključeva. Nakon početka Drugog svjetskog rata, Britanci su, predvođeni Alanom Turingom, uspjeli razbiti šifre Enigme te pratiti Njemačke poruke, što je bio odlučujući faktor u pobjedi.

Poslije rata, nastavio se razvoj elektroničnih računala koja su se sada mogla iskoristiti za brže pretraživanje i razbijanje šifri, no i za stvaranje sve složenijih šifra. U počecima je kriptiranje računalima bilo ograničeno na vojsku, no kada su računala 60 – ih godina postala jeftinija i pristupačnija, tvrtke su ih počele primjenjivati za kriptiranje osjetljivih podataka (Singh, 2003.). Najupečatljiviji izum u povijesti kriptografije je koncept kriptografije sa javnim ključem, prvi puta objavljen 1976. godine od strane autora Bailey Whitfield Diffie i Martin Hellman. Iako autori u to vrijeme nisu imali praktični primjer upotrebe ovoga algoritma, ideja je izazvala zanimanje i daljnje istraživanje. Godine 1978. autori Ron Rivest, Adi Shamir i Leonard Adleman su izumili prvi praktičan primjer uporabe kriptografije sa javnim ključem, danas nazvan RSA algoritam. RSA algoritam je prvi algoritam prikladan za potpisivanje i enkripciju podataka. Prvi međunarodni standard za digitalni potpis (ISO/IEC 9796) je prihvaćen 1991. godine te je zasnovan na RSA algoritmu. Vlada SAD - a je 1994. godine prihvatila Digital Signature Standard, dokument koji je zasnovan na ElGamal nacrtu kriptografije sa javnim ključem, objavljene 1985. godine od strane autora Taher Elgamal. Godine 1985. autori Neal

Koblitz i Victor S. Miller predstavljaju korištenje eliptičkih krivulja nad konačnim poljima u algoritmima s javnim ključem. Na temelju njihovoga rada nastao je ECDSA algoritam (engl. Elliptic Curve DSA) koji pomoću manjeg ključa i približno jednakim vremenom izvođenja daje sigurniji digitalni potpis.

Prema Dujella (2007) „kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Osnovna namjena kriptografije je omogućiti dvjema osobama – pošiljatelju (Alice) i primatelju (Bob) – komuniciranje preko nesigurnog kanala na način da treća osoba (Eve) ne može razumjeti njihove poruke“. Pošiljalac šalje poruku koja može biti napisana na nekom jeziku (npr. engleskom ili hrvatskom) ili sadržavati neke numeričke podatke te ju transformira koristeći unaprijed određeni ključ. Rezultat transformacije je nečitljiv materijal koji se naziva šifrat (engl. *chipertext*). Nakon toga, pošiljatelj šalje kriptiranu poruku, tj. šifrat preko nekog komunikacijskog kanala, npr. telefonska linija, računalna mreža i sl. Primatelj može putem ključa dešifrirati zaprimljeni šifrat te pročitati poruku. Dešifriranje ili dekriptiranje je proces pretvaranja šifrata u originalnu poruku.

Ciljevi kriptografije su sljedeći: povjerljivost (engl. *confidentiality*), integritet sadržaja (engl. *data integrity*), autentifikacija (engl. *authentication*) te nepobitnost (engl. *non-repudiation*). Kriptografija pokušava adekvatno provesti navedene ciljeve u teoriji i praksi.



Slika 1: Primjer klasične kriptografije (Dujella A.; Maretić. M. Kriptografija)

3. Algoritmi za kriptiranje

Prije nego su računala ušla u široku uporabu, tj. prije nego su se dovoljno razvila, većina kriptografskih metoda šifriranja se bazirala na tajnosti šifre. Ali tako bazirani algoritmi su se pokazali dosta nepouzdani, te su se morale pronaći neke druge metode šifriranja.

Današnje metode šifriranja zasnivaju se na uporabi ključa. Ključ je najvažniji dio u pravilnom kriptiranju i dekriptiranju poruka. Ovisno o načinu korištenja ključa, razvile su se dvije klase algoritama. Simetrični algoritmi kriptiranja i asimetrični algoritmi kriptiranja. Razlika je u tome da simetrični algoritmi koriste isti ključ za enkripciju i dekripciju neke poruke (ili se ključ za dekripciju može lako proizvesti iz originalnog ključa za enkripciju), dok asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju iste.

3.1. Enkripcija sa privatnim ključem – simetrični algoritmi

Simetrični sustav kriptiranja predstavlja metodu kriptiranja kod koje se za kriptiranje i dekriptiranje koristi isti tajni ključ. Osobe koje komuniciraju moraju unaprijed dogovoriti ključ koji će znati samo one. Simetrični algoritmi su brzi pa se mogu koristiti za šifriranje većih datoteka ili implementaciju u kripto-sisteme datoteka. Simetrične algoritme dijelimo u dvije grupe: *stream* šifriranje i blok šifriranje. *Stream* šifriranje radi tako da se enkripcija poruke originala vrši bit po bit, dok se kod blok šifriranja enkripcija vrši po blokovima podataka, tj. uzimaju se blokovi od više bitova (64, 128, 196, 256 ...) i kriptiraju se kao cjelina. Primjeri blok šifriranja su DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), AES/RIJNDAEL (Advanced Encryption Standard). Dekripcija se najčešće vrši inverznim kriptiranjem, tj. algoritam je isti, ali se pod-ključevi enkripcije koriste obrnutim redoslijedom.

Menezes et. al (2001) prikazuju sljedeći primjer simetričnog algoritma: neka je $A = \{A, B, C, \ldots, X, Y, Z\}$ skup slova engleske abecede. M i C su skupovi od pet znakova iz skupa A, ključ e je permutacija skupa A. Da bi kriptirali poruku na engleskom jeziku, poruka je podijeljena na skupove od pet slova te je permutacija e primijenjena na svakom slovu. Za dekriptiranje, koristi se inverzna permutacija $\mathrm{d} = e^{-1}$ koja se

primjenjuje na svakom slovu šifrata. Na primjer, e može biti permutacija koja mapira svako slovo abecede s onim koje je za tri mjesta dalje.

$$e = \begin{pmatrix} \text{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \text{D E F G H I J K L M N O P Q R S T U V W X Y Z A B C} \end{pmatrix}$$

Slika 2: Permutacija $\boldsymbol{e}$ (izvor: http://cacr.uwaterloo.ca/hac/)

Sljedeća poruka "*This chyper is certanly not secure*" se prvo dijeli na skupove od pet slova te se kriptira putem ključa e.

$$m = \text{THISC IPHER ISCER TAINL YNOTS ECURE}$$

$$c = E_e(m) = \text{WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH.}$$

Slika 3: Kriptiranje poruke $\boldsymbol{m}$ ključem $\boldsymbol{e}$ (Menezes et. al 2001, 2019-01-02, url)

Prednost simetričnog algoritma su brzina izvođenja te su korisni za šifriranje podataka koji se ne prenose, već se pohranjuju. Također, ključevi mogu biti kraći od onih za asimetrični algoritam. Nedostatak je problem sigurne razmjene tajnog ključa jer postoji opasnost od krađe ako se koristi neki od nesigurnih kanala. Osoba koja ukrade tajni ključ može čitati te mijenjati šifrirane podatke. U komunikaciji između dvije osobe, ključ se često mora mijenjati, po mogućnosti za svaku novu komunikacijsku sesiju.

3.2. Enkripcija s javnim ključem – asimetrični algoritmi

Godine 1976. Diffie i Hellman razvili su algoritam koji omogućava da se šifriranje izvede pomoću jednog ključa, a dešifriranje pomoću drugog ključa, te se smatraju začetnicima asimetričnog algoritma. Asimetrični algoritam se još naziva i algoritam sa javnim ključem jer se jedan ključ može objaviti javno. Najpoznatiji asimetrični algoritmi su RSA i Diffie-Hellman.

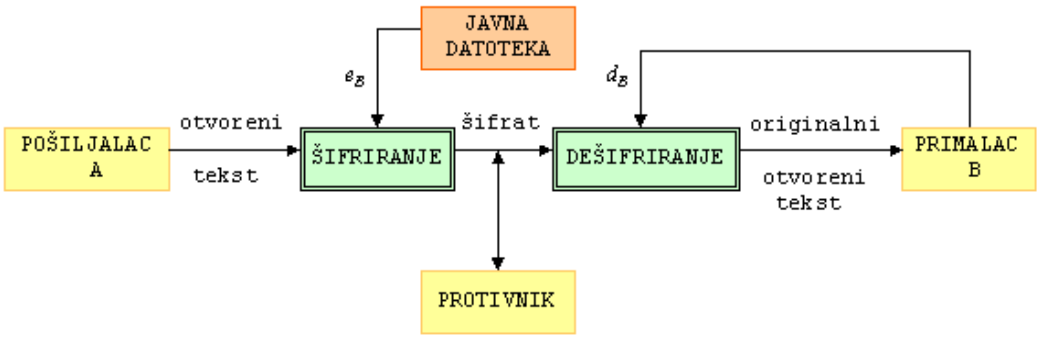
Kod asimetričnog algoritma, glavna ideja je da poznavanje funkcije za kriptiranje e_K ne označava mogućnost izračuna funkcije za dekriptiranje d_K. U ovom algoritmu bitno je korištenje jednosmjernih funkcija (engl. *one-way function*). Kod jednosmjerne funkcije f, izračun f je lagan, a izračun f^{-1} je težak. Ako imamo poznati podatak koji će nam olakšati izračun f^{-1} onda je funkcija f osobna jednosmjerna funkcija (engl. *trapdoor*

one-way function), gdje je taj poznati podatak skriveni ulaz, tj. *trapdoor*. U svom radu Dujella (2007) definira asimetrični algoritam kao "kripto-sustav s javnim ključem koji se sastoji od dviju familija $\{\mathrm{eK}\}$ i $\{\mathrm{dK}\}$ funkcija za šifriranje i dešifriranje (ovdje K prolazi skupom svih mogućih korisnika) sa svojstvom:

- Za svaki K je d_K inverz e_K.
- Za svaki K je e_K javan, ali je d_K poznat samo osobi K.
- Za svaki K je e_K osobna jednosmjerna funkcija.

e_K se zove javni ključ, a d_K tajni ili osobni ključ.".

Primjer korištenja asimetričnog ključa je sljedeći: primatelj poruke B šalje pošiljatelju poruke javni ključ e_B preko bilo kojega komunikacijskog kanala, dok drugi ključ d_B ostaje tajan. Pošiljatelj poruke A kriptira poruku m korištenjem ključa e_B te šalje šifrat $\mathrm{c} = e_B(\mathrm{m})$ primatelju poruke B. Primatelj poruke B dekriptira šifrat c pomoću tajnog ključa d_B.



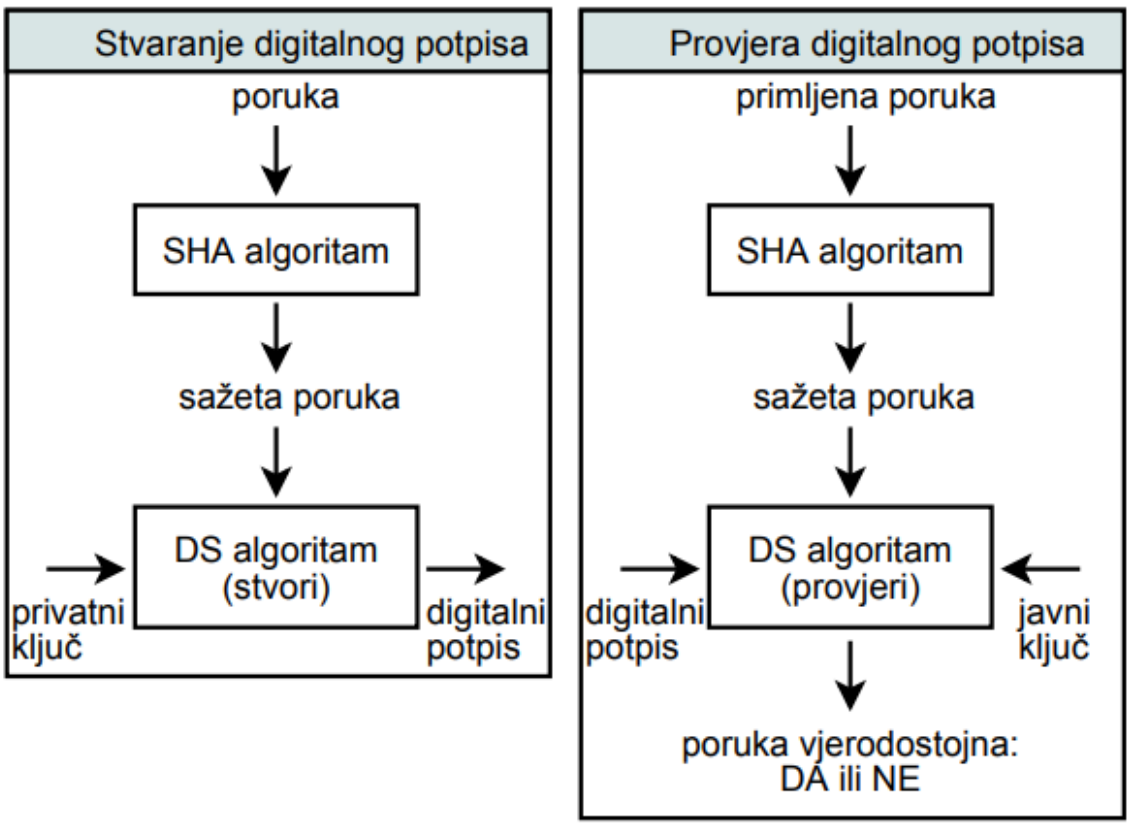
Slika 4: Prikaz korištenja asimetričnog algoritma (izvor: Dujella A.; Maretić. M. Kriptografija)

Autentičnost poruke koju je poslala osoba A može se provjeriti na sljedeći način: osoba A poruci doda neki slučajan broj a, a osoba B generira svoj slučajan broj b te osobi A šalje poruku $e_A(\mathrm{a}+\mathrm{b})$. Osoba A može izračunati b pomoću formule $\mathrm{b} = d_A(e_A(\mathrm{a} + \mathrm{b})) - \mathrm{a}$ te ponovno šalje prvu poruku kojoj je dodan b.

Asimetrični algoritmi se koriste za stvaranje digitalnih potpisa. Digitalni potpis se stvara pomoću privatnog ključa, dok se za njegovu provjeru koristi javni ključ koji nije jednak privatnom ključu. Oba ključa pripadaju jednom korisniku, te se na taj način identificira potpisnik poslane poruke. Privatni ključ je dostupan samo vlasniku digitalnog potpisa

čime se onemogućuje krivotvorenje, a javni ključ je dostupan svima.

Enkripcija sa javnim ključem ima više dobrih strana, no proces je vrlo zahtjevan jer uključuje veliku količinu računanja, što ga čini sporim. No, taj problem je riješen šifriranjem samo sažete inačice poruke, umjesto šifriranja cijelog sadržaja. Naime, za digitalni potpis nije potrebno šifrirati cijeli sadržaj. Sigurna jednosmjerna funkcija – SHA algoritam (engl. *Secure Hash Algorithm*) se koristi pri izradi digitalnog potpisa. Jednosmjerne funkcije se koriste za jednosmjerno šifriranje te se iz jednom šifriranog podatka se ne može dobiti originalni sadržaj. Pomoću sigurne jednosmjerne funkcije se stvara sažeta inačica poruke. Iz te sažete poruke korištenjem nekog algoritma stvara se digitalni potpis. Ta sažeta poruka se onda šalje primatelju koji pomoću javnog ključa utvrđuje vjerodostojnost poruke.



Slika 5: Stvaranje i provjeravanje digitalnog potpisa putem SHA algoritma (https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf)

Prednosti šifriranja sažete poruke su sljedeći – potpis će biti puno kraći, a cjelokupni postupak brži, u slučaju javnih dokumenata koji moraju biti dostupni oni se spremaju

bez enkripcije, a priloženi digitalni potpis garantira vjerodostojnost dokumenta. Asimetrični algoritmi se smatraju sigurnijim od simetričnih algoritama te omogućuju bolju tajnost podataka. Ostale prednosti su sljedeće: nema potrebe za sigurnim komunikacijskim kanalom za razmjenu ključeva s obzirom da je ključ javan, no mora se osigurati autentičnost javnog ključa, par javnog i privatnog ključa se može koristiti dulje vrijeme, može se koristiti za potpisivanje poruke.

3.2.1. RSA algoritam

RSA (Rivest, Shamir, Adleman) algoritam je nastao 1977. godine od strane autora Ronalda Rivesta, Adi Shamira i Leonarda Adlemana koji su htjeli potražiti jednosmjernu funkciju o kojoj su pisali Diffie i Hellman. Zasniva se na dva ključa, javnom i tajnom, koji mogu biti dužine od 40 i 2048 bita. Algoritam se primjenjuje u protokolima za sigurnu komunikaciju putem Interneta kao što su SSL, HTTPS i sl.

Rivest je za asimetrični algoritam stvorio jednosmjernu funkciju koja može poslužiti za enkriptiranje poruke te se ta poruka, koja je zapravo broj, stavlja u funkciju te se dobiva šifrirani tekst, odnosno drugi broj. Poseban dio funkcije, nazvan samo N, omogućuje da jednosmjerna funkcija postane reverzibilna pod određenim uvjetima. N je fleksibilan dio funkcije te svatko može izabrati osobnu vrijednost N tako da pomnoži dva prim-broja, p i q. Tako izabran N postaje javni ključ koji može biti objavljen i vidljiv svima, dok prim-brojevi p i q tvore privatni ključ. Da bi osoba poslala poruku drugoj osobi, koristi njezin javni ključ, odnosno N. Druga osoba pomoću prethodno odabranih prim-brojeva može dešifrirati poruku. Da bi se osigurala sigurnost privatnog ključa, osoba može izabrati vrlo velike brojeve p i q, koje će računalo brzo pomnožiti kako bi se dobio N, no osoba koja pokušava otkriti p i q iz javnog ključa N neće moći lako otkriti te informacije.

Prednost RSA algoritma je rješavanje problema razmjene ključa. S obzirom da je N javni ključ, nema potrebe za sigurnim slanjem ključa drugoj osobi.

Napad primjenom sile (engl. *brute force attack*) je napad gdje osoba želi doći do privatnog ključa uz pomoć javnog ključa. Postoji nekoliko algoritama za faktorizaciju koji predstavljaju najbolje mogućnosti za napad na RSA algoritam, a to su dijeljenje,

kvadratni Sieve algoritam, više polinomski kvadratni Sieve algoritam, Sieve algoritam sa općim brojčanim poljima te Sieve algoritam sa specifičnim brojčanim poljima. S razvojem računalne moći i snižavanjem cijena računala, postoji veća mogućnost da se probije RSA algoritam, no korištenje velikih brojeva za generiranje sigurnog ključa smanjuje tu mogućnost.

Kako bi izveo napad korištenjem odabranog šifriranog teksta (engl. *chosen chipertext attack*), napadač mora imati mogućnost da mu potpisnik koji zna privatni ključ dešifrira bilo koji šifrirani tekst te mu pošalje rezultat. Analiziranjem izabranog šifriranog teksta te zaprimljenog teksta napadač može pogoditi privatni ključ. Za ovakav napad mora postojati interakcija između napadača i potpisnika. Obrana od ovoga napada temelji se na tome da se nikada ne potpisuje dokument koji se šalje, već samo vrijednost jednosmjerne funkcije izračunate nad tim dokumentom.

Vremenski bazirani napad (engl. *timing attack*) je napad u kojem napadač pokušava kompromitirati sustav analiziranjem vremena potrebnog da se izvrši kriptografski algoritam. Napad iskorištava vremensku varijaciju u operaciji. Najjednostavnija obrana od ovoga napada je osigurati da operacija traje ujednačeno, bez obzira na podatke. Drugi način obrane je maskiranje podataka prije obrade te se maska nakon kriptiranja uklanja.

3.2.2. DSA (Digital Signature Algorithm)

DSA algoritam je patentiran 1991. godine te je propisan DSS (engl. Digital Signature Standard) standardom u Sjedinjenim Američkim državama. Algoritam se sastoji od tri koraka:

1. Stvaranje ključeva – odabir 160-bitnog prostog broja q, odabir prostog broja p veličine oko 1024 bitova takav da je $p = qz + 1$ za neki $z \in N$. Odabir h tako da vrijedi $1 < h < p - 1, g = h^z \, mod \; p > 1$. Izabere se slučajni $x < q$ te izračuna $y = g^x mod \, p$. Javni ključ je (p, q, g, y), a tajni x.
2. Potpisivanje poruke – generira se slučajni $k, 0 < k < q$, računa se $r = (g^k mod \, q)$ te $s = (k^{-1}(SHA - 1(m) + xr)) \, mod \, q$. Ako je $r = 0$ ili $s = 0$ onda se računa novi potpis. Ako nije, onda je potpis (r, s).
3. Provjera potpisa - ako ne vrijedi $(0 < r < q)$ ili $(0 < s < q)$, potpis nije valjan.

Izračunava se $w = s^{-1} mod\ q, u_1 = (SHA-1(m) * w) mod\ q, u_2 = (rw)\ mod\ q,$ $v = ((g^{u1} y^{u2}) mod\ p)\ mod\ q$. Ako je $v = r$ onda je potpis valjan.

U usporedbi sa RSA algoritmom, DSA je sporiji u šifriranju i verifikaciji, ali je brži u generiranju ključeva i dešifriranju.

4. Izdavanje i vrste certifikata

Korištenje digitalnog potpisa zahtjeva i korištenje certifikata. Pomoću certifikata vrši se provjera javnog ključa koji povezuje identitet osobe sa podacima. Prema Ministarstvu gospodarstva, certifikat označava potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa (javni ključ) s nekom osobom i potvrđuje identitet te osobe. Certifikat sadrži informacije o vlasniku, vijeku trajanja certifikata, izdavatelju, potpis izdavatelja te javni ključ. Jedini ovlašteni izdavatelj certifikata (CA – *certificate authority*) u Republici Hrvatskoj je Financijska Agencija (FINA) koja izdaje certifikate pravnim subjektima, fizičkim osobama te tijelima državne uprave. Certifikacijska služba koristi korijenski CA (*Root CA*) kao najviši entitet dok svi hijerarhijski niži entiteti vjeruju korijenskom CA. (Brzica, Katulić, Stančić, 2014.). Osim izdavanja certifikata, CA objavljuje informacije o nevažećim, tj. opozvanim certifikatima te održava javni imenik izdanih certifikata. Certifikati izdani od strane FINE su usklađeni s normom X.509 v3, koji je međunarodno priznati standard. Također, u pružanju usluge certificiranja primjenjuju se odredbe Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, odredbe Zakona o provedbi Uredbe (EU) 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Finini dokumenti: Opća pravila pružanja usluga certificiranja, Pravilnik o postupcima certificiranja za FINA Root CA, Opća pravila pružanja usluga certificiranja za kvalificirane Certifikate za elektroničke potpise i pečate, Pravilnik o postupcima certificiranja za kvalificirane Certifikate za elektroničke potpise i pečate, Opća pravila pružanja usluga certificiranja za nekvalificirane Certifikate te Pravilnik o postupcima certificiranja za nekvalificirane Certifikate.

Kvalificirani certifikat (engl. *qualified certificate*) je certifikat koji zadovoljava kriterije navedene u Direktivi 1999/000/EC, a to su:

- Dokaz da je certifikat izdan kao kvalificirani certifikat,
- identifikaciju izdavatelja certifikata te državu u kojoj je izdan,
- podatak o nazivu potpisnika certifikata,
- podatak o specifičnom atributu korisnika koji može biti uključen ako je

relevantan, što ovisi o svrsi certifikata,

- podaci za provjeru potpisa koji odgovaraju podacima o potpisivanju,
- početak i kraj valjanosti certifikata,
- identifikacijski kod certifikata,
- napredni elektronički potpis izdavatelja certifikata,
- ograničenja korištenja certifikata, ako postoje,
- limit vrijednosti transakcija za koje se certifikat može koristiti, ako postoje.

Osim navedenih kriterija, kvalificirani certifikat mora biti izdan od strane izdavatelja certifikata koji zadovoljava skup kriterija također navedenih u Direktivi 1999/000/EC.

Postoji više vrsta certifikata koji se izdaju u svrhe digitalnih potpisa, autentikacije i kriptiranja podataka. Certifikat za udaljeni e-Potpis izdaje se za fizičke osobe, poslovne subjekte te TDU. Certifikati na sigurnom kripto uređaju ili na QSCD kripto uređaju izdaju se za također za fizičke osobe, pravne subjekte te TDU dok se Soft certifikat izdaje za fizičke osobe i poslovne subjekte. Za testiranje i demonstraciju koriste se demo certifikati koji su jednaki produkcijskim certifikatima.

4.1. Certifikat za udaljeni e-Potpis (ePotpis u oblaku)

Certifikat za udaljeni e-Potpis je kvalificirani certifikat za koji korisnik ne mora posjedovati kripto uređaj kao što su USB, kartica ili drugi hardverski uređaji u kojemu se nalazi privatni ključ, već ključ aktivira koristeći mobilni uređaj ili tablet. ePotpis u oblaku je neovisan o platformi ili pregledniku, kao i o instalaciji Jave ili ostalih komponenti te ga korisnik može koristiti na bilo kojem željenom operativnom sustavu ili pregledniku. Certifikat ima srednju razinu sigurnosti, a pripadajući privatni ključ se čuva u Fininom servisu udaljenog elektroničkog potpisivanja i pečatiranja.

ePotpis u oblaku je namijenjen fizičkim osobama, poslovnim subjektima, zaposlenicima unutar poslovnog subjekta, djelatnicima u državnim uredima te IT tvrtkama. Usluga je sukladna pravnim regulativama i EU uredbama te je pravni učinak jednak kao i kod certifikata sa kripto uređajima. Certifikat se izdaje na rok od 5 godina nakon čega se mora produžiti kako bi se mogao dalje koristiti.

Za izdavanje certifikata, poslovni subjekt ili fizička osoba moraju ispuniti dokumentaciju te dobivaju aktivacijske podatke putem elektroničke pošte i SMS – a. Za korištenje certifikata neophodno je da su proslovni subjekt ili fizička osoba u PKI sustavu FINE (Sustav za izdavanje digitalnih certifikata).Nakon što je certifikat izdan, korisnik kreira zaporku koja je neophodna za korištenje certifikata. Certifikat se preuzima putem web stranice https://mojcert.fina.hr/finacms/. Portalu se pristupa upisom referentnog broja i autorizacijskog koda zaprimljenog putem elektroničke pošte i SMS – a. Primjer zahtjeva za izdavanje osobnog certifikata za fizičke osobe prikazan je na slici 4.

Fina

Fina RDC 2015 CA

Zahtjev za izdavanje osobnih certifikata za fizičke osobe - građane

1. Podaci o podnositelju zahtjeva

Ime*

Prezime*

OIB podnositelja zahtjeva*

Identifikacijska isprava ☐ Osobna iskaznica ili ☐ Putovnica Vrijedi do: . . .

Broj identifikacijske isprave*

Državljanstvo*

Adresa prebivališta i kontakt podaci

Ulica i broj*

Broj pošte* Mjesto*

Država*

Mobitel*

Adresa e-pošte*

2. Specifikacija traženog certifikata*
Znakom x označite koji tip certifikata tražite

☐ **Osobni certifikat na kriptografskom uređaju**

Odabir certifikata ☐ Kvalificirani certifikat za elektronički potpis ☐ Certifikat za autentikaciju

Odabir kriptografskog uređaja ☐ Siguran kriptografski uređaj ☐ Kvalificirani (QSCD) kriptografski uređaj
(Kvalificirani (QSCD) kriptografski uređaj nužan je za izradu kvalificiranog elektroničkog potpisa).

Preuzimanje Fina e-kartice/USB tokena s certifikatima ☒ U podružnici Fine

Način dostave PIN-a ☒ Na adresu e-pošte

☐ **Osobni soft certifikat** - certifikat za autentikaciju i elektronički potpis, izdaje se u obliku datoteke.

Preuzimanje aktivacijskih podataka ☐ Dostava SMS-om i e-poštom ☐ U poslovnim jedinicama Fine

☐ **Osobni kvalificirani certifikat za ePotpis u oblaku - certifikat za udaljeno potpisivanje**

Preuzimanje aktivacijskih podataka ☒ Dostava SMS-om i e-poštom

3. Zaporka za opoziv i suspenziju certifikata

Podnositelj zahtjeva samostalno definira zaporku koja služi za identifikaciju u slučaju hitnog opoziva i suspenzije certifikata te se ista primjenjuje za sve osobne certifikate izdane podnositelju zahtjeva. Zaporka može sadržavati hrvatska i engleska slova te brojeve, a može biti dugačka minimalno osam i maksimalno petnaest znakova. Zaporka ne smije sadržavati specijalne te dijakritičke znakove.

Zaporka za opoziv i suspenziju certifikata*

4. Izjava podnositelja zahtjeva

Izjavljujem da su svi podaci navedeni u ovom Zahtjevu točni i cjeloviti te da su dobrovoljno stavljeni na raspolaganje Fini koja će ih koristiti u cilju obavljanja ovdje zahtijevane usluge. Potpisom Zahtjeva potvrđujem da sam upoznat s informacijama ispitaniku o obradi osobnih podataka prikupljenih ovim Zahtjevom koje su dane na sljedećoj stranici ovog Zahtjeva i s Fininim Uvjetima pružanja usluga certificiranja za osobne certifikate te pristajem na njihovu primjenu. Suglasan sam s javnim objavljivanjem izdanog certifikata iz točke 2. ovog Zahtjeva sukladno Fininim Uvjetima pružanja usluga certificiranja za osobne certifikate.

Podnositelj zahtjeva izjavljuje i jamči da samo on može pristupiti i pročitati poruku upućenu na adresu e-pošte iz točke 1. ovog Zahtjeva.

U slučaju odabira dostave aktivacijskih podataka SMS-om i e-poštom za osobni soft certifikat podnositelj zahtjeva izjavljuje i jamči da samo on može pristupiti i pročitati poruku upućenu SMS-om na mobitel i na adresu e-pošte iz točke 1. ovog Zahtjeva.

Podnositelj zahtjeva koji želi izdavanje certifikata za udaljeni e-potpis izjavljuje i jamči da je mobilni uređaj čijim se brojem autenticira na servis za udaljeni e-potpis njegovo vlasništvo i da samo on može pristupiti i pročitati poruku upućenu SMS-om na broj mobitela iz točke 1. Ovog Zahtjeva.

5. Potpis podnositelja zahtjeva

Potpis podnositelja zahtjeva

** Obvezno ispuniti sve podatke u označenom stavku ili polju zahtjeva.*
Ako se certifikati izdaju na FINA e-kartici, uz karticu se izdaje i čitač kartice. Naknada za čitač kartice naplaćuje se prema službenom cjeniku Fine.

POPUNJAVA DJELATNIK FINE

Datum zaprimanja | Potpis djelatnika koji je zaprimio zahtjev | Štambilj

Službenik za registraciju — Ime i prezime službenika — Potpis službenika

Službenik za registraciju — Ime i prezime službenika — Potpis službenika

Str: 1/2

Slika 6: Zahtjev za izdavanje osobnog certifikata za fizičke osobe/građane (izvor: https://www.fina.hr/osobni-soft-certifikat-finasoftcert)

4.2. Soft certifikat

Soft certifikat (u zaštićenoj datoteci) za fizičke osobe i osobe unutar poslovnog subjekta ima standardnu razinu sigurnosti te je namijenjen za elektronički potpis, autentikaciju i kriptiranje. Također, fizičke osobe mogu koristiti Soft certifikat za pristup e-uslugama unutar projekta e-Građani koje za prijavu zahtijevaju minimalnu razinu sigurnosti 3. Ovaj certifikat moguće je pohraniti na računalo ili mobilni uređaj te je zastupljen na svim platformama. Certifikat je usklađen sa međunarodnom normom X.509 v3 te normom HRN ETSI/EN 319 411-3.

Soft certifikat se izdaje nakon dostavljanja dokumentacije u FINU. Certifikat se izdaje na rok od 5 godina te se nakon isteka toga razdoblja mora obnoviti da bi se omogućilo daljnje korištenje. Nakon obrade dokumentacije, korisnik dobiva aktivacijske podatke putem elektroničke pošte te SMS – a ili u uredu FINE.

Certifikat se preuzima sa web adrese https://mojcert.fina.hr/finacms/ unošenjem zaprimljenih aktivacijskih podataka. Prilikom preuzimanja certifikata stvara se datoteka sa ekstenzijom .p12 u kojoj se nalaze certifikat i korisnikov privatni ključ.

4.3. Certifikati na uređaju

Poslovni certifikati na uređaju izdaju se za fizičke osobe unutar poslovnog subjekta, te se na uređaju mogu nalaziti dva certifikata – certifikat za autentikaciju i kvalificirani certifikat. Certifikat za autentikaciju se koristi za jaku autentikaciju i enkripciju, a kvalificirani certifikat se koristi za potpise. Navedeni certifikati mogu se koristiti za pristup Fininim e-servisima, servisima državnih službi i drugim e-servisima.

Postoje dvije vrste uređaja na kojima se izdaju certifikati – QSCD uređaj ili siguran kripto uređaj. QSCD (engl. *Qualified Electronic Signature Creation Device*) je korisnički kripto uređaj u obliku USB tokena ili kartice za izradu potpisa (QES – *Qualified Electronic Signature*) koji je jednako vrijedan kao vlastoručni potpis. QSCD uređaj se preporučuje umjesto dosad korištenog sigurnog kripto uređaja radi veće sigurnosti, priznavanja van države te izjednačenosti sa vlastoručnim potpisom unutar Europske

Unije. Siguran kripto uređaj je uređaj starije generacije, sadrži dva certifikata, kvalificirani certifikat za napredni elektronički potpis (AdESQC - *Advanced Electronic Signature with a Qualified Certificate*) i certifikat za autentikaciju. Zbog EU uredbe eIDAS (engl. *electronic Identification, Authentication and trust Services*) iz 2014. godine, certifikati na starijim generacijama sigurnih kipto uređaja se ne izdaju novim korisnicima.

5. Primjena digitalnog potpisa

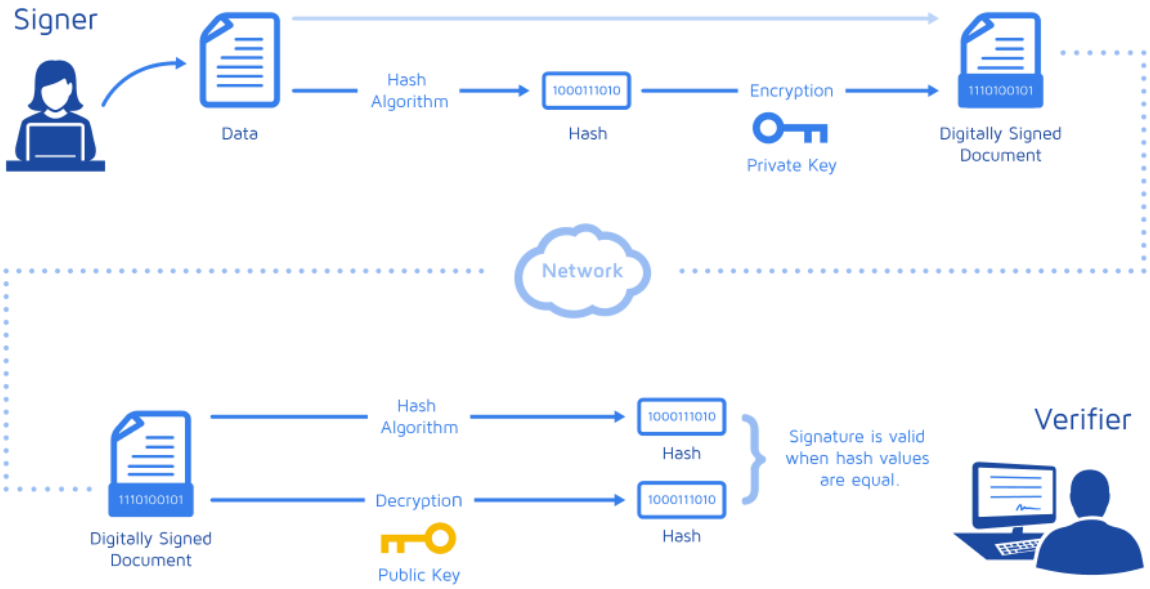
Elektronička komunikacija je brža, jeftinija te se sve više koristi u svakodnevnom životu. S obzirom da se sve više poslova obavlja online, digitalni potpis predstavlja bitan element koji omogućuje pouzdanost i sigurnost komunikacije. Potpis se može koristiti za autorizaciju elektronske pošte, dokumenata, ugovora i drugih dokumenata, za slijepi potpis, potpis u web aplikacijama te zaštitu multimedijskih sadržaja digitalnim potpisom.

5.1. Potpisivanje dokumenata

Prednost korištenja digitalnog potpisa u dokumentima je osiguravanje autentičnosti, integriteta te onemogućuje nepriznavanje dokumenta od strane potpisnika. Digitalni potpis je pravno obvezujući kao i vlastoručni potpis, te obvezuje potpisnika prema uvjetima u potpisanom dokumentu. Za dokumente koji se šalju nesigurnim komunikacijskim kanalom, digitalni potpis daje potvrdu da je dokument poslan upravo onaj za kojega se tvrdi da je pošiljatelj te daje dokaz o izvornosti podataka. Također, digitalni potpis je teže krivotvoriti od vlastoručnog potpisa.

Kada korisnik potpisuje dokument, potpis je kreiran korištenjem korisnikovog privatnog ključa, koji je poznat samo njemu. Sažeta inačica poruke se kriptira korištenjem privatnog ključa, a vjerodostojnost potpisa utvrđuje se javnim ključem.

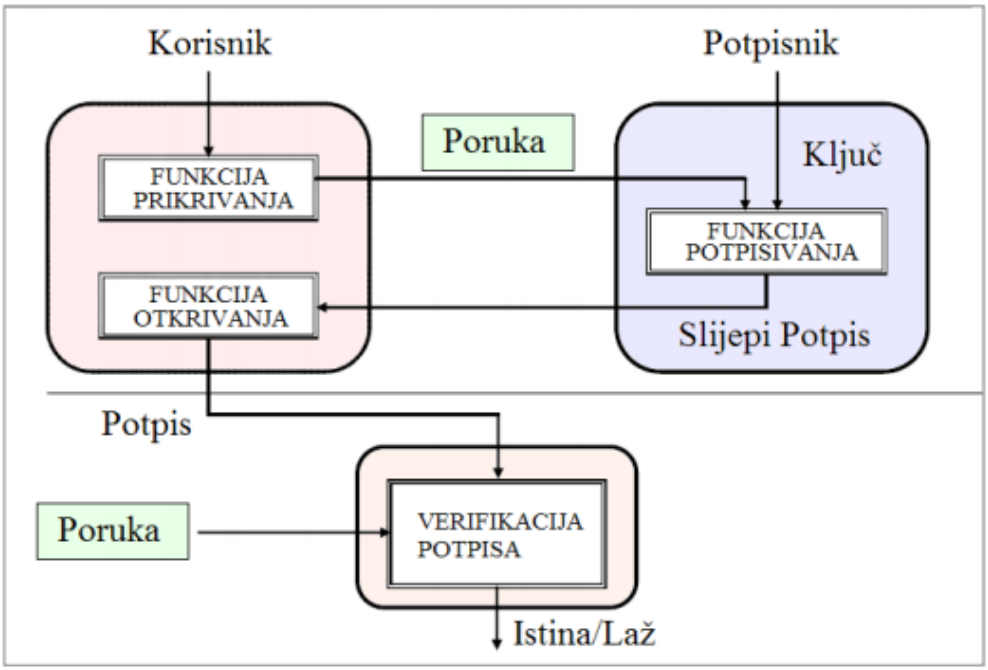
Na sljedećoj slici nalazi se primjer potpisivanja dokumenta. Potpisnik šalje dokument potpisan vlastitim digitalnim potpisom. Dokument je poslan primatelju koji također posjeduje javni ključ potpisnika. Pomoću javnog ključa, primatelj utvrđuje da li je digitalni potpis valjan. Ukoliko primatelj nije u mogućnosti dešifrirati digitalni potpis javnim ključem, to znači da potpis nije izrađen od strane potpisnika ili je mijenjan.



Slika 7: Primjer potpisivanja dokumenta digitalnim potpisom (izvor: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq)

5.2. Slijepi potpis

Ideja digitalnog potpisa podrazumijeva da je potpisnik upoznat sa sadržajem poruke ili dokumenta koji potpisuje. No, ponekad uvid u sadržaj nije poželjan. Iz toga razloga, stvoren je slijepi potpis (engl. *blind signature*) koji koristi tri funkcije: funkciju potpisivanja, prikrivanja i otkrivanja. Slijepo potpisivanje moguće je implementirati pomoću raznih algoritama sa javim ključem. Poruka se prije potpisivanja skriva, te se zatim potpisuje nekim od uobičajenih algoritama.



Slika 8: Protokol slijepog potpisa (izvor: Marijana Zelanto., Slijepi potpis)

Slijepi potpis, kao i digitalni potpis, ima svojstva autentičnosti, integriteta i neporecivosti. Potpisnik ne može povezati prikrivenu poruku koju je dobio na potpis sa konačno potpisanom porukom nastalom nakon funkcije otkrivanja. Slijepi potpis koristi se za anonimno elektroničko glasovanje, elektroničko plaćanje ili korištenje elektroničkog novca, odnosno, kad god je potrebno osigurati anonimnost korisnika.

5.3. Potpis u web aplikacijama

XML potpisi mogu biti primijenjeni na bilo koji digitalni sadržaj, uključujući XML. W3C XML Signature standard međunarodne standardizacijske organizacije World Wide Web Consortium je zadužen za reguliranje XML potpisa. Postoje tri vrste XML potpisa: omotani (engl. *enveloped*), gdje se potpis nalazi unutar istog dokumenta kao i podaci; omotavajući (engl. *enveloping*), gdje su podaci ugrađeni u XML potpis, te odvojeni (engl. *detached*), potpis je odvojen od podataka koji se potpisuju.

XML potpis moguće je koristiti za potpisivanje XML elemenata, skupove XML čvorova te njihov sadržaj, vanjske URI oznake, vanjske binarne datoteke te binarne podatke ugrađene u XML dokument.

5.4. Multimedijski sadržaji

Autentikacija multimedijskog sadržaja se obično temelji na dvije mogućnosti: digitalni potpis ili vodeni žig (engl. *watermark*). Vodeni žig sadrži informacije kao što su autor, godina nastanka te mogu biti skriveni ili vidljivi korisniku. Vidljivi vodeni žigovi služe za ograničavanje korištenja multimedijskog sadržaja, dok skriveni vodeni žigovi služe za utvrđivanje porijekla.

Postoje dvije vrste autentikacije multimedijskog sadržaja: potpuna autentikacija koja ne dopušta nikakve manipulacije ili transformacije, te autentičnost sadržaja, gdje se dopuštaju modifikacije kao što je sažimanje podataka no bez promjene samog sadržaja.

Za neobrađene i nesažete multimedijske sadržaje pogodnije je koristiti vodeni žig iz sljedećih razloga:

- Žig je izravno vezan za podatke i moguće ga je brzo i jednostavno provjeriti,
- Žig je moguće ugraditi bilo gdje unutar multimedijskog sadržaja bez da narušava kvalitetu (nevidljivi žig).

Standardi za kompresiju kao što su JPEG ili MPEG imaju unaprijed definiran prostor za smještanje digitalnog potpisa. Ako je sadržaj izmijenjen, to je moguće otkriti zbog nepodudaranja *hash* vrijednosti datoteke i potpisa. Potpis je također moguće spremiti u zaseban dokument koji se onda dobavlja uz multimedijski sadržaj ako je potrebna autentikacija.

Potpisivanje multimedijskih sadržaja je slično potpisivanju ostalih dokumenata, glavna razlika su informacije koje se koriste za stvaranje potpisa. Multimedijski sadržaj se potpisuje tako da se zaštite vizualne i zvučne informacije.

6. Zakoni

6.1. Zakoni u Hrvatskoj

Zakon o elektroničkom potpisu donesen je 24. siječnja 2002. godine. Prema Članku 1., ovim se Zakonom uređuje pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa, ako posebnim zakonom nije drukčije određeno.

Prema Članku 3., Elektronički potpis u smislu ovoga Zakona je skup podataka u elektroničkom obliku koji služe za identifikaciju potpisnika i potvrdu vjerodostojnosti potpisanoga elektroničkog zapisa.

Unutar Zakona definiraju se certifikat, kvalificirani certifikat te davatelji usluga certificiranja. Certifikat je, u smislu ovoga Zakona, svaka elektronička potvrda kojom se potvrđuje identitet potpisnika u postupcima razmjene elektroničkih zapisa. Prema Članku 10., da bi certifikat mogao biti kvalificirani, mora sadržavati kriterije navedene u Zakonu, a koji su istovjetni onima navedenima u Direktivi 1999/000/EC. Za izdavanje certifikata nadležno je Ministarstvo gospodarstva te za davatelje usluga certifikata ne postoji posebna dozvola. Početak obavljanja djelatnosti izdavanja certifikata obrazloženo u je člancima 15 i 16.

Članak 15: Davatelj usluge certificiranja mora prijaviti Ministarstvu početak obavljanja usluga certificiranja najmanje osam dana prije početka rada.
Uz prijavu iz stavka 1. ovoga članka ili u slučajevima promjena u obavljanju usluge, davatelj usluge certificiranja mora dostaviti Ministarstvu dokumentaciju o internim pravilima poslovanja u svezi s izradom i ovjerom elektroničkih potpisa te o unutarnjoj organizaciji, kao i dokumentaciju kojom dokazuje ispunjavanje uvjeta iz članka 12. ovoga Zakona.

Članak 16: Ministarstvo upisuje davatelje usluga certificiranja u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj (u daljnjem tekstu: evidencija), odmah nakon što davatelj usluge certificiranja podnese prijavu kojom obavještava Ministarstvo o početku obavljanja usluga.

Upis u evidenciju ne podliježe vođenju upravnog postupka.
Ministar gospodarstva propisat će pravilnikom sadržaj evidencije, način vođenja evidencije, kao i obrasce prijave za upis u evidenciju te prijave za upis promjena.

Ministarstvo Gospodarstva održava evidenciju o davateljima usluga certificiranja te Registar davatelja usluga izdavanja kvalificiranih certifikata u Republici Hrvatskoj u koji se upisuju davatelji usluga izdavanja kvalificiranih certifikata. Evidencije su javne te se vode u elektroničkom obliku.

Davatelj usluga certificiranja dužan je prekinuti uslugu certificiranja potpisnicima koji su to tražili, za koje je utvrđena netočnost podataka, koji su umrli ili izgubili poslovnu sposobnost te obavijestiti Ministarstvo gospodarstva o svakom opozivu. Davatelj usluga certificiranja dužan je osigurati sve tehničke i organizacijske mjere zaštite certifikata i podataka te upoznati potpisnika sa svim tehničkim zahtjevima potrebnim za usluge certificiranja.

Zakon o elektroničkom potpisu prestao je važiti danom stupanja na snagu Zakona o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.

Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ na snazi je od 08.07.2017. godine te se njime utvrđuju nadležna tijela i zadaće nadležnih tijeka za provedbu Uredbe, utvrđuju tijela za inspekcijski nadzor nad provedbom Uredbe, određuje tijelo nadležno za akreditaciju tijela za ocjenu sukladnosti, utvrđuju prava, obveze i odgovornosti potpisnika i pružatelja usluga povjerenje te određuju prekršajne odredbe za postupanje protivno Uredbi.

Nadležno tijelo za provedbu Uredbe je središnje tijelo državne uprave nadležno za poslove e-Hrvatske. Tijelo nadležno za akreditaciju Tijela za ocjenjivanje sukladnosti kvalificiranih pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža je nacionalno akreditacijsko tijelo.

Inspekcijski nadzor nad provedbom Uredbe provode državni službenici središnjeg tijela državne uprave nadležnog za poslove e-Hrvatske ovlašteni za provedbu nadzora.

Prava, obveze i odgovornosti potpisnika te pružatelja usluga povjerenja se usklađuju s onima navedenim u Uredbi.

Novčane kazne određuju se za fizičke osobe i pravne osobe. Prema članku 18, (1) Novčanom kaznom od 2000,00 do 10.000,00 kuna kaznit će se za prekršaj fizička osoba koja:
– neovlašteno pristupi i uporabi podatke i sredstva za izradu elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata.
(2) Novčanom kaznom od 2000,00 do 10.000,00 kuna kaznit će se za prekršaj potpisnik, odnosno fizička osoba ili odgovorna osoba pravne osobe koja zastupa potpisnika, a koja:
1. ne koristi sredstva i podatke za izradu elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata s pažnjom dobrog domaćina (članak 9. ovoga Zakona)
2. davatelju usluga certificiranja u roku od sedam dana od nastalih promjena ne dostavi potrebne podatke i informacije o promjenama koje utječu ili mogu utjecati na točnost elektroničkog potpisa, naprednog elektroničkog potpisa, kvalificiranoga potpisa, elektroničkog pečata, naprednog elektroničkog pečata, kvalificiranog elektroničkog pečata (članak 10. ovoga Zakona)
3. davatelju usluga certificiranja pravodobno ne dostavi zahtjev za opoziv certifikata, odnosno ako odmah po saznanju ne zatraži opoziv svog certifikata u slučajevima gubitka ili oštećenja sredstava/podataka za izradu svog elektroničkog potpisa (članak 10. ovoga Zakona).

Prema Članku 19, novčanom kaznom od 5000,00 do 100.000,00 kuna kaznit će se za prekršaj kvalificirani pružatelj usluga povjerenja koji:
1. ne utvrdi pravovaljano identitet fizičke ili pravne osobe za koju izdaje kvalificirani certifikat,

2. ne obavijesti nadzorno tijelo o svim promjenama u vezi s pružanjem svojih kvalificiranih usluga povjerenja te o namjeri prestanka obavljanja te djelatnosti najmanje 3 (tri) mjeseca prije isteka ugovorom povjerenih mu usluga povjerenja,
3. ne zapošljava osoblje i/ili podizvođače koji posjeduju potrebna stručna znanja, pouzdanost, iskustvo i kvalifikacije i koji su prošli odgovarajuće osposobljavanje u vezi sa sigurnošću i propisima o zaštiti osobnih podataka te ne primjenjuju upravne i upravljačke postupke u skladu s europskim ili međunarodnim normama,
4. ne raspolaže dostatnim financijskim sredstvima i/ili nije sklopio odgovarajuće osiguranje od odgovornosti za štetu,
5. ne obavijesti prije stupanja u ugovorni odnos, na jasan i sveobuhvatan način, svaku osobu koja želi koristiti kvalificiranu uslugu povjerenja o točnim uvjetima korištenja tom uslugom, uključujući bilo kakva ograničenja korištenja,
6. ne koristi vjerodostojne sustave i proizvode koji su zaštićeni od preinaka te osiguravaju tehničku sigurnost i pouzdanost postupaka koje ti sustavi i proizvodi podržavaju,
7. ne koristi vjerodostojne sustave za pohranu podataka koji su mu dostavljeni, u obliku koji se može provjeriti,
8. ne poduzima odgovarajuće mjere protiv krivotvorenja i krađe podataka,
9. ne bilježi i ne čini dostupnim tijekom odgovarajućeg razdoblja, uključujući razdoblje nakon prestanka obavljanja djelatnosti kvalificiranog pružatelja usluga povjerenja, sve bitne informacije u vezi s podacima koje izdaje i prima kvalificirani pružatelj usluga povjerenja, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge,
10. nema uspostavljen i ažuriran plan prekida pružanja usluge radi osiguravanja njezina kontinuiteta u skladu s odredbama koje je potvrdilo nadzorno tijelo,
11. ne osigurava zakonitu obradu osobnih podataka,
12. ne uspostavi i ne ažurira bazu podataka certifikata, kada se radi o kvalificiranim pružateljima usluga povjerenja koji izdaju kvalificirane certifikate.

6.2. Zakoni u Europskoj Uniji

Uredba (EU) br. 910/2014 Europskoj parlamenta i vijeća izdana 23. srpnja 2014. godine o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.

Ovom Uredbom nastoji se povećati povjerenje u elektroničke transakcije pružanjem temelja za sigurnu elektroničku interakciju građana, poduzeća i tijela javne vlasti. Direktivom 1999/93/EZ uređeni su samo elektronički potpisi, no ne i prekogranični i međusektorski okvir za sigurne i vjerodostojne elektroničke transakcije. Cilj ove Uredbe je osigurati da pri pristupu prekograničnim *online* uslugama koje nude države članice postoji mogućnost sigurne elektroničke identifikacije i autentikacije te nema cilj zadirati u elektroničke sustave upravljanja identitetom u državama članicama. Države članice trebale bi odrediti nadzorno tijelo za provedbu aktivnosti prema ovoj Uredbi te bi nadzorna tijela trebala surađivati sa tijelima za zaštitu podataka.

Prema Članku 1, ovom se Uredbom:
(a) utvrđuju uvjeti pod kojima države članice priznaju sredstva elektroničke identifikacije fizičkih i pravnih osoba koja su obuhvaćena prijavljenim sustavom elektroničke identifikacije druge države članice;
(b) utvrđuju pravila za usluge povjerenja, posebno za elektroničke transakcije; i
(c) uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.

Odjeljak 4 Uredbe odnosi se na elektroničke potpise. Kvalificirani elektronički potpis ima jednak pravni učinak kao i vlastoručni potpis te se priznaje kao kvalificirani elektronički potpis u članicama Europske unije ako je izdan u jednoj državi članici.

Članak 26 utvrđuje zahtjeve naprednog elektroničkog potpisa:
(a) na nedvojben način je povezan s potpisnikom;
(b) omogućava identificiranje potpisnika;
(c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja,
koristiti pod svojom isključivom kontrolom; i
(d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.

Kvalificirani certifikati za elektroničke potpise moraju ispunjavati zahtjeve navedene u

Uredbi. Mogu uključivati dodatna obilježja koja nisu obavezna te ne utječu na priznavanje kvalificiranih elektroničkih potpisa. Kvalificirana sredstva za izradu elektroničkih potpisa moraju ispunjavati zahtjeve navedene u Uredbi. Države članice moraju obavijestiti Komisiju o informacijama o sredstvima za izradu kvalificiranog elektroničkog potpisa te o poništenju sredstava kako bi na temelju prikupljenih informacija Komisija vodila popis certificiranih kvalificiranih sredstava za izradu elektroničkog potpisa.

Prema Članku 32, postupkom validacije kvalificiranog elektroničkog potpisa potvrđuje se valjanost kvalificiranog elektroničkog potpisa pod sljedećim uvjetima:
a) certifikat koji podržava potpis je u trenutku potpisivanja bio kvalificirani certifikat za elektronički potpis koji je u skladu Prilogom I.;
(b) kvalificirani certifikat izdao je kvalificirani pružatelj usluga povjerenja i bio je valjan u trenutku potpisivanja;
(c) podaci za validaciju potpisa odgovaraju podacima koji se pružaju pouzdajućoj strani;
(d) jedinstveni skup podataka koji predstavlja potpisnika u certifikatu ispravno je dostavljen pouzdajućoj strani;
(e) korištenje pseudonimom, ako je pseudonim bio korišten u trenutku potpisivanja, jasno je naznačeno pouzdajućoj strani;
(f) elektronički potpis izrađen je sredstvom za izradu kvalificiranog elektroničkog potpisa;
(g) nije ugrožena cjelovitost potpisanih podataka;
(h) zahtjevi predviđeni u članku 26. bili su ispunjeni u trenutku potpisivanja.

7. Zaključak

Počeci kriptografije sežu još u doba starih Grka te do 19. stoljeća kriptografija je bila znanost koju su razumjeli samo vladini zaposlenici te vojska koja je najviše ovisila o sigurnosti poruka koje su se prenosile. Tek 60 – ih godina 20. stoljeća, sa napretkom i smanjenjem cijena računala, kriptografija se sve više počela koristiti u komercijalne svrhe za prijenos osjetljivih podataka. Daljnji razvoj simetričnih i asimetričnih ključeva, izum DSA, RSA te razvoj Interneta, omogućio je korištenje digitalnih potpisa u svakodnevnom životu.

Digitalni potpisi se danas koriste svakodnevno, od razmjene email poruka do bankovnih transakcija. Glavni faktor koji potiče rast korištenja digitalnih potpisa je razvoj online poslovanja, koje bi do 2020. godine trebalo nadmašiti 4 trilijuna USD (https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369). To dovodi i do smanjenja korištenja papira i slanje dokumenata poštom, što značajno smanjuje troškove poslovanja. Digitalni potpisi omogućuju brže i jeftinije poslovanje što će značajno pridonijeti njegovom korištenju u budućnosti. Sa sve većom zastupljenošću digitalnih potpisa, rastu i pokušaji napada te zlouporabe. Stoga je važno dalje razvijati sigurnosne mehanizme koji će omogućiti još veću sigurnost digitalnog potpisa.

Možemo očekivati u budućnosti da će digitalni potpis biti glavna metoda potpisivanja, dok će vlastoručni potpis ostati u primjeni u određenim slučajevima.

Literatura

Knjige:

1. Anić, V. i dr. (2004) *Hrvatski enciklopedijski rječnik*, Zagreb: EPH d.o.o. i Novi Liber d.o.o.
2. Dujella A.; Maretić. M. (2007) *Kriptografija*, Zagreb: Udžbenici Sveučilišta u Zagrebu
3. Radovan M. (2011) *Računalne mreže 2*, Rijeka: Digital point tiskara
4. Singh S. (2003) *Šifre: kratka povijest kriptografije*, Zagreb: Mozaik knjiga

Članci:

1. Zovkić, M.; Vrbanec, T. (2010) *Digitalni potpis*, Hrvatska udruga za mikroprocesorske, procesne i informacijske sustave, mikroelektroniku i elektroniku - MIPRO, 2010, 349-353
2. Brzica, H.; Katulić, T.; Stančić, H. (2014) *Analiza utjecaja hrvatskoga zakonodavnog okvira na elektroničko poslovanje i dugoročno očuvanje elektronički potpisanih dokumenata*, Arh. vjesn. 57(2014), str. 129-157

Mrežni izvori:

1. CARNet. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf (pristupljeno 30.prosinca 2018.)
2. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. (2001) *Handbook of Applied Cryptography*. URL http://cacr.uwaterloo.ca/hac/ (pristupljeno 02.siječnja 2019.)
3. Direktiva 1999/000/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51999AG0028&qid=1552667613433&from=EN (pristupljeno 15.ožujka 2019.)
4. Ministarstvo gospodarstva, poduzetništva i obrta. URL: https://www.mingo.hr/page/kategorija/e-potpis (pristupljeno 17. ožujka 2019.)
5. Zelanto, M. (2008) *Slijepi potpis*. URL: https://bib.irb.hr/datoteka/407742.Smaugos2protokoli2008_zelantoSlijepi_potpis.pdf (pristupljeno 19. ožujka 2019.)
6. FINA (2005): *Uvjeti pružanja usluga certificiranja za osobne certifikate*.

Zagreb: Narodne novine d.d. URL: https://rdc.fina.hr/pds/PDSo-hr.pdf (pristupljeno 21. ožujka 2019.)

7. Ching-Yung Lin (2000): *Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection*. URL: http://www.ee.columbia.edu/ln/dvmm/publications/PhD_theses/cylin-thesis.pdf (pristupljeno 30. ožujka 2019.)
8. Narodne Novine (2002) *Zakon o elektroničkom potpisu*. Zagreb: Narodne Novine d.d. URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html (pristupljeno 08. travnja 2019.)
9. UREDBA (EU) br. 910/2014 EUROPSKOG PARLAMENTA I VIJEĆA od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014R0910&from=EN (pristupljeno 08. travnja 2019.)
10. Narodne Novine (2017) *Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ*. Zagreb. Narodne Novine d.d. URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2017_06_62_1430.html (pristupljeno 08. travnja 2019.)
11. Contractworks.com, URL: https://www.contractworks.com/blog/the-future-of-electronic-signatures-is-handwritten-identification-dead (pristupljeno 10. lipnja 2019.)
12. eMarketer.com, URL: https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369 (pristupljeno 10. lipnja 2019.)

Popis slika

Slika 1: Primjer klasične kriptografije (Dujella A.; Maretić. M. Kriptografija)..... 4

Slika 2: Permutacija e (izvor: http://cacr.uwaterloo.ca/hac/) 6

Slika 3: Kriptiranje poruke m ključem e (Menezes et. al 2001, 2019-01-02, url)..... 6

Slika 4: Prikaz korištenja asimetričnog algoritma (izvor: Dujella A.; Maretić. M. Kriptografija) 7

Slika 5: Stvaranje i provjeravanje digitalnog potpisa putem SHA algoritma (https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf) 8

Slika 6: Zahtjev za izdavanje osobnog certifikata za fizičke osobe/građane (izvor: https://www.fina.hr/osobni-soft-certifikat-finasoftcert) 15

Slika 7: Primjer potpisivanja dokumenta digitalnim potpisom (izvor: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq) 18

Slika 8: Protokol slijepog potpisa (izvor: Marijana Zelanto., Slijepi potpis) 19

Sažetak

Digitalni potpis predstavlja tehnologiju koja omogućuje brzo i jednostavno poslovanje. Predstavlja zamjenu za tradicionalni vlastoručni potpis, zakonski jednako vrijedi te se njime utvrđuje autentičnost dokumenta. Najčešći algoritmi za implementaciju digitalnih potpisa su RSA, DSA i ECDSA. U usporedbi sa RSA algoritmom, DSA je sporiji u šifriranju i verifikaciji, ali je brži u generiranju ključeva i dešifriranju. Korištenje digitalnog potpisa zahtjeva i korištenje certifikata. Certifikat sadrži informacije o vlasniku, vijeku trajanja certifikata, izdavatelju, potpis izdavatelja te javni ključ. Digitalni potpis se primjenjuje za potpisivanje dokumenata, slijepo potpisivanje, u web aplikacijama te potpisivanje multimedijalnih sadržaja. Regulacija digitalnih potpisa određena je zakonima u Europskoj Uniji te državnim zakonima. Očekuje se da će u budućnosti korištenje digitalnih potpisa samo rasti te će postati glavna metoda potpisivanja.

Ključne riječi:

Digitalni potpis, certifikat, asimetrični algoritmi, simetrični algoritmi, kriptografija

Summary

A digital signature is a technology that makes business fast and easy. It represents a replacement for traditional signature, it is legally binding as traditional and it is used to determine the authenticity of the document. The most common algorithms used for digital signatures are RSA, DSA, and ECDSA. Comparing to the RSA algorithm, DSA is slower in encrypting and verification, but it is faster in generating keys and decrypting. In order to use a digital signature, the certificate is needed. It contains information about the owner, validity period, issuer, signature, and public key. A digital signature is used for signing the documents, blind signature, in web applications and multimedia. The regulation of digital signatures is defined in the European Union laws and state laws. It is expected that the use of digital signatures will grow in the future and will become the main method of signing documents.

Keywords:

Digital signature, certificate, asymmetric algorithms, symmetric algorithms, cryptography