Digitalni potpis i CA certifikati

Tucaković, Nives

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

NIVES TUCAKOVIĆ

DIGITALNI POTPIS I CA CERTIFIKATI

Završni rad

Pula, prosinac 2020. godine

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

NIVES TUCAKOVIĆ

DIGITALNI POTPIS I CA CERTIFIKATI

Završni rad

JMBAG: 0303046068, redoviti student

Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i tehnologija

Mentor: prof. dr. sc. Mario Radovan

Pula, prosinac 2020. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____Nives Tucaković_____, kandidat za prvostupnika informatike, smjera
____Informatika_____ime 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

Nives Tucaković

U Puli, prosinac 2020. godine

IZJAVA

o korištenju autorskog djela

Ja, _____Nives Tucaković_____dajem odobrenje Sveučilištu Jurja Dobrile

u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom ___Digitalni potpis i Ca certifikati_____ 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, prosinac 2020.

Potpis

Nives Tucaković

_____

SAŽETAK

Tema ovog završnog rada je Digitalni potpis i Ca certifikati. U daljnjem radu opisat ću što je to digitalni potpis, šifriranje sa simetričnim ključem te javnim i privatnim i hash algoritam. Tri algoritma digitalnog potpisa: DES (najpoznatiji algoritam šifriranja sa privatnim ključem), RSA (algoritam šifriranja sa javnim ključem) i MD5 (najrasprostiraniji kriptografski algoritam kontrolni zapis).

U daljnjem tekstu pišem i o digitalnim certifikatima koje koristimo kod zahtjevnijih implementacija enkripcije (šifriranja) s javnim ključem. Među certifikatima navela sam i Fina i Zaba certifikate.

Korištenje digitalnog potpisa već nam je u punom jeku i po mome vlastitom mišljenju najzanimljiviji tipovi digitalnog potpisa: pametne kartice, usb stickovi, biometrijski otisci prstiju te uređaj za digitalni potpis.

Uz sve prednosti digitalnog potpisa uvijek postoje i potencijalni napadi na digitalni potpis koje sam detaljnije objasnila u nastavku.

Ključne riječi: Digitalni potpis, Ca certifikati, šifriranje sa simetričnim, javnim i privatnim ključem, Hash algoritam, DES, RSA, MD5, pametna kartica, usb stickovi, biometrijski otisci prstiju, uređaj za digitalni potpis.

ABSTRACT

The title of this final paper is Digital Signature and Ca Certificates. In the following work I will describe what a Digital signature is, encryption with a symmetric key, and public and private and hash algorithms. Three digital signature algorithms: DES (the best known private key encryption algorithm), RSA (public key encryption algorithm) and MD5 (the most common cryptographic control record algorithm).

In the following text, I also write about digital certificates that we use in more demanding implementations of encryption with a public key. Among the certificates, I listed the Fina and Zaba certificates.

The use of Digital signatures is already in full swing and in my opinion the most interesting types of digital signatures: smart cards, usb sticks, biometric fingerprints and a digital signature device.

In addition to all the benefits of a Digital signature, there are always potential attacks on a digital signature, which I have explained in more detail below.

Keywords: Digital signature, Ca certificates, symmetric, public and private key encryption, Hash algorithm, DES, RSA, MD5, smart card, usb sticks, biometric fingerprints, digital signature device.

SADRŽAJ

UVOD

U ovome završnom radu obrađivat ću temu Digitalni potpis i CA certifikati (eng. Digital signature and CA certificate).

Naime, uza svu silnu tehnologiju i napredak znanosti, digitalni potpis i CA certifikati olakšali su nam svakodnevni život i rad.

Digitalni potpis utvrđuje nam autentičnost elektroničkog dokumenta. Naravno, dokument nam je autentičan ukoliko nam je poznat njegov autor i nije neovlašteno izmijenjen. Kako bismo provjerili vjerodostojnost dokumenta koje namjeravamo potpisati potrebno je da koristimo enkripciju iliti šifriranje. Šifriranje je postupak kodiranja (šifriranja) podataka prije slanja kako bi samo primatelj mogao dekodirati (dešifrirati) i razumjeti poslanu poruku. Ključevi prilikom šifriranja mogu biti jednaki (isti ključ) ili različiti ključevi. Tako nam i postoje dvije vrste: sustav sa simetričnim ključem (symetric key systems) te privatni i javni ključ. Sustav sa simetričnim ključem koristi isti ključ i prilikom šifriranja i dešifriranja. Potrebno je da se unaprijed odredi ključ između osoba koje komuniciraju, također on treba biti poznat samo njima, znači riječ je o tajnom ključu. Druge dvije vrste algoritama digitalnog potpisa: javni i privatni (tajni) ključ. Kod njih je riječ o različitim ključevima prilikom šifriranja i dešifriranja. U postupku šifriranja prije slanja pomaže nam privatni ključ, dok javni ključ ima ulogu kod dešifriranja. Javni ključ dostupan je naravno svima jer on nam provjerava autentičnost poruke, dok privatni ključ je tajan tj. jedino ga zna pošiljatelj.

U slučaju da nam dođe do zahtjevnije implementacije šifriranja s javnim ključem – onda koristimo digitalni certifikat.

U daljnjem radu opisala sam algoritme digitalnog potpisa te njihovu primjenu. Tu sam također navela i pametne kartice, usb stickove, biometrijske otiske prstiju te uređaj za digitalni potpis. Svaki od digitalnih potpisa ima naravno i svoje mane kao i svoje prednosti, no prednosti su nam uvijek od veće važnosti.

DIGITALNI POTPIS

Digitalni potpis danas je jedna od sasvim standardnih potpisa 21. stoljeća, uvelike nam je olakšao te uštedio dosta vremena.

Možemo reći da početak ideje započeo je još davne 1860.godine - > Morseova abeceda za prijenos poruka preko telegrafa, što je 1869. proglašeno pravomoćno. Tijekom 1980-ih godina na snagu nam stupa faks -> kao uređaj za hitan prijenos papirnatih dokumenata. Takva vrsta potpisa naziva se elektroničkom jer se i njezin prijenos vrši elektronički.

U podskupini elektroničkih potpisa nalazi nam se naravno i digitalni potpis.

Naime, digitalni potpis je način dokazivanja autentičnosti digitalne poruke ili dokumenta. To je matematički niz bajtova koji se koriste asimetričnim kriptografskim algoritmima. Kreira se iz sadržaja dokumenta i privatnog ključa pošiljatelja te se dodaje u dokument. Primatelj dešifrira hash koristeći javni ključ navodnog pošiljatelja te uspoređuje hasheve. Ako je digitalni potpis valjan, (tj. Hash od dokumenta i dešifriranje se podudaraju) na kraju svega primatelj može biti siguran u svog autora iliti pošiljatelja.

Istoznačan je kao pismeni (ručni) potpis i kao pečat, ali ga je teže krivotvoriti.

Digitalni potpis ima sljedeća svojstva:

- Autentifikacija -> Primatelj može reći tko je poslao dokument

- Ne odbacivanje -> Potpisnik ne može poreći potpisivanje dokumenta

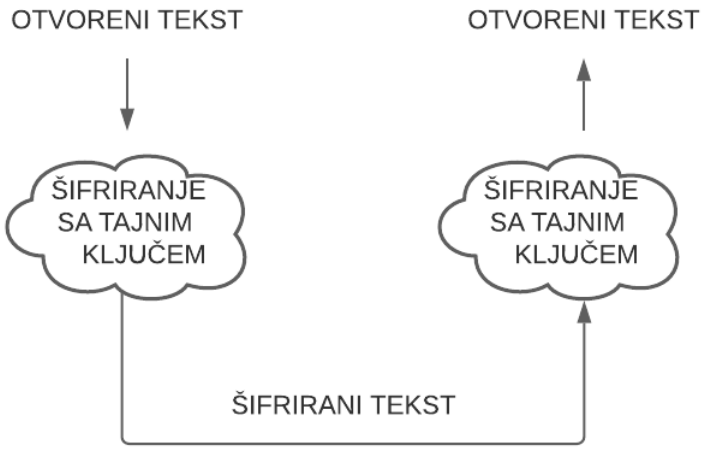
- Integritet -> Dokument nije promijenjen na putu do primatelja

ŠIFRITRANJE SA SIMETRIČNIM KLJUČEM

Naime, jedna od mana simetričnog ključa je to što je moguće da bude otkriven od strane napadača. Vlasnici ključa greškom mogu učiniti da ključ postane poznat i iz toga razloga obično se ne koristi isti ključ duže vrijeme. Osobe A i B na početku svake komunikacije mogu odrediti novi simetrični ključ koji bi se koristio u određenoj komunikaciji. Takav ključ naziva se ključem sesije (session key).[2]

Čimbenici zbog kojih bi bilo dobro redovno uvoditi novi simetrični ključ:
- koliko je važan sadržaj koji se prenosi
- da li se prenosi mnogo sadržaja ili pak malo.

Slika 1. Šifriranje sa simetričnim ključem (tajnim)



Izvor: Samostalni rad prema primjeru iz knjige: Computer Nerworks A Systems Approach, 3rd Edition-Petersen.pdf

ŠIFRIRANJE SA PRIVATNIM KLJUČEM

U prijašnjem odjeljku došli smo do zaključka kako su nam od velike važnosti i privatni i javni ključ.

Naime, šifriranje s privatnim ključem govori nam kako svako računalo ili korisnik (pošiljatelj) treba posjedovati tajni ključ pomoću kojega se podaci prije slanja računalnom mrežom, šifriraju. Idući korak je da primatelj treba znati pošiljateljev tajni ključ kako bi mogao dešifrirati primljene podatke. Kako bi sve teklo bez poteškoća, prije uspostavljanja komunikacije potrebno je znati koja računala će razmjenjivati poruke i naravno potrebno je da svako računalo ima instalirane privatne ključeve računala s kojih se očekuju poruke. To je proces kroz koji će primanje poruka biti sigurno i izvršeno.

DES (Data Encryption Standard) je najpoznatiji primjer šifriranja algoritma privatnog ključa, dok je IDEA (International Data Encryption Algorithm) drug.

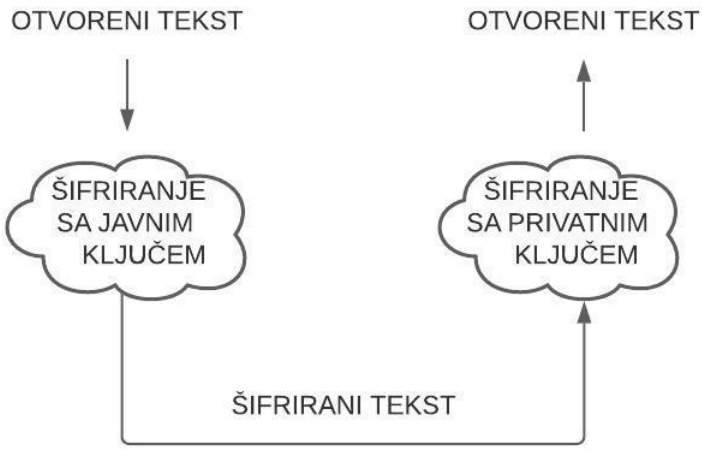
ŠIFRIRANJE SA JAVNIM KLJUČEM

Općenito govoreći utvrđeno je kako svaki korisnik posjeduje vlastiti privatni i javni ključ. Svaki korisnik ima mogućnost da provjerava potpis pomoću javnog ključa. Dok, privatnim ključevima mogu pristupiti samo vlasnici i na taj način je onemogućeno krivotvorenje potpisa. Podaci koji se obrađuju digitalnim potpisom nazivaju se porukom. Kroz tijek stvaranja digitalnog potpisa za dobivanje sažete inačice poruke (eng. message digest) funkcija koja se koristi je jednosmjerna tzv. SHA (eng. Secure Hash Algorithm) algoritam.

Riječ je o funkcijama koje se matematički vrlo jednostavno izračunavaju, ali im je teško pronaći inverznu funkciju. Iz sažete inačice poruke DS algoritmom stvara se digitalni potpis. Poruka se, zajedno s pripadnim potpisom, šalje primaocu koji pomoću pošiljateljeva javnog ključa utvrđuje vjerodostojnost poruke i samog digitalnog postupka.[2] U procesu provjere potrebno je koristi SHA algoritam isti onaj korišten prilikom stvaranja potpisa.

RSA - nazvan po izumiteljima, Rivestu, Shamiru i Adlemanu - najpoznatiji je algoritam šifriranja javnog ključa.

Slika 2. Šifriranje sa javnim i privatnim ključem



Izvor: Samostalni rad prema primjeru iz knjige: Computer Nerworks A Systems Approach, 3rd Edition-Petersen.pdf

HASH

Naime, prve dvije vrste algoritama naravno uključuju upotrebu ključeva, dok kriptografske hash funkcije (SHA (eng. Secure Hash Algorithm)) većinom ne uključuju upotrebu ključeva. No, umjesto toga, ideja je mapirati potencijalno veliku poruku u mali broj fiksne duljine, analogno procesu na koji uobičajena hash funkcija preslikava vrijednosti iz velikog prostora u vrijednosti iz malog prostora.

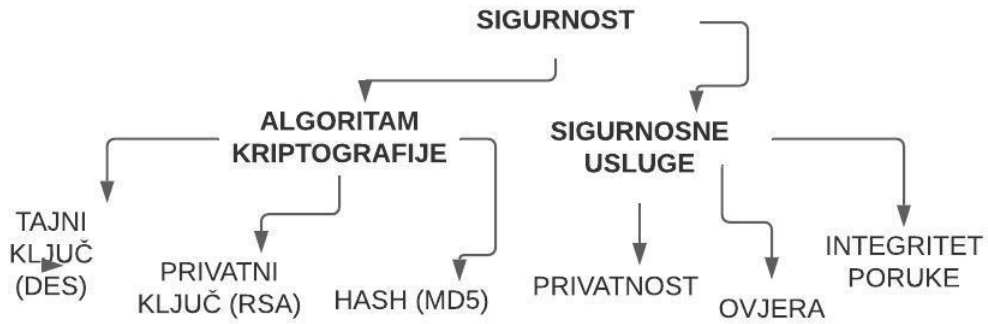
Najbolji način kako bi se kriptografska hash funkcija shvatila je taj što ona izračunava kriptografski kontrolni zapis preko poruke tj. Redoviti kontolni zapis štiti primatelja od slučajnih promjena poruke, tako i kriptografski kontrolni zapis štiti primatelja od zlonamjernih promjena u trenutnoj poruci. Jednostavno govoreći, svi kriptografski hash algoritmi pažljivo su odabrani da budu jednosmjerne funkcije - s obzirom na kriptografski kontrolni zapis

poruku, te je gotovo nemoguće shvatiti koja je poruka proizvela taj kontrolni zapis.

Naime, računski nije izvedivo pronaći dvije poruke koje se raspršuju u isti kriptografski kontrolni zbroj. Ako ste dobili kontrolni zapis za poruku (zajedno s porukom) i ako ste u mogućnosti izračunati potpuno istu kontrolni zapis, naravno da je velika vjerojatnost da je ova poruka stvorila kontrolni zapis koju ste dobili. [2]

Najrasprostranjeniji kriptografski algoritam kontrolni zapis je Message Digest verzija 5 (MD5). Također, mnogo ga je učinkovitije izračunati od DES ili RSA.

Slika 3. Mrežna sigurnost, DES,RSA i MD5 algoritmi



Izvor: Samostalni rad prema knjizi: Computer Nerworks A Systems Approach, 3rd Edition-Petersen.pdf

ALGORITMI DIGITALNOG POTPISA

DES

(Secret Key Encryption)

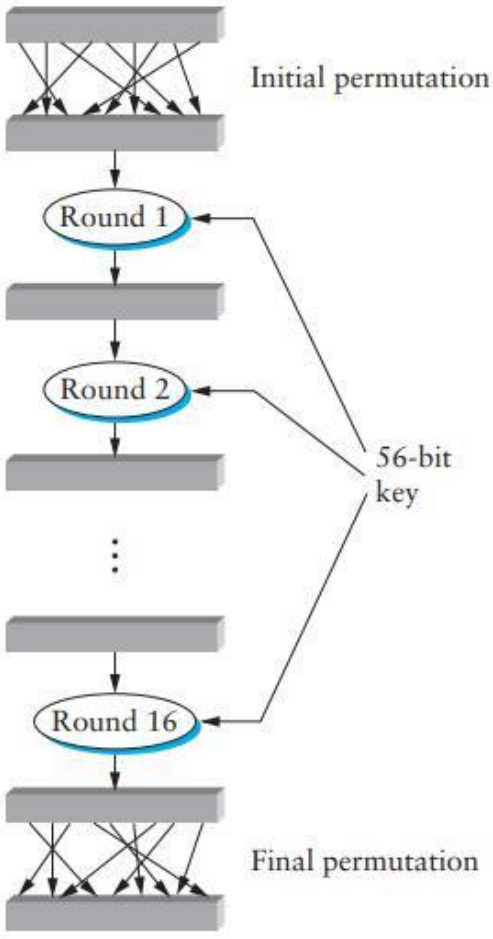
DES šifrira 64-bitni blok otvorenog teksta pomoću 64-bitnog ključa. Ključ sadrži samo 56 upotrebljivih bitova - zadnji bit svakog od 8 bajtova u ključu bit je za taj bajt. Također, poruke veće od 64 bita mogu se šifrirati pomoću DES-a.

DES ima tri različite faze:

- 64 bita u bloku su izmiješana

- Šesnaest krugova identične operacije primjenjuje se na rezultirajuće podatke i ključ

- Na rezultat se primjenjuje inverzna izvorna permutacija.



Slika 4. DES na visokoj razini

Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

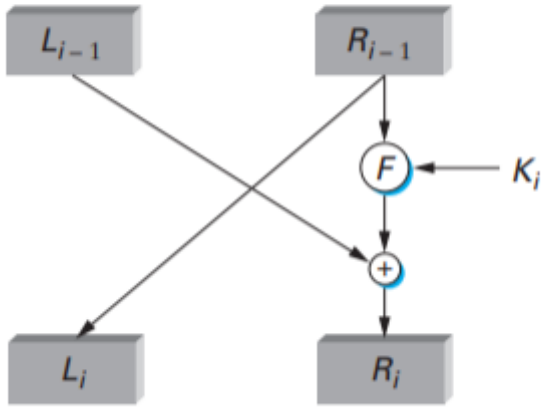
Slika 5. Početna i konačna DES permutacija

Input Position	1	2	3	4	5	...	60	61	62	63	64
Output Position	40	8	48	16	56	...	9	49	17	57	25

Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

Naime, Slika 5. predstavlja dio početne permutacije. Konačna permutacija je inverzna (npr. Bit 40 bio bi permutiran u položaj bita 1). Općenito se slaže da ove dvije permutacije ne pružaju nikakvu sigurnost DES-a. Neki sigurnosni stručnjaci nagađaju da su oni bili uključeni kako bi proračun trajao dulje, no jednako je vjerojatno da su oni početne hardverske implementacije.
Tijekom svakog kruga, 64-bitni blok se dijeli na dvije 32-bitne polovice, a različitih 56 bitova odabire se iz 56-bitne tipke. [2]

Slika 6. Manipulacija u svakom krugu DES-a



Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

Ako lijevu i desnu polovicu bloka u krugu i označimo kao Li, odnosno Ri, a 48-bitni ključ u krugu i kao Ki, tada se ova tri dijela kombiniraju tijekom i kruga prema slijedećem pravilu:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

gdje je F kombinirana funkcija opisana u nastavku, a $\oplus$ je ekskluzivno-ILI (XOR) operator.

Slika 6. ilustrira osnovnu operaciju svakog kruga. Imajte na umu da L0 i R0 odgovaraju lijevoj i desnoj polovici 64-bitnog bloka koji je rezultat početne permutacije, te da se L16 i R16 kombiniraju natrag zajedno da tvore 64-bitni blok na koji se primjenjuje konačna inverzna permutacija.

Sada moramo definirati funkciju F i pokazati kako je svaki Ki izveden iz 56-bitnog ključa. Počinjemo s ključem. U početku se 56-bitni ključ permutira prema Slici 7.

Imajte na umu da se svaki osmi bit zanemaruje (tj. Bit 64 nedostaje u tablici), smanjujući ključ sa 64 bita na 56 bita. Zatim se za svaki krug trenutnih 56 bitova podijeli u dvije 28-bitne polovice i svaka se polovica neovisno okreće ulijevo ili u jedan ili dva bita, ovisno o rundi. Opseg rotacije u bitovima za svaki krug dan je u Slici 8.

56 bitova koji su rezultat ovog pomaka koriste se i kao ulaz za sljedeću rundu (tj. ponavlja se prethodni pomak) i za odabir 48 bitova koji čine ključ za trenutnu rundu.

Slika 9. pokazuje kako je odabrano 48 od 56 bitova; imajte na umu da se istovremeno biraju i permutiraju.[2]

Slika 7. Permutacija DES ključa

Input Position	1	2	3	4	5	...	59	60	61	62	63
Output Position	8	16	24	56	52	...	17	25	45	37	29

Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

Slika 8. DES ključ, rotacija iznosa po rundi

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Rotation Amount	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

Slika 9. DES permutacija kompresije

Input Position	1	2	3	4	5	6	7	8	10	11	12	13	14	15	16	17
Output Position	5	24	7	16	6	10	20	18	12	3	15	23	1	9	19	2

Input Position	19	20	21	23	24	26	27	28	29	30	31	32	33	34	36	37
Output Position	14	22	11	13	4	17	21	8	47	31	27	48	35	41	46	28

Input Position	39	40	41	42	44	45	46	47	48	49	50	51	52	53	55	56
Output Position	39	32	25	44	37	34	43	29	36	38	45	33	26	42	30	40

Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

RSA

(Public Key Enctryption)

Naime, RSA je puno drugačiji algoritam, ne samo zato što uključuje različite ključeve za šifriranje (javni ključ) i dešifriranje (privatni ključ), već i zato što je utemeljen u teoriji brojeva.

Čin šifriranja ili dešifriranja poruke izražava se kao jednostavna funkcija, iako ta funkcija zahtijeva ogromnu računsku snagu. Konkretno, RSA obično koristi duljinu ključa od 1024 bita, što čini računanje puno skupljim od DES-a.

Prvi je zadatak generirati javni i privatni ključ. Kako bi to bilo obavljeno, potrebno je odabrati dva velika prosta broja p i q i pomnožiti ih zajedno da bi se dobio n. I p i q trebali bi biti otprilike 256 bita. Zatim je potrebno odabrati ključ za šifriranje e, tako da su e i (p - 1) × (q - 1) relativno prosti. (Dva broja relativno su prosta ako nemaju zajednički faktor veći od 1.) Na kraju, izračunavanje ključa za dešifriranje d tako da je

$$d = e^{-1} \bmod ((p - 1) \times (q - 1))$$

Javni ključ je konstruiran iz para e, n, a privatni ključ daje par d, n. Izvorni prosti brojevi p i q više nisu potrebni. Mogu se odbaciti, ali ne smiju se otkriti.

S obzirom na ova dva ključa, šifriranje je definirano sljedećom formulom:

$$c = m^e \bmod n,$$

a dešifriranje je definirano

$$m = c^d \bmod n,$$

gdje je m poruka otvorenog teksta, a c rezultirajuća šifra teksta. Nemoguće je da bude manje od n, što znači da ne može biti duže od 1024 bita. Veća poruka jednostavno se tretira kao spajanje više 1024-bitnih blokova

Sljedeći primjer pokazuje vrlo male vrijednosti p i q. Pretpostavimo da odaberemo p = 7 i q = 11. To znači da je

$n = 7 \times 11 = 77$ i

$$(p - 1) \times (q - 1) = 60,$$

tako da moramo odabrati vrijednost e koja je relativno prosta prema 60. Odabiremo e = 7; 7 i 60 nemaju zajednički faktor osim 1. Sada moramo izračunati d tako da je

$$d = 7^{-1} \bmod ((7 - 1) \times (11 - 1)),$$

što znači

$$7 \times d = 1 \bmod 60$$

Ispada iz toga je d = 43, budući da je

$$7\times43=301$$

$$= 1 \bmod 60$$

Dakle, sada imamo javni ključ e, n = 7, 77 i privatni ključ d, n = 43, 77. Iduće prikazujemo jednostavnu operaciju šifriranja. Pretpostavimo da želimo šifrirati, a poruka koja sadrži vrijednost 9. Slijedeći gornji algoritam šifriranja:

$$c = me \bmod n$$

$$= 9\ 7 \bmod 77$$

$$= 37$$

Dakle, 37 je šifrirani tekst koji bismo poslali.

Po primitku poruke šifrirani tekst šifrirao bi se na sljedeći način:

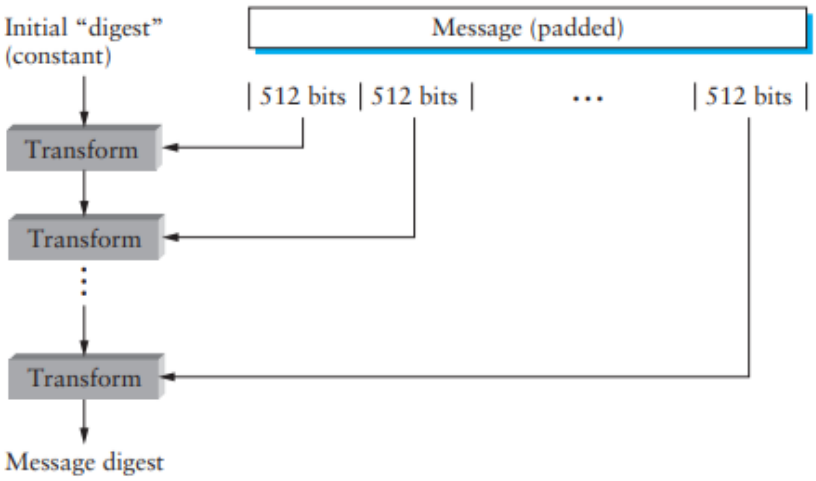
$m = c\ d \bmod n = 3743 \bmod 77 = 9$

Dakle, prema potrebi, izvorna poruka se obnavlja.

Primijetite da kada dva sudionika žele za šifriranje podataka koje međusobno šalju pomoću algoritma javnog ključa poput RSA potreban je par javnih / privatnih ključeva. Ne radi šifriranje privatnim ključem, a druga strana neka dešifrira javnim ključem, jer svi imaju pristup javnom ključu, pa bi tako mogla dešifrirati poruku. Drugim riječima, sudionik šifrira podatke koje šalje sudioniku B pomoću B-ovog javnog ključa, a B koristi svoj privatni ključ za dešifriranje tih podataka, dok B šifrira podatke koje šalje A koristeći javni A ključ, a A dešifrira ovu poruku pomoću svog privatnog ključa. Primijećeno je kako A ne može dešifrirati poruku koju je poslao B; samo B ima potrebni privatni ključ. RSA sigurnost dolazi od pretpostavke da je računanje velikih brojeva računski skup prijedlog. Konkretno, ako biste mogli računati faktor n, mogli biste oporaviti p i q, što bi ugrozilo d.

Brzina kojom se mogu računati veliki brojevi funkcija je i dostupne brzine procesora i algoritma faktoringa koji se koristi. Procjenjuje se da će 512-bitni brojevi biti dostupni u sljedećih nekoliko godina zbog čega ljudi sada koriste 1024-, pa čak i 2048-bitne ključeve.[2]

Slika 10. Pregled operacije sažetka poruke.



Izvor: Computer Networks A Systems Approach, 3rd Edition-Petersen.pdf

MD5

(Message Digest Algorithms)

Postoji niz popularnih algoritama za izračunavanje sažetka poruke poznat kao MDn za različite vrijednosti n.

Sigurni hash algoritam (SHA) još je jedna poznata funkcija sažetka poruka. Sve ove funkcije obavljaju gotovo istu stvar, a to je izračunavanje kriptografske sume fiksne duljine iz proizvoljno ulazne poruke. Matematički algoritmi sakupljanja poruka imaju tendenciju više zajedničkog s DES-om nego s RSA-om. Odnosno, nemaju formalne matematičke temelje, već se oslanjaju na složenost algoritma kako bi proizveli slučajni izlaz tako da su ispunjeni gore navedeni zahtjevi.

Naime, sam MD5 algoritam čini se da je slučajna zbirka transformacija, pa nije niti čudno da daje odgovarajuće slučajne izlaze.

3 Osnovna operacija MD4, MD5 i SHA prikazana je na Slici 10.

Ti algoritmi istodobno djeluju na poruku od 512 bita, pa je prvi korak dodavanje poruke na višekratnik od 512 bita. To se postiže slijedeći poruku između 1 i 512 bita za popunjavanje, od kojih je prvi 1, ostatak je 0, a zatim slijedi onaj s 64-bitnim cijelim brojem koji je izvorna duljina poruke u bitovima. Imajte na umu da ovo omogućuje poruke proizvoljne duljine do 264 bita. Izračun sažetka započinje sa sažetkom vrijednosti inicijaliziranim u konstantu; ta se vrijednost kombinira s prvih 512 bitova poruke kako bi se dobila nova vrijednost sažetka, koristeći složenu transformaciju opisanu u nastavku; nova vrijednost kombinira se sa sljedećih 512 bitova poruke koristeći istu transformaciju, i tako dalje, sve dok se ne proizvede konačna vrijednost sažetka.

Stoga je glavni sastojak MD5 algoritma transformacija koja uzima za ulaz trenutnu vrijednost 128-bitnog sažetka, plus 512 bitova poruke i daje novi 128-bitni sažetak.

MD5, poput ostalih modernih algoritama za sažetak, radi na 32-bitnim količinama, jer se njima učinkovito rukuje u modernim procesorima. Tako da trenutnu vrijednost sažetka možemo zamisliti kao četiri 32-bitne riječi (d0, d1, d2, d3), a dio poruke koja se trenutno probavlja kao šesnaest 32-bitnih riječi (m0 do m15). Osnovna transformacija koju izvodi MD5 može se podijeliti u četiri prolaza. U prvom prolazu, nova vrijednost sažetka izrađuje se od stare vrijednosti i 16 riječi poruka pomoću 16 koraka, od kojih je prvih 6 prikazano u nastavku:

$$d0 = (d0 + F(d1, d2, d3) + m0 + T1) \leftarrow 7$$

$$d3 = (d3 + F(d0, d1, d2) + m1 + T2) \leftarrow 12$$

$$d2 = (d2 + F(d3 , d0, d1) + m2 + T3) \leftarrow 17$$

$$d1 = (d1 + F(d2, d3, d0) + m3 + T4) \leftarrow 22$$

$$d0 = (d0 + F(d1, d2, d3) + m4 + T5) \leftarrow 7$$

$$d1 = (d3 + F(d0, d1, d2) + m5 + T6) \leftarrow 12$$

Taj se postupak nastavlja dok se svih 16 riječi ne probavi. Svaki korak dovodi do prepisivanja jedne sažetke riječi, pri čemu nova vrijednost ovisi o njenoj staroj vrijednosti, trenutnoj vrijednosti ostale tri sažete riječi i jednoj riječi poruke koja se probavlja.

Funkcija F (a, b, c) kombinacija je bitnih operacija (ILI, I, NE) na svojim argumentima. Ti su konstante. ← n operator okreće operand lijevo za n bitova. Drugi prolazak izgleda otprilike isto kao i prvi prolazak.

Razlike su sljedeće:

- F je zamijenjen nešto drugačijom funkcijom G.

- Konstante T1 do T16 zamjenjuju se drugim skupom (T17 do T32).

- Količina lijeve rotacije iznosi {5, 9, 14, 20, 5, 9, ...} u svakom koraku.

- Umjesto da se bajtovi poruke uzimaju redom od m0 do m15, bajt poruke koji se koristi u fazi i je m (5i + 1) mod16.

U trećem prijelazu:

- G je zamijenjen još jednom funkcijom H, koja je samo XOR njegovih argumenata.

- Koristi se drugi skup konstanti (T33 do T48).

- Količina lijeve rotacije iznosi {4, 11, 16, 23, 4, 11, ...} u svakom koraku.

- Bajt poruke koji se koristi u fazi i je m (3i + 5) mod16.

Četvrti prijelaz ima sljedeća svojstva:

- H je zamijenjen funkcijom I, koja je kombinacija bitnih XOR, OR i NOT na svojim argumentima.

- Koristi se drugi skup konstanti (T49 do T64).

- Količina lijeve rotacije iznosi {6, 10, 16, 21, 6, 10, ...} u svakom koraku.

- Bajt poruke koji se koristi u fazi i je m (7i) mod16. Nakon cijelog ovog rada, izvorne vrijednosti (d0, d1, d2, d3) temeljito su iskrivljene na način koji, iako potpuno ovisan o bajtovima poruke, ne pruža algoritamski način da se otkrije koji su to bajtovi poruke.

Iskrivljeni sažetak sada se dodaje vrijednosti sažetka koja je postojala prije trenutne faze i to postaje nova vrijednost sažetka. Algoritam sada probavlja sljedećih 16 bajtova poruke sve dok više ne bude probavljeno; rezultat posljednje faze je sažetak poruke. Iako nije baš toliko računski učinkovit kao neki raniji probavni provodi, MD5 je po tom pitanju još uvijek prilično dobar. Imajte na umu da se sve operacije - u bitovima ILI, A NE, XOR, dodavanje i rotacija - lako implementiraju u moderne procesore.[2]

CA CERTIFIKATI

Za digitalne certifikate možemo reći da se koriste prilikom zahtjevnije implementacije šifriranja sa javnim ključem (public key). CA certifikat sadrži javni ključ i naziv CA koji je izdao certifikat.

Certifikat je elektronički dokument, koristi se u svrhu identificiranja osoba, servera, određene tvrtke za povezivanje identiteta sa javnim ključem. On nam daje vjerodostojan dokaz o identitetu.
Kriptografija javnog ključa (Public key criptography) koristi certifikate kako ne bi imala probleme s lažnim predstavljanjem.
Certifikacijske vlasti (Certificate authorities **CA**) su službe koje potvrđuju određene identitete i izdaju certifikate, a koja predstavljaju dio PKI (eng. Public key infrastructure) sustava. PKI djeluje kao posrednik između dva računala ili korisnika te potvrđuje njihove identitete i razmjenjuje javne ključeve.
Elektroničke transakcije zaštićene korištenjem PKI-a bazirane na digitalnom certifikatu i elektroničkom potpisu zadovoljavaju sljedeće osnovne zahtjeve:

1) Autentikacija – proces provjere korisničkog identiteta, odnosno korisnik dokazuje da je zaista onaj za kojeg se predstavlja
2) Integritet – sigurnost da podaci u prijenosu ili obradi nisu uništeni ili promijenjeni. Elektroničkim potpisom osigurava se cjelovitost i izvornost podataka pohranjenih na određeno vrijeme ili onih koji se šalju mrežom.
3) Tajnost - Šifriranje podataka koji će biti pohranjeni ili poslani mrežom štiti čitanje sadržaja od neovlaštenih osoba.
4) Neporecivost – onemogućavanje megiranje akcije koje je osoba poduzela ili autorizirala. Ova mogućnost je realizirana kroz napredni elektronički potpis.

Mreža povjerenja (eng. web of trust) predstavlja alternativu centraliziranim PKI sustavima, a koristi se kod PGP (eng. Pretty Good Privacy), GnuPGP i drugih sustava kompatibilnih s OpenPGP standardom.

Korisnici koristeći vlastite privatne ključeve, potpisuju identifikacijske certifikate drugih korisnika. [2]

FINA CA CERTIFIKATI

Za korištenje certifikata izdanih od strane Fina RDC 2015 i Fina RDC-TDU 2015 CA-ova, potrebno je jednokratno u računalo importirati Fina Root CA certifikat kako bi se u naknadnoj primjeni certifikata mogla uspješno obavljati verifikacija istih.

FISKALIZACIJA

Aplikacijski certifikati koje Fina izdaje za potrebe fiskalizacije su certifikati u soft obliku, oni su naravno u skladu s međunarodnim standardima i njihovo korištenje moguće je na raznim platformama, što znači da nisu ograničeni niti na jednu specifičnu računalnu platformu.

Obveznici fiskalizacije, kako bi se fiskalizacija provela:

- potrebno je da od Fine zatraže izdavanje produkcijskog aplikacijskog certifikata koji se u postupku fiskalizacije koristi za elektroničko potpisivanje elemenata računa te za identifikaciju obveznika fiskalizacije prilikom elektroničke razmjene podataka.

Ukoliko Informatička tvrtka želi u ime obveznika fiskalizacije nabaviti produkcijski aplikacijski certifikat, to nažalost ne može, nego je sam obveznik dužan sam zatražiti.

Iznimka, osoba ovlaštena za zastupanje može dati pravo skrbnika osobi koja nije zaposlena kod obveznika (npr. djelatniku informatičke tvrtke koja kod obveznika uspostavlja sustav fiskalizacije). U tome slučaju 'skrbnik' bi preuzeo certifikat u ime obveznika fiskalizacije.

Skrbnik je fizička osoba koja ima određene zadatke: preuzimanje, uporaba, briga i čuvanje certifikata koji je izdan za aplikaciju. Skrbnik može biti i osoba ovlaštena za zastupanje poslovnog subjekta.
Kako bi se olakšao i ubrzao postupak uspostave sustava fiskalizacije koje provode informatičke tvrtke, Fina je na temelju iskustva u razvoju sličnih

rješenja za elektroničko potpisivanje, razvila programsku komponentu za elektroničko potpisivanje poruka - Modul XmlSigner**.** [3]

PRIMJER AKTIVACIJE FISKALIZACIJE

Prva stvar koju je potrebno u FINI je omogućiti FISKAL 1 - certifikat potreban za šifriranje podataka u komunikaciji sa poreznom upravom

U postupku preuzimanja FISKAL 1 certifikata sa FINA-e potrebno je da osoba upiše lozinku. Lozinku je potrebno upisati da bi se osiguralo da certifikat može koristiti samo osoba koja zna tu lozinku.

Vlastita poslovna jedinica alatni uređaj prijavljuje se preko sustava ePorezna. Nakon prijave poslovne jedinice i nakon što preuzmete FISKAL 1 certifikat potrebno je u programu postaviti opcije fiskalizacije.

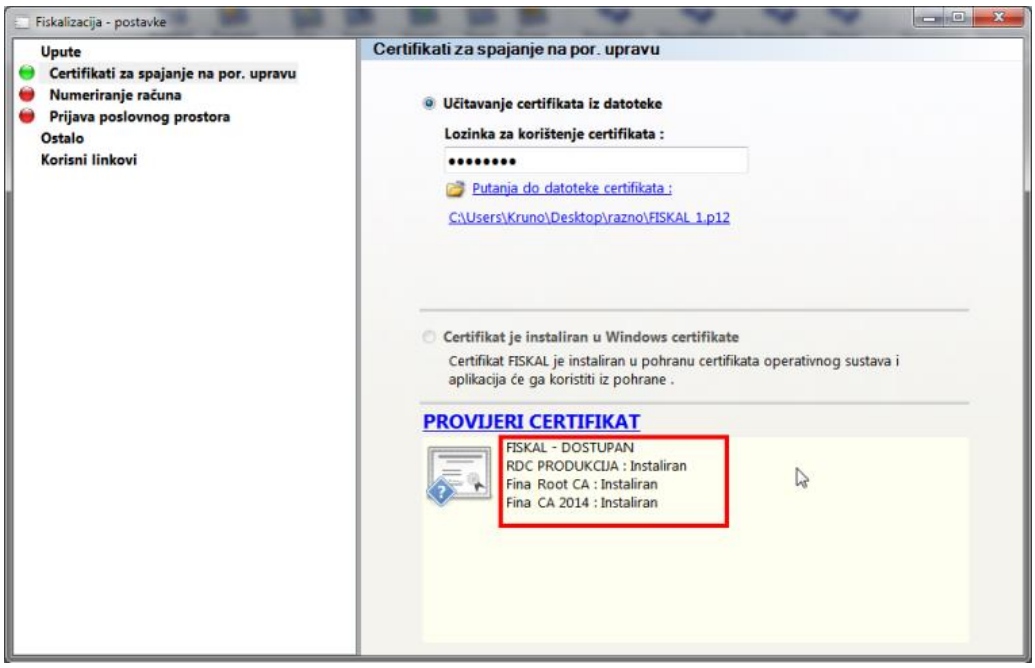
Aktivacija fiskalizacije:

1. Certifikati za fiskalizaciju
2. Numeracija računa, poslovne jedinice i naplatni uređaj
3. Aktivacija fiskalizacije
4. Naknadna promijena lokacije FISKAL 1 certifikata

1. Certifikati za fiskalizaciju

Prvi korak je upisivanje lozinke koju smo definirali kod preuzimanja certifikata. Nakon što je lozinka upisana potrebno je kliknuti na link "Putanja do datoteke certifikata" i pokazati programu lokaciju certifikata na računalu.
Nakon toga slijedi "PROVJERI CERTIFIKAT" te se u popisu kategorija pojavljuje se zelena kuglica kraj kategorije "Certifikati za spajanje na poreznu upravu".

Slika 11. Prikazuje provjeru certifikata pri prvom koraku fiskalizacije



Izvor: http://www.fakturiranje.biz/Help/FiskalizacijaAktivacija.htm

2. Numeracija računa, poslovne jedinice i naplatni uređaj

Ovdje je potrebno upisati podatke koji su prijavljeni preko sustava ePorezna.

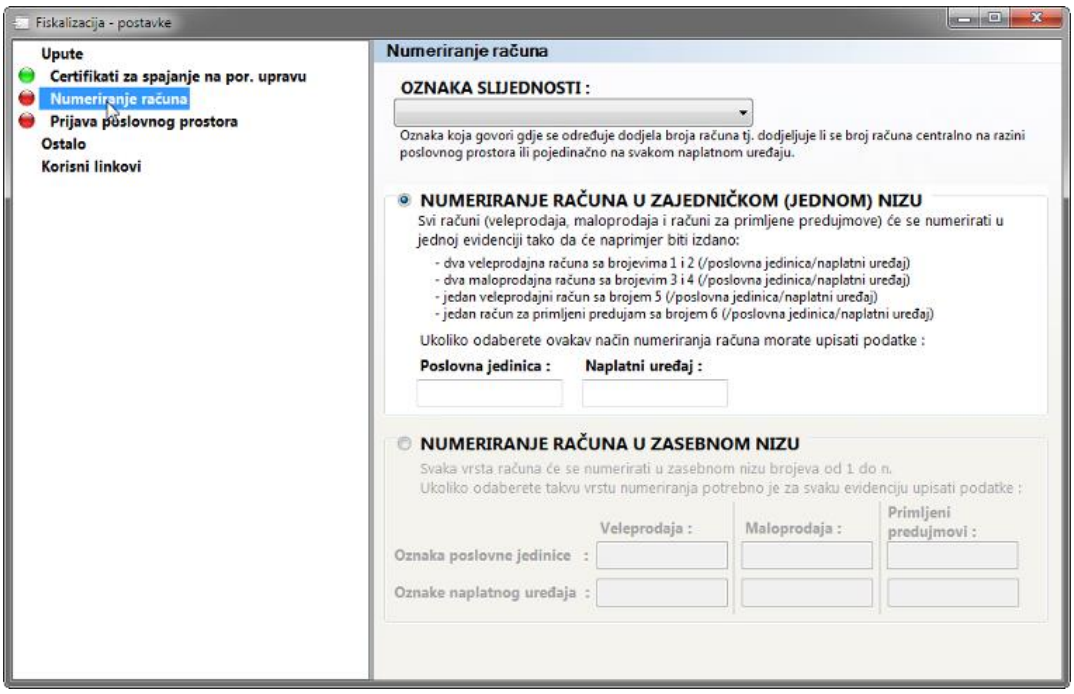
Odabire se slijednost i evidencija računa.
Obavezno je upisati nazive poslovnih jedinica i naplatnog uređaja.

Primjer :

- Ukoliko u programu koristite sustave "Veleprodaja" i "Maloprodaja" zasebno i želite da Vam tako i ostane a preko ePorezne ste prijavili dvije poslovne jedinice označite opciju "Numeriranje u zasebnom nizu" te kvačicama ispod potrebne evidencije koje će se fiskalizirati.Za "Veleprodaju" upišite njezine fiskalne oznake a za "Maloprodaju" posebno njezine fiskalne oznake.

Također je vrlo važno da donesete interne akte koji definiraju nazive poslovnih jedinica i naplatnih uređaja koje ste unijeli u program.

Slika 12. Prikazuje numeriranje računa

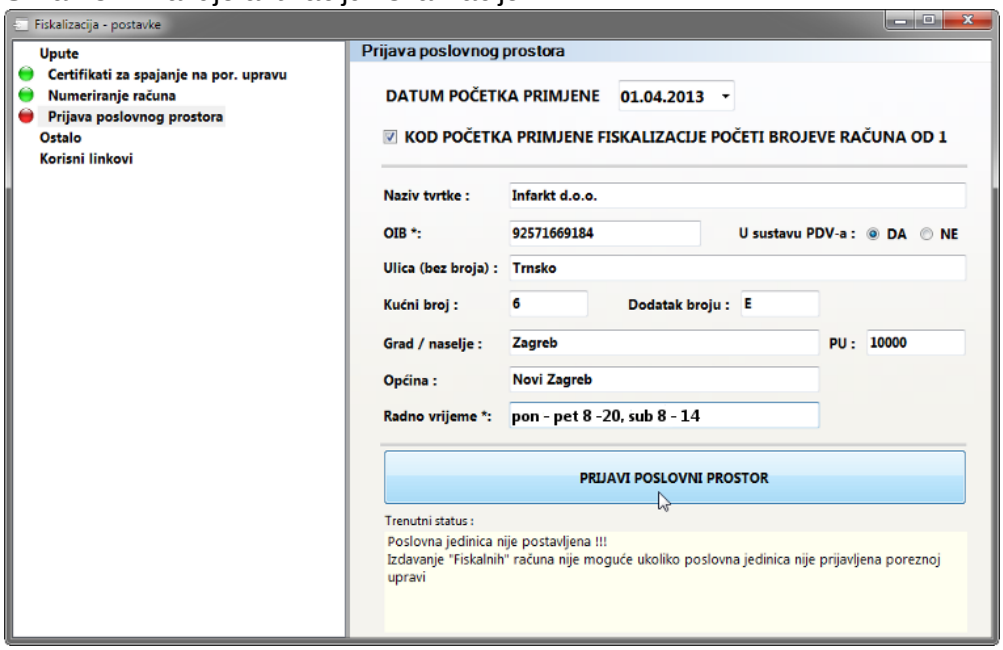


Izvor: http://www.fakturiranje.biz/Help/FiskalizacijaAktivacija.htm

3. Aktivacija fiskalizacije

Nakon što su uneseni podaci preko ePorezne potrebno je kliknuti na gumb "Prijavi poslovnu jedinicu" i u program fiskaliziranje računa počinje biti aktivan.

Slika 13. Pikazuje aktivaciju fiskalizacije

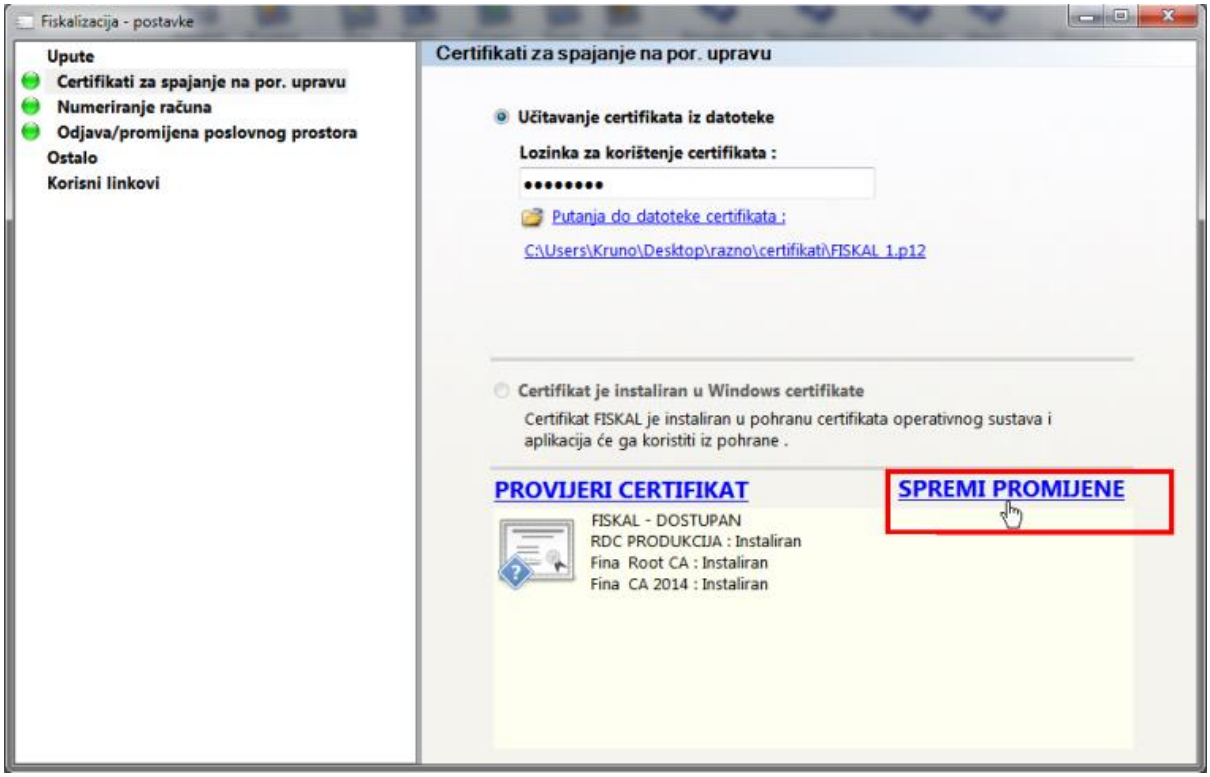


Izvor: http://www.fakturiranje.biz/Help/FiskalizacijaAktivacija.htm

4. Naknadna promjena lokacije FISKAL 1 certifikata

Naime, fiskalizacija nije moguća ukoliko se FISKAL 1 ne nalazi u mapi u kojoj je bio kod prijave poslovne jedinice. Za postavljanje nove lokacije FISKAL 1 certifikata potrebno je kliknuti na link "Putanja do datoteke certifikata" i pokazati programu lokaciju gdje se nalazi certifikat. Nakon toga "PROVIJERI CERTIFIKAT" da program provjeri da li je sa certifikatom sve u redu. Ukoliko je provjera uspješna pojaviti će se link "SPREMI PROMIJENE" i program će FISKAL 1 učitavati iz novo postavljene lokacije.

Slika 14. Prikazuje naknadnu promjenu lokacije certifikata



Izvor: http://www.fakturiranje.biz/Help/FiskalizacijaAktivacija.htm

ZABA CA CERTIFIKATI

Banka za svoje klijente građane i poslovne subjekte omogućava ugovaranje određenih proizvoda i usluga na direktnim kanalima Banke kvalificiranim elektroničkim potpisom koji ima istu snagu kao vlastoručni potpis.

Zaba QPKI sustav certificiranja: cilj joj je pružanje usluga certificiranja tj. izdavanja i korištenja kvalificiranih certifikata, izrade kvalificiranog elektroničkog potpisa te izdavanja kvalificiranog vremenskog žiga.

Zaba QTSA kao dio Zaba QPKI sustava, koji se primarno koristi za očuvanje dugotrajnosti elektroničkih potpisa - > to je servis za izdavanje kvalificiranih vremenskih žigova.

Usluge certificiranja i vremenskog žiga usklađene su sa zakonskom regulativom o elektroničkom potpisu u Republici Hrvatskoj, europskom Uredbom o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (eID.AS - EU regulation No. 910/2014), te primjenjivim međunarodnim normama iz područja pružanja usluge certificiranja i izdavanja kvalificiranog vremenskog žiga.

Banka kao davatelj usluga certificiranja za korisnike izdaje sljedeće grupe certifikata:

Osobni potpisni kvalificirani certifikat (QCP-n-qscd) - certifikat visoke razine sigurnosti koji se izdaje fizičkim osobama na daljinu unutar Zaba QPKI infrastrukture, a koristi se isključivo za udaljenu izradu kvalificiranog elektroničkog potpisa u sklopu pružanja usluga Banke na direktnim kanalima, također pravila vrijede i ta poslovne subjekte.[4]

ELEKTONIČKA OSOBNA ISKAZNICA (eOI)

Elektronička osobna iskaznica (eOI) sadrži elektroničku identifikaciju i elektronički potpis te pouzdan pristup elektroničkim servisima javne uprave. Također, nudi nam korištenje elektroničkog potpisa, online pristup službenim dokumentima i obrascima te dodatna mogućnost korištenja drugih servisa u području e-usluga.

Naša stara osobna iskaznica imala je funkciju isključivo za fizičku identifikaciju građana RH. Dok je u novu elektroničku iskaznicu ugrađen čip koji sadrži: - ----identifikacijski certifikat -> on nam služi za osiguranje elektroničke potvrde identiteta osobe kojoj je izdana osobna iskaznica

-te autentikaciju -> pristupanje elektroničkim uslugama te potpisni certifikat koji nam je potreban za podršku naprednom elektroničkom potpisu koji ima istu pravnu vrijednost i zamjenjuje vlastoručni potpis.

Oba certifikata mogu se koristiti u kombinaciji s osobnim PIN-om.

Certifikati sadrže identifikacijske podatke od određene osobe i njezin javni ključ (public key) u elektroničkom obliku.

Javni ključ omogućuje da se podaci povežu s fizičkom osobom kako bi došlo do verificiranja elektroničkog potpisa i potvrde identiteta osobe.

Certifikati na eOI su kvalificirani.

Rok valjanosti certifikata je 5 godina, a kada dođe do isteka, osoba između 18 i 65 godina starosti je dužna podnijeti zahtjev za izdavanje nove osobne iskaznice.

Identifikacija

Kako bi pristupili sustavu e-Građani - https://pretinac.gov.hr koristimo svoju elektroničku osobnu iskaznicu koja nam naravno mora imati aktivan identifikacijski certifikat.

Kvalificirani digitalni potpis

Elektronička osobna iskaznica također nam služi i za obavljanje aktivnosti vezanih uz ovjeru dokumenata elektroničkim potpisom kao pravomoćnom zamjenom za vlastiti potpis.

Opoziv certifikata podrazumijeva poništenje važenja izdanog certifikata.

U slučaju da želimo opozvati certifikat, više ga nije moguće povući ni obnoviti. Naime, potrebno je podnijeti zahtjev za izdavanje novog certifikata, odnosno zahtjev za izdavanje nove osobne iskaznice.

Sve je toliko ažurno da već nakon opoziva certifikata, informacija o tome objavljuje se na listi opozvanih certifikata davatelja usluga certificiranja.

Opoziv certifikata podnosi se isključivo osobno u policijskoj upravi/postaji.

U AKD-u je uspostavljena PKI (*Public Key Infrastructure*) infrastruktura koja omogućuje izdavanje certifikata za eOI.

AKD PKI:

PKI infrastruktura je uređena je hijerarhijski i sastoji se od:

-krovnog ovjerovitelja AKDCA Root, koji samom sebi izdaje certifikat i

-podređenog ovjerovitelja HRIDCA, koji izdaje certifikate fizičkim osobama.

Certifikati koje izdaje AKD PKI su kvalificirani i izdaju se u skladu sa Zakonom o elektroničkom potpisu, Uredbom EU, te vezanim pod zakonskim aktima i normama.

Certifikati su usklađeni s pravilima za „QCP public + SSCD“ prema normi EN 319 411-2.

AKD je upisan u evidenciju ministarstva nadležnog za poslove gospodarstva kao davatelj usluga certificiranja koji obavlja usluge izdavanja kvalificiranih certifikata.

HRIDCA nam je pravilnik o postupcima certificiranja. Njegova zadaća je da definira postupke i mjere koje primjenjuju Agencija za komercijalnu djelatnost d.o.o. i Ministarstvo unutarnjih poslova tijekom upravljanja postupaka certificiranja za elektroničku osobnu iskaznicu (eOI), fizičke osobe i zainteresirane strane prilikom korištenja certifikata na eOI.

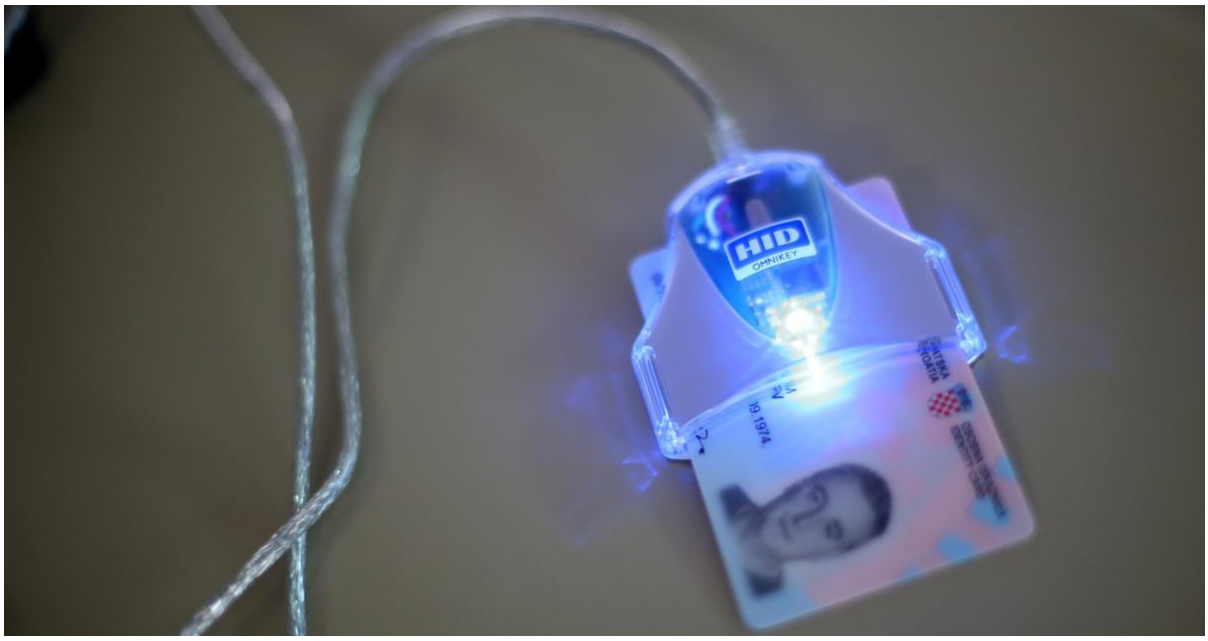
AKD PKI spadaju u opća pravila davanja usluga certificiranja. Ona definiraju skup pravila i sigurnosnih zahtjeva koji se moraju upotrebljavati prilikom upravljanja postupcima certificiranja za elektroničku osobnu iskaznicu (eOI) i korištenja certifikata na eOI.

Svi certifikati osoba potpisani su od strane ovjerovitelja HRIDCA.

Certifikat ovjerovitelja HRIDCA potpisuje krovni ovjerovitelj AKDCA Root.

AKDCA Root je samo potpisni certifikat.[8]

Slika 15. Prikazuje električnu osobnu iskaznicu i čitač



Izvor: https://www.vecernji.hr/vijesti/mup-poziva-na-aktivaciju-e-osobne-objavili-i-video-upute-1298046

KORIŠTENJE DIGITALNOG POTPISA

PAMETNE KARTICE

Pametna kartica ima MCU opremljen algoritmom za potpisivanje i obično nepristupačan, privatni ključ pohranjen u memoriji. Dokument Hash šalje se na pametnu karticu radi potpisivanja i vraća se digitalni potpis. Javni ključ poznat je svima i može se potvrditi autentičnost.

Pametne kartice također su zaštićene PINOM. Moguće ih je slobodno koristiti i u slučaju gubitka ili krađe, brzo se otkriju.

Nedostatak: stroj za digitalno potpisivanje mora imati instaliran čitač pametnih kartica i dodatni softver. Čitač i pametna kartica zahtijevaju zasebne upravljačke programe.

Brojni su proizvođači pametnih kartica i mnogi od njih koriste nestandardizirane protokole za komunikaciju sa svojim karticama.

Stoga se mora dodatno instalirati upravljački program za svaki model kartice koji se koristi u sustavu potpisivanja, osim ako kartica koristi široko podržani komunikacijski protokol.

ČITAČI PAMETNIH KARTICA

Neki od proizvođača čitača pametnih kartica su:

HID Global

Identiv

IOGEAR

Gemalto

Rocketek

Dell

Slika 16. Prikazuje IOGEAR čitat smart card-a

Izvor: Google search: IOGEAR smart card reader

Najčešći tip povezivanja čitača pametnih kartica je USB.

Gotovo svi noviji USB čitači pametnih kartica slijede CCID specifikaciju, ali ne naravno svi. Moderni OS imaju podršku za CCID čitače pametnih kartica.

Čitači koji nisu u skladu s CCID-om dolaze sa svojim upravljačkim programima, ali može se dogoditi da proizvođač podržava samo jedan OS, obično MS Windows.

Ovdje treba napomenuti da čitači pametnih kartica s ugrađenom tipkovnicom pružaju bolju sigurnost prilikom čitanja pametnih kartica s PIN-om. Na ovaj način moguće key-logger napad na računalo pomoću čitača neće moći dobiti uneseni PIN.

USB STICKOVI

USB stickovi mogu se koristiti na sličan način kao i pametne kartice.

To mogu biti posebni uređaji koji izvršavaju iste funkcije kao i pametne kartice (zvani i USB tokeni) ili mogu biti uobičajeni uređaji za masovnu pohranu zaključani u načinu samo za čitanje koji sadrže digitalno potpisane izvršne datoteke koje izvršavaju istu funkciju kao pametne kartice, tj. Potpisuju hasheve.

Sigurnost također potvrđuje serijski broj uređaja. Međutim, sve nespecijalizirane USB stickove može lako kopirati.

Većina USB-a koji nisu sigurni za provjeru autentičnosti su uređaji za masovnu pohranu koji sadrže samo privatni ključ.

Najsigurniji su specijalizirani diskovi izrađeni isključivo za digitalno potpisivanje, tj. USB tokeni.

USB stickovi su praktični jer su jeftini i mogu se povezati s većinom uređaja bez potrebe za dodatnim posebnim hardverom. Za specijalizirane USB stickove potreban je dodatni softver.

O USB stickovima za digitalno potpisivanje možemo razmišljati kao o pametnim karticama koje koriste svoj čitač.

Doista, neki USB tokeni u potpunosti oponašaju protokole pametnih kartica, a ponekad su opremljeni istim firmwareom,[1] a između njih nema praktične razlike. Postoje čak i USB tokeni koji sadrže SIM pametne kartice koje pružaju samo USB sučelje za SIM koje se zatim koristi za provjeru autentičnosti i / ili digitalno potpisivanje.

[1] trajni softver programiran u memoriju samo za čitanje.

Pametne kartice i USB stickovi mogu se lako ukrasti, ali njihova se krađa obično brzo otkrije, pa se privatni ključevi koje oni mogu poništiti i spriječiti zlouporaba. [5]

Slika 17. Prikazuje USB stickove – USB tokene

Izvor: Google search: usb stick digital signature

BIOMETRIJSKI OTISCI PRSTIJU

Biometrija je znanost o stvaranju digitalnih identifikatora na temelju jedinstvenih mjerljivih bioloških karakteristika pojedinog čovjeka.
Koristimo npr. biometrijski podaci o otisku prsta osobe kako bi se generirao ključ koji se zatim koristi u standardnim postupcima digitalnog potpisivanja.

Nevolja je u tome što otisak osobe ne daje potpuno isti rezultat svaki put kad se mjeri. To je uzrokovano promjenama na ljudskoj koži, ozljedama, vlažnim ili mokrim rukama i uglavnom nesavršenostima senzora za očitavanje otiska prsta.
Biometrijski otisci prstiju dobivaju se u obliku matrice, tj. 2D crno-bijele bit mape.

Da bi se izbjegao gore spomenuti problem, u odabiru ključeva koriste se samo odabrani pikseli. Ali ovo još uvijek može biti neispravno.
U idealnim bismo okolnostima koristili prst osobe kao uređaj za pohranu koji sadrži informacije potrebne za generiranje privatnog ključa koji se koristi za digitalno potpisivanje, a potpisivanje / provjera autentičnosti izvodila bi se svaki put izravno iz dobivenih podataka. Ali ne možemo jamčiti da se generirani ključ neće mijenjati s vremena na vrijeme zbog promjena u otiscima prstiju.

Uobičajena metoda razvijena za izbjegavanje ovog problema je slanje skeniranog otiska prsta na poslužitelj koji vrši provjeru autentičnosti i vraća privatni ključ za identificiranu osobu. Pohranjeni privatni ključ prethodno je generiran iz biometrijskih podataka o otiscima prstiju te osobe.

To uvodi svoje probleme. Prvo od njih je pouzdanje poslužitelja koji čuva sve privatne ključeve. Ako je poslužitelj ugrožen, biometrijski otisci prstiju gube smisao u sigurnosti.
Ali i ova metoda rješava neke probleme i uvodi neke prednosti.

Slika 18. Prikazuje biometrijski otisak prsta

Izvor: Google search: biometric finger scanner

Biometrijski otisci prstiju korisni su jer nema potrebe za pohranjivanjem privatnih ključeva na vanjskim hardverskim uređajima koji se nose uokolo. Ne mogu se lako ukrasti i / ili lažirati, a sasvim sigurno ih se ne može slučajno izgubiti.

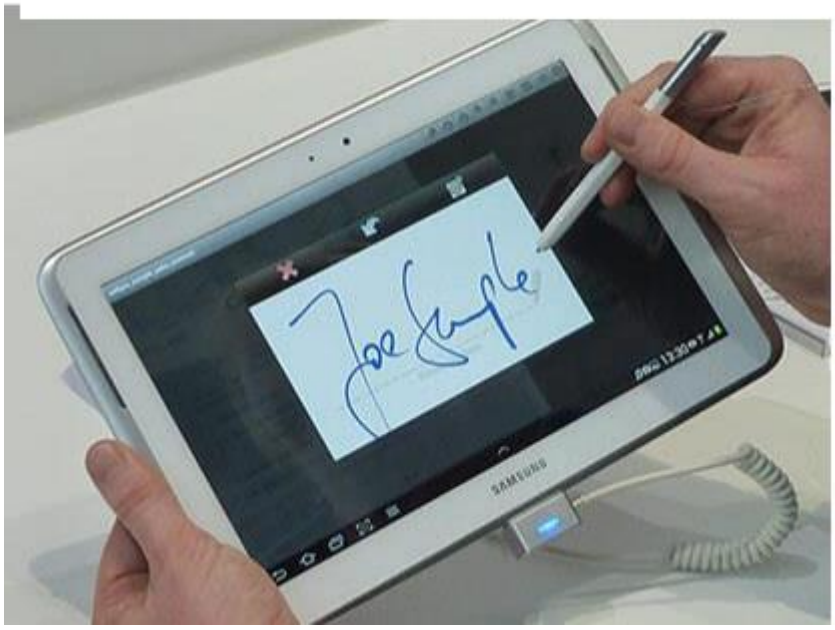
Postoje etički nedostaci upotrebe otisaka prstiju za autentifikaciju i / ili digitalno potpisivanje.
Ljudi koji nemaju prste ili se rađaju s adermatoglifijom (genetski poremećaj ljudi rođenih bez otisaka prstiju) ili nekim sličnim stanjem bili bi diskriminirani u takvom sustavu.
Naravno, to je lako rješivo pružanjem alternativne metode biometrijske identifikacije kao što je prepoznavanje lica.[7]

UREĐAJ ZA DIGITALNI POTPIS

(Signature pad)

Uređaj za elektronični / digitalni potpis je specijalizirani hardver koji se koristi za hvatanje vlastitog potpisa osobe. Takvi uhvaćeni biometrijski podaci tada se mogu koristiti za stvaranje privatnog ključa i izravnu provjeru autentičnosti. U dokumente se ponekad dodaju samo grafički podaci, ali često se generirani privatni ključ koristi zajedno za digitalno potpisivanje.
Biometrijski potpis pati od svih nedostataka jer biometrijski otisci prstiju plus neki od vlastitih tj. podaci se uzimaju iz vlastitog potpisa osobe koji može oponašati druga osoba. Potpise snimljene uređajem za potpis malo je teže krivotvoriti, jer je uključeno malo više podataka.
Npr. uređaj za potpis također može zabilježiti određene detalje potpisa, poput toga koliko je snažno pritisnuta olovka, kut prema površini uređaja i brzina pisanja.

Slika 19. Digitalni potpis na uređaju



Izvor: Google search: digital signature on pad

Uređaji za potpis su praktični jer su ljudi navikli potpisivati papirnate dokumente i ova je metoda vrlo slična njima.
Dakle, vrlo je malo toga što morate objasniti potpisnicima dokumenata i oni imaju fizičko iskustvo s potpisom dokumenta.

Nedostatak uređaja za potpis je taj što nude malo veću zaštitu, ali potreban je specijalizirani hardver i softver koji nije jeftin kao što su, na primjer, čitači pametnih kartica.

Kao i kod otisaka prstiju i većine biometrijskih podataka koji se koriste za provjeru autentičnosti, autentifikacija vlastitog potpisa često uključuje rukopis na strani poslužitelja i prepoznavanje potpisa.

POTENCIJALNI NAPADI NA DIGITALNI POTPIS

MJERENJEM VREMENA

Prilikom izrade digitalnog potpisa vrijeme je uvijek različito za određene poruke. Za to su nam zadužene su različite optimizacije performansi, kako bi došlo do uklanjanja nepotrebnih operacija, granjanja i ispitivanja uvjeta, različita stanja RAM priručne memorije te procesorske instrukcije s različitim vremenom izvođenja.

Mjerenjem vremena potrebnog za stvaranje digitalnog potpisa, osoba koja napada može doći u posjed korisnikovog tajnog ključa. Ovaj napad primjenjuje se na Diffie-Hellman, RSA, DSS i druge DS algoritme.

Naime, ako se koriste javno dostupne informacije i informacija koje je moguće i prisluškivati, na taj način napadač mjerenjem vremena potrebnog za potpisivanja većeg broja poruka pomoću jednog tajnog ključa može otkriti njegovu vrijednost, bit po bit.

Postoji naravno i iznimka, koja kaže da napad mjerenjem vremena nije primjenjiv ako se za potpisivanje svake poruke koristi drugačiji tajni ključ. Znači radi sigurnosti potrebno je mijenjati tajni ključ.

Bilježenjem vremena primitka poruke na napadnutom sustavu i vremena odgovora na spomenutu poruku može se provesti način mjerenja vremena potpisivanja. Napad se u većini slučajeva može opisati kao problem uočavanja signala. „Signal“ se sastoji od vremenskih varijacija uzrokovanih bitom privatnog ključa kojega se pokušava otkriti i „šuma“ koji se sastoji od netočnosti mjerenja vremena i vremenskih varijacija uzrokovanih ostalim nepoznatim bitovima privatnog ključa. Uz j poruka yo, y1, …, yj-1 s

$$P(x_b) \propto \prod_{i=0}^{j-1} F\left(T_i - t(y_i, x_b)\right)$$

odgovarajućim vremenskim mjerenjima To, T1, …, Tj-1, vjerojatnost pogađanja xb prvih b bitova privatnog ključa proporcionalna je:

gdje je t(yi , xb) vrijeme potrebno za prvih b iteracija proračuna digitalnog potpisa pomoću privatnog ključa xb, a F je pretpostavljena funkcija raspodjele vjerojatnosti T – t(y, xb) za sve vrijednosti y i za ispravan xb. Ako je xb-1 ispravno određen moguće su dvije vrijednosti bita xb. Vjerojatnost da je xb točna vrijednost, a xb' netočna je:

$$\frac{\prod_{i=0}^{j-1} F\left(T_i - t\left(y_i, x_b\right)\right)}{\prod_{i=0}^{j-1} F\left(T_i - t\left(y_i, x_b\right)\right) + \prod_{i=0}^{j-1} F\left(T_i - t\left(y_i, x_b'\right)\right)}.$$

Način sprječavanja napada je maskiranje trajanja postupka potpisivanja tako da ono bude jednako za sve poruke. Proces izgradnje algoritma koji traje jednako dugo neovisno o ulaznim parametrima i platformi na kojoj se izvodi vrlo je komplicirano zbog prevoditeljskih optimizacija, stanja RAM priručne memorije, vremena izvođenja instrukcija i drugih čimbenika koji unose nepredvidljive vremenske varijacije. Ako se za produživanje trajanja postupka potpisivanja do postavljene vrijednosti koristi kašnjenje, karakteristike kao što su potrošnja energije ili zauzetost procesorskih resursa od strane pojedinih procesa mogu otkriti stvarno trajanje potpisivanja. Zbog toga je najbolji način sprječavanja napada promjenama tehnika slijepih potpisa maskirati i napadaču nedostupnim učiniti poruku koja ulazi u postupak potpisivanja.[1]

MASKIRANJE PORUKE RSA

Unutar pojedinih implementacija RSA algoritma, koje koriste algoritam za maskiranje poruke (eng. padding) prema RSASSA-PKCS1-v1_5 specifikaciji, otkriven je sigurnosni propust koji omogućuje krivotvorenje. Hash vrijednost poruke M se prije potpisivanja maskira kako bi se otežala analiza potpisa, a time i njegovo krivotvorenje:

00 01 FF FF … FF 00 || ASN.1 || H(M)

gdje je 00 01 FF FF … FF 00 znakovni niz korišten za maskiranje, ASN.1 je duljina hash vrijednosti i druge informacije o korištenoj hash funkciji, a H(M) je hash vrijednost poruke. Nakon primitka potpisane poruke digitalni potpis se dekriptira korištenjem javnog eksponenta (npr. e = 3). Time se dobiva maskirana poruka opisane strukture, iz koje se izdvaja H(M) i uspoređuje s hash vrijednosti poruke na koju se potpis odnosi. Propust se javlja u postupku izdvajanja H(M) iz dekriptiranog potpisa zbog toga što neke implementacije ne provjeravaju jesu li potpisu naknadno dodani podaci. U slučaju korištenja PKCS1- v1_5, kao hash vrijednosti se izdvaja sve što se nalazi iza znakovnog niza korištenog za maskiranje i ASN.1 vrijednosti. Za bilo koju poruku M' s hash vrijednošću H(M') lako je pronaći treći korijen znakovnog niza oblika:

00 01 FF FF … FF 00 || ASN.1 || H(M’) || smeće

gdje je broj ponavljanja niza FF unutar znakovnog niza za maskiranje smanjen, a smeće je znakovni niz takav da je cjelokupna izmijenjena maskirana poruka predstavlja treću potenciju nekog broja. Napad je opisan u slučaju korištenja javnog eksponenta e = 3, ali ga je moguće izvesti za bilo koju malenu vrijednost eksponenta e za koju je lako pronaći e-ti korijen znakovnog niza, kao u primjeru. Napad je moguće spriječiti korištenjem javnog eksponenta većeg iznosa i uvođenjem dodatne provjere u postupku izdvajanja hash vrijednosti iz potpisa.[1]

ZAKLJUČAK

U današnje vrijeme nezamislivo je da neki posao funkcionira bez određene vrste računala i interneta. Iz toga razloga nam je od velike važnosti i očuvanje autentičnosti i sigurnosti naših dokumenata / poruka te privatnost prije svega. Digitalni potpis nam u tome pomaže. Osim brzine i olakšavanja mnogih 'papirnatih' procedura koje i u današnje vrijeme nažalost još nismo izbacili, barem što se tiče Hrvatske. U banci ikako svi potpisujemo dokumente na uređaju za elektronski potpis, no na kraju obavljene usluge većinom svi dobijemo kuvertu papira.

Digitalni potpis nam osigurava i sigurnu upotrebu. Naravno, dolazi i do raznih napada i zlouporabe potpisa, no zbog toga nam služe sigurnosni mehanizmi kao i algoritmi koji to sprječavaju.

Mnogi govore kako je i pitanje kada će se i prestat koristit rukom pisani potpis, što će donijeti još više pozitivnih stvari.

LITERATURA

Internetske stranice:

[1] Microsoft Word – CCERT – PUBDOC – 2006 – 12 – 178.DOC, https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2007-02-182.pdf, lipanj 2020.

[2] Ca Fina Root Certifikati – Fina, https://www.fina.hr/ca-fina-root-certifikati, rujan 2020.

[3] Sustav certificiranja Zagrebačke banke – Zagrebačka banka, https://www.zaba.hr/home/o-nama/sustav-certificiranja-zagrebacke-banke, rujan 2020.

[4] Security token, https://en.wikipedia.org/wiki/Security_token, rujan 2020.

[5] Biometrija i otisci prstiju, https://www.mercury-processing.com/hr/blog/biometrija-sigurnost-na-vrscima-prstiju/, rujan 2020.

[6] Stručni članak: Želimir Radmilović: Biometrijska identifikacija, https://hrcak.srce.hr/, rujan 2020.

[7] eOI, https://www.eid.hr/hr/content/koja-je-razlika-izmedu-osobne-iskaznice-i-elektronicke-osobne-iskaznice-eoi, prosinac 2020.

Knjige:

[1] Računalne mreže 2: Mario Radovan, prosinac 2020.

[2] Computer Networks_A Systems Approach, 3rd Edition-Peterson.pdf(Peterson, L. Larry; Davie, S. Bruce: Computer Networks: A System Approach, Morgan Kaufmann, CA: San Francisco, 2011.) https://doc.lagout.org/network/Computer%20Networks_%20A%20Systems%20Approach%2C%203rd%20Edition-Petersen.pdf, kolovoz 2020.

PRILOZI