SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Tehnologije za dugotrajno očuvanje digitalno potpisanih arhivskih zapisa

DIPLOMSKI RAD

Studentica: Magdalena Kuleš
Mentori: red. prof. dr. sc. Hrvoje Stančić
dr. sc. Ivan Dunđer

Zagreb, rujan 2018.

UNIVERSITY OF ZAGREB
FACULTY OF HUMANITIES AND SOCIAL SCIENCES
DEPARTMENT OF INFORMATION AND COMMUNICATION SCIENCES

Technologies for long-term preservation of digitally signed archival records

DIPLOMA THESIS

Student: Magdalena Kuleš
Supervisors: PhD Hrvoje Stančić, full professor
PhD Ivan Dunđer

Zagreb, September 2018.

Sadržaj

1. Uvod ... 3
2. Koncept dugotrajnog očuvanja ... 4
3. Koncept digitalnog zapisa ... 6
3.1. Digitalno potpisani zapis ... 8
4. Elektronički potpis ... 10
4.1. Elektronički potpis kao dio kriptografije ... 11
4.1.1. Osnovne vrste šifriranja ... 16
4.1.1.1. Simetrična kriptografija ... 17
4.1.1.2. Asimetrična kriptografija ... 19
4.1.2. Hash funkcije ... 22
4.1.3. PGP-primjer hibridnog kriptosustava ... 28
4.1.4. Kriptografski algoritmi ... 30
4.1.4.1. Simetrični ... 31
4.1.4.2. Asimetrični ... 32
4.1.5. Kriptografske hash funkcije ... 33
4.1.6. Algoritmi za generiranje elektroničkog potpisa ... 34
4.1.7. Upravljanje ključevima ... 34
4.1.8. Generiranje, verifikacija i validacija elektroničkog potpisa ... 37
5. Upravljanje elektroničkim potpisom ... 41
5.1. PKI- infrastruktura javnog ključa ... 41
5.2. Digitalni certifikat ... 46
5.2.1. Metode povlačenja digitalnih certifikata: CRL i OCSP ... 48
6. Istraživanje – analiza Fina okruženja ... 52
6.1. Analiza usluge certificiranja u Fini ... 52
7. Izazov dugotrajnog očuvanja digitalno potpisanih zapisa ... 65
7.1. Napredni elektronički potpis ... 66
7.2. Pravno i normativno okruženje vezano uz elektroničke potpise ... 70
7.3. Postojeći pristupi dugotrajnom arhiviranju i očuvanju digitalno potpisanih zapisa ... 72
8. Blockchain tehnologija kao novi pristup dugotrajnom očuvanju digitalno potpisanih zapisa ... 78
8.1. TrustChain model ... 83
9. Zaključak ... 89
Literatura ... 90
Popis slika ... 95
Popis tablica ... 95

1. Uvod

Svrha knjižnica, arhiva i sličnih institucija je očuvanje dokumenata koji će zadržati određenu vrijednost, a buduće generacije će im moći s lakoćom pristupiti. S vremenom su se digitalni mediji pokazali kao rješenje za arhivsku pohranu. Međutim, pojavila su se i brojna pitanja koja upućuju na probleme koji se mogu pojaviti u tom procesu dugotrajnog očuvanja. Jedan od problema je dugotrajno očuvanje digitalnih zapisa koji imaju pridružene digitalne potpise/certifikate/pečate/vremenske žigove. Zapravo je srž problema u očuvanju valjanosti digitalnih potpisa i mogućnosti provjere valjanosti dugo nakon nastanka elektroničkog potpisa. U ovom radu bit će pojašnjen koncept dugotrajnog očuvanja digitalnog zapisa. Važno je pojasniti i koncept digitalnog potpisa i kriptografije kao okruženja u kojem je elektronički potpis nastao te kao infrastrukture koja se primjenjuje u procesu digitalnog potpisivanja. Istraživanje provedeno za potrebe ovog rada obuhvaća analizu usluge certificiranja koju pruža Fina kao prvi davatelj takve usluge u Republici Hrvatskoj. Fina primjenjuje PKI infrastrukturu (engl. *Public Key Infrastructure*) javnog ključa koja će također biti pojašnjena. Zasad postoje određeni pristupi i rješenja koja se primjenjuju u očuvanju digitalnih zapisa koji imaju pridružene digitalne potpise, a također postoji i zakonska regulativa. U sklopu ovog rada bit će analizirana i tehnologija ulančanih blokova (eng. *blockchain*) kao moguća tehnologija koja bi se mogla primijeniti u dugotrajnom očuvanju digitalno potpisanih zapisa, a bit će predstavljen i TrustChain model koji je razvijen upravo u svrhu dugotrajnog očuvanja, a temelji se na navedenoj tehnologiji.

2. Koncept dugotrajnog očuvanja

Pojavila su se brojna pitanja koja upućuju na probleme koji se mogu pojaviti u procesu dugotrajnog očuvanja. Dugotrajno očuvanje (engl. *Long-Term preservation*) je koncept koji ima tri glavne zadaće: očuvati dokument, osigurati njegovu dostupnost i zadržati njegovu razumljivost i izvorno značenje. Pohrana i čuvanje dokumenata su zapravo temeljne zadaće koje bi svaki digitalni repozitorij trebao ispuniti, dok se dostupnost odnosi na mogućnost pronalaska i pristupa sadržaju dokumenta u repozitoriju. Problem dugotrajnog očuvanja je relativno jednostavno riješiti ako se radi o razdoblju od desetak godina, ali razdoblje od trideset i više godina zahtijeva poduzimanje niza koraka u svrhu efikasnog očuvanja dokumenata. Postoji nekoliko ključnih komponenti koje predstavljaju rizik i stoga zahtijevaju konstantno ulaganje i održavanje. Riječ je o hardveru, softveru, formatu i gubitku izvornog značenja sadržaja dokumenta. U dugotrajnom očuvanju digitalnih dokumenata jako važnu ulogu imaju i metapodaci, tj. podaci o podacima. Metapodaci predstavljaju sve one informacije koje su potrebne kako bi se određeni dokument opisao. Određeni dokument i njemu pridruženi metapodaci su čvrsto povezani, jer upravo metapodaci omogućuju što lakši pronalazak i razumijevanje dokumenta.

Postoji nekoliko tehničkih pristupa koji se primjenjuju u dugotrajnom očuvanju. Osim tehničkih pristupa, potrebno je uzeti u obzir i pitanje standardnih formata te zakonski i društveni aspekt dugotrajnog očuvanja. Tehnički pristupi dijele se u dvije kategorije. Prvu kategoriju čine oni pristupi kojima je zadaća očuvati izvorno stanje dokumenta uz pomoć sustava koji su sposobni pročitati i prikazati dokument u izvornom formatu, dok drugoj kategoriji pripadaju pristupi koji su zaduženi za kontinuiranu transformaciju digitalnih dokumenata u formate novih verzija sustava za prikaz dokumenata, ali tako da dokument ipak zadrži izvorni izgled i značenje. Najpoznatiji pristupi su migracija (engl. *migration*) i emulacija (engl. *emulation*). „Emulacija je postupak koji obuhvaća ponovno programsko stvaranje prvotne računalno-programske radne okoline zapisa i programa na suvremenim računalima radi omogućavanja njihova izvornog načina djelovanja“ [1] . „Migracija je prebacivanje dokumenta ili zapisa s jednoga medija za pohranu, aplikacije, sustava i/ili tehnološkoga konteksta zapisa u drugi, osobito iz zastarjeloga u suvremeni, čuvajući njegovu autentičnost, pouzdanost, cjelovitost i iskoristivost“[2]. U procesu emulacije tzv. emulatori su se najprije koristili u razvoju novog hardvera. Kroz emulaciju softver je taj koji simulira razne

[1] Multilingual Archival Terminology. Emulacija. URL: http://www.ciscra.org/mat/mat/term/4549. (23.09.2018.).
[2] Multilingual Archival Terminology. Migracija. URL: http://www.ciscra.org/mat/mat/term/4622/6029. (23.09.2018.).

komponente hardvera što ujedno omogućava i testiranje prije same ugradnje novog hardvera. Godine 1999. Rothenberg je predložio primjenu emulacije u svrhu dugotrajnog očuvanja.[3] Kada je riječ o zakonskim i društvenim aspektima, ključno je prije ulaska dokumenta u arhiv riješiti pitanje autorskog prava. Knjižnice i arhivi imaju i kriterije koje primjenjuju prilikom odabira dokumenata koji su vrijedni čuvanja. U procesu dugotrajnog očuvanja troškovi su svakako ograničavajući faktor, stoga je potrebno odrediti koja su to tijela zakonski i financijski odgovorna za dugotrajno očuvanje. Kroz naredno poglavlje definirat će se što je uopće digitalni zapis i zašto dugotrajno očuvanje digitalnih zapisa predstavlja izazov.

[3] Borghoff, Uwe: Rodig, Peter; Scheffczyk, Jan; Schmitz, Lothar. Long-Term preservation of Digital Documents: Principles and Practices.USA: International Computer Science Institute, 2012., str. 16.

3. Koncept digitalnog zapisa

Danas postoje dva osnovna načina nastajanja digitalnih dokumenata. Digitalni dokumenti mogu nastati digitalizacijom postojećih dokumenata u papirnatom obliku, a s druge strane javljaju se dokumenti izvorno nastali u digitalnom obliku (engl. *born digital*). Digitalizacija (engl. *digitisation*) u najširem smislu predstavlja prevođenje analognog signala u digitalni oblik, a u užem smislu predstavlja pretvorbu različitih vrsta gradiva u digitalni oblik, tj. binaran kôd zapisan kao računalna datoteka.[4] Digitalizacijom se pojam očuvanja počinje dijeliti na dva dijela – očuvanje informacijskog sadržaja, tj. informacije koju određeni dokument nosi, te očuvanje fizičkog objekta, medija, kao nositelja informacije. Informacijski sadržaj se digitalizira i sprema odvojeno od objekta nositelja.[5] Važno je napomenuti kako zapis u elektroničkoj inačici nije niti samo dokument niti samo objekt, ne ovisi o mediju na kojem se nalazi te nije fizički zapisan u računalnom sustavu u logičkom slijedu, nego je fragmentiran i može se nalaziti i na fizički različitim jedinicama. Zapis je zapravo ono što je stvoreno i sačuvano kao dokaz funkcija, aktivnosti i transakcija neke tvrtke ili pojedinca. Kako bi se smatrao dokazom, mora imati sadržaj, strukturu i kontekst, te biti dio sustava za arhiviranje. U informacijskoj tehnologiji zapis se definira kao grupa povezanih podataka, riječi ili polja koja se tretiraju kao jedna cjelina (npr. ime i prezime, adresa i broj telefona). Zatim kao skup jedne ili više povezanih jedinica podataka grupiranih u svrhu obrade.[6]

S obzirom na sve veću količinu dokumenata nastalih izvorno u digitalnom obliku te one dokumente koji su digitalizirani, konstantno je prisutna problematika njihova arhiviranja i dugotrajnog očuvanja. Iznova se postavljaju pitanja kako riješiti sve probleme, izazove i zahtjeve, koje tehnologije primijeniti, na koje standarde i norme se oslanjati kako bi proces arhiviranja i dugotrajnog očuvanja bio što kvalitetniji. Potrebno je naglasiti kako bi svaki digitalni zapis morao prilikom arhiviranja i dugotrajnog očuvanja ostati vjerodostojan, autentičan, potpun te bi trebao sačuvati dovoljno konteksta. Vjerodostojan je onaj zapis koji dolazi iz pouzdanog izvora. Potpun je onaj kojem je pridruženo vrijeme i mjesto nastajanja, pojedinosti o korisniku, naslov, predmet te sadržaj. Autentičan zapis ima očuvanu povijest nastanka, prijenosa, korištenja i očuvanja kroz vrijeme, dok se kontekst odnosi na međusobne

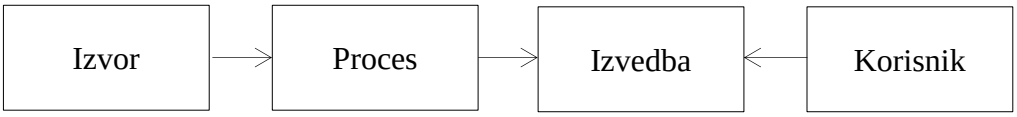
[4] Hrvatska enciklopedija, s.v. digitalizacija. URL: http://www.enciklopedija.hr/natuknica.aspx?id=68025. (23.09.2018.).
[5] Stančić, Hrvoje.Digitalizacija građe, 2. i 3. seminar Arhivi, knjižnice, muzeji. Mogućnosti suradnje u okruženju globalne informacijske infrastrukture, Zagreb, 2000., str. 64.
[6] IBM Terminology, s.v. record. URL: https://www-01.ibm.com/software/globalization/terminology/r.html. (23.09.2018.).

veze pojedinih zapisa te okolinu u kojoj je zapis stvoren.[7] Arhiviranje i očuvanje predstavljaju jedinstveni izazov upravo zbog termina "dugotrajno" (engl. *long-term*). Pitanje je kako dugotrajno očuvati i održati digitalne informacije, gdje dugotrajno može značiti samo toliko dugo da se ne treba brinuti o zastarijevanju tehnologije, ali isto tako može značiti očuvanje desetljećima, stoljećima ili trajno. Digitalni objekti zahtijevaju neprestano i trajno održavanje te ovise o razrađenim sustavima hardvera, softvera, normi, modela i zakonske regulative koji se konstantno nadopunjavaju ili zamjenjuju novima.

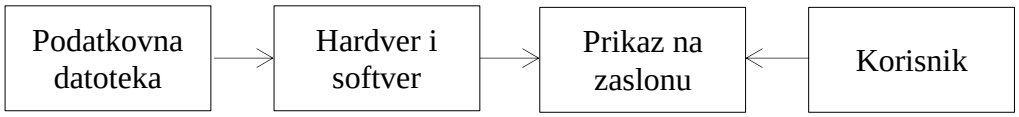
Potrebno je pojasniti kako je priroda digitalnih zapisa posve drugačija od dokumenata u papirnatom obliku. Za arhiviste, problem očuvanja zapisa usredotočen je na objekt, pa ukoliko je objekt očuvan, očuvan je i zapis na njemu. Glavna razlika je u tome što su digitalni zapisi ovisni o tehnologiji i da bi ih se moglo koristiti potrebno je imati odgovarajuću kombinaciju hardvera i softvera. Digitalni zapisi tako prestaju biti fizički objekti te postaju rezultat posredovanja tehnologije i podataka. Iskustvo objekta traje sve dok su tehnologija i podaci u interakciji. Kao rezultat toga, dvije osobe mogu u isto vrijeme pristupiti istom zapisu i iskusit će jednaku "izvedbu" tog zapisa. Model izvedbe "razbija" koncept digitalnog zapisa na nekoliko komponenti što zapravo pomaže boljem razumijevanju prirode digitalnog zapisa. *Izvor* zapisa je fiksna poruka koja je u interakciji s tehnologijom. Ona osigurava jedinstveno značenje zapisa. Međutim sama po sebi nema smisla, nego ju je potrebno kombinirati s tehnologijom kako bi se postigla željena svrha njezina stvaratelja. *Proces* je tehnologija koja je potrebna kako bi se prikazalo značenje iz izvora zapisa. Kombinacijom izvora i procesa dolazi do *izvedbe* koja dostavlja značenje zapisa korisniku. Završetkom interakcije izvora i procesa, završava i izvedba. Izvor digitalnog zapisa je podatkovna datoteka koja ima definiranu strukturu, a koja ovisi o formatu (npr. Microsoft Word dokument, Adobe Actrobat datoteka). Proces je specifična kombinacija hardvera i softvera i konfiguracije potrebne za razumijevanje formata datoteke izvora, dok je izvedba ono što je zapravo prikazano korisniku na zaslonu ili nekom drugom izlaznom uređaju.[8] Na slikama 1 i 2 prikazan je prethodno opisani model.

[7] Stančić, Hrvoje. Arhiviranje digitalnih dokumenata, 4. seminar Arhivi, knjižnice i muzeji. Mogućnosti suradnje u okruženju globalne informacijske infrastrukture. Zagreb, 2001., str. 210 - 211.

[8] Heslop, Helen; Davis, Simon; Wilson, Andrew. An Approach to to the Preservation of Digital Records, National Archives of Australia, 2002., str. 8-9, URL: http://www.imaginar.org/taller/dppd/DPPD/40%20pp%20Approach.pdf. (13.03.2018.).



Slika 1. Model izvedbe: izvor i proces komponente



Slika 2. Model izvedbe: digitalni zapis

Digitalno gradivo je, za razliku od analognog, izloženo znatno većem riziku od propadanja, a razlog tome su ponajviše brzi ciklusi razvoja u području informacijskih tehnologija. Očuvanje digitalnoga gradiva ne svodi se samo na očuvanje datoteka, nego je cilj i omogućiti pristup sadržaju te osigurati očuvanje ili repliciranje infrastrukture koja osigurava prikaz datoteka korisniku. Houghton [9] navodi nekoliko glavnih izazova u području očuvanja digitalnih dokumenata. Kao prvi izazov ističe velike količine podataka s kojima se softveri za očuvanje te sustavi za pohranu možda ne mogu nositi, što zahtijeva novu infrastrukturu i softver. Drugi izazov su višestruke kopije izvorno digitalnoga gradiva, zatim hardver koji je podložan zastarijevanju. Izazov je i softver, tj. njegove nove verzije. Često datoteke neće biti ispravno prikazane na novim verzijama softvera dok datoteke koje stvore novije inačice nekog softvera u pravilu neće biti uopće moguće pročitati starijim verzijama tog softvera. Osim ovih, kao izazove izdvaja i formate datoteka koje se s vremenom prestaje koristiti, metapodatke koji predstavljaju jedan od najvažnijih aspekta digitalnog očuvanja, pravna pitanja, privatnost i potrebne financijske resurse.

3.1. Digitalno potpisani zapis

Digitalna komunikacija danas predstavlja standardni način komunikacije, a e-poslovanje je način poslovanja koji se sve više primjenjuje. E-poslovanje predstavlja jednostavan način komuniciranja između poslovnih partnera, stoga je takvo poslovanje postalo iznimno važan, siguran i nezamjenjiv način komunikacije. Rezultat takvog načina komunikacije je nastajanje sve većeg broja digitalnih dokumenata, tj. digitalnih zapisa koji imaju pridodane elektroničke

[9] Houghton, Bernadette. Preservation Challenges in the Digital Age, D-Lib Magazine, 22(7/8), srpanj/kolovoz 2016. URL:http://www.dlib.org/dlib/july16/houghton/07houghton.html. (13.03.2018).

potpise ili elektroničke pečate. Stoga je potrebno analizirati problematiku dugotrajnog očuvanja takvih digitalnih zapisa. Oni također moraju zadržati svoje temeljne karakteristike, a to su autentičnost, integritet, pouzdanost i upotrebljivost, što zahtijeva složeniji pristup očuvanju nego kad je riječ o digitalnim zapisima koji nisu digitalno potpisani ili digitalno ovjereni. Kao što postoji razlika u kratkotrajnom ili dugotrajnom očuvanju digitalnih zapisa u odnosu na dokumente u analognom obliku, isto tako postoji i razlika u očuvanju digitalno potpisanih ili ovjerenih zapisa u odnosu na digitalne zapise bez elektroničkog potpisa ili pečata. Digitalno potpisanim ili ovjerenim zapisima dodana je još jedna razina složenosti, tj. eletronički potpis, zbog čega je njihovo očuvanje složenije.

Iako se digitalno potpisani zapisi mogu dobro očuvati kroz duže vremensko razdoblje, oni mogu izgubiti pravnu valjanost ako elektronički potpis ne može biti potvrđen ili ako je izgubio svojstvo neporecivosti (engl. *non-repudiation*). Ako se prilikom provjere valjanosti elektroničkog potpisa pojavi greška, pouzdanost tog istog digitalnog zapisa je ugrožena. Problem je u tome što elektronički potpis, tj. potpisni certifikat na kojem se temelji, ima određeni vijek trajanja te provjera njegove valjanosti zahtijeva povezanost s certifikacijskom službom (engl. *Certification Authority, CA*) koja se oslanja na infrastrukturu javnog ključa (engl. *Public Key Infrastructure, PKI*). Ako neki od elemenata ne funkcionira kako bi trebao, provjera valjanosti također neće biti uspješna. Ovo je posebno važno kod očuvanja onih zapisa koji imaju pridodane napredne elektroničke potpise.[10]

[10] Herceg, Boris; Brzica, Hrvoje; Stančić, Hrvoje. Digitally Signed Records – Friend or Foe?, u: Anderson, Karen; Duranti, Luciana; Jaworski, Rafał; Stančić, Hrvoje; Seljan, Sanja; Mateljan, Vladimir (ur.), e-Institutions - Openness, Accessibility, and Preservation. Zagreb: Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, Croatia, 2015., str. 148.

4. Elektronički potpis

U poslovnom i ICT svijetu sve je češći pojam elektronički potpis, elektronički potpis ili *e-signature* koji značajno ubrzava i pojednostavljuje poslovanje uz uštedu vremena. Prije svega, potrebno je definirati pojam elektroničkog potpisa.

- Elektronički potpis odnosi se na podatke u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje.
- Napredan elektronički potpis znači potpis koji je na nedvojben način povezan s potpisnikom; omogućava identificiranje potpisnika; izrađen je korištenjem podataka za izradu elektroničkog potpisa koji potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom; povezan je s njime potpisnim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.
- Kvalificirani elektronički potpis znači napredan potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.[11]

Prema Hrvatskom enciklopedijskom rječniku[12] elektronički potpis je „šifriranje kojim se dokazuje autorstvo, tj. izvor elektroničkog dokumenta“.

Uz pojam elektroničkog potpisa važno je pobliže objasniti i pojmove elektroničkog pečata, elektroničkog certifikata i elektroničkog vremenskog žiga. Elektronički pečat Uredbom eIDAS postaje ključni način za potvrđivanje cjelovitosti i izvornosti dokumenata kod pravnih osoba, dok se digitalni certifikati primjenjuju u PKI infrastrukturi, tj. kod zahtjevnijih implementacija javnim ključem i stoga će kasnije biti detaljnije pojašnjeni. Uloga elektroničkog vremenskog žiga je potvrda postojanja podataka u određeno vrijeme.

[11] Uredba eIDAS, čl. 3., 2014., str. 84. URL. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014R0910&from=HR. (23.09.2018.).

[12] Anić, Vladimir; Rončević Brozović, Dunja; Goldstein, Ivo; Goldstein, Slavko; Jojić, Ljiljana; Matasović, Ranko; Pranjković, Ivo . Hrvatski enciklopedijski rječnik. Zagreb: EPH d.o.o. i Novi Liber d.o.o., 2004., str. 100.

Elektronički pečat

- Elektronički pečat odnosi se na podatke u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.
- Napredan elektronički pečat znači elektronički pečat koji je na nedvojben način povezan s autorom pečata; omogućava identificiranje autora pečata i povezan je s podacima na koje se odnosi tako da se može otkriti bilo koja naknadna izmjena podataka.
- Kvalificiran elektronički pečat znači napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat.[13]

Elektronički vremenski žig

- Elektronički vremenski žig odnosi se na podatke u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.
- Kvalificirani vremenski žig znači elektronički vremenski žig koji povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka; temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom i potpisan je pomoću naprednog elektroničkog potpisa ili pečata.[14]

4.1. Elektronički potpis kao dio kriptografije

U svrhu što boljeg razumijevanja funkcioniranja elektroničkog potpisa, potrebno je proučiti okruženje u kojem je elektronički potpis nastao i koju infrastrukturu je iskoristio. Prije pojave elektroničkog potpisa postojale su određene metode zaštite dokumenata, a te iste metode su dio znanstvene discipline – kriptografije. Stoga je potrebno proučiti koje su to metode postojale tada, a na nekima od njih se temelji i princip rada elektroničkog potpisa, što ukazuje na popriličnu povezanost između kriptografije i načina na koji funkcionira elektronički potpis. Jedan od temeljnih aspekata sigurne komunikacije je kriptografija. Ona je potrebna, ali ne i dovoljna za sigurnu komunikaciju. Ona je samo prvi od niza koraka koje je potrebno poduzeti

[13] Uredba eIDAS, n. dj., čl. 3., str. 85.
[14] Ibid.

radi sigurnosti u raznim situacijama. Kriptografija predstavlja znanost tajnog pisanja. Neki elementi iste bili su prisutni već kod starih Grka. Kriptografija je potrebna uslijed svake komunikacije putem nepovjerljivog medija, kao što je internet. Potrebno je razlikovati kriptologiju i kriptografiju.

Kriptologija je termin koji potječe od grčkih riječi *kriptos* (tajan, skriven) i *logos* (nauka), a radi se o disciplini koja se bavi sigurnim (tajnim) načinima komunikacije te obuhvaća kriptografiju i kriptoanalizu. Kriptografija je ta koja se brine o sigurnosti, kontroli i identifikaciji podataka, dok je kriptoanaliza znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptoanaliza ili dekriptiranje je nužna za kriptografiju jer će upravo rezultat kriptoanalize ukazati na kvalitetu kriptografskih koraka. Negativan rezultat kriptoanalize ukazuje na ispravne kriptografske korake, tj. dovoljno sigurni kanal za komunikaciju ili pohranu informacija.

Kriptografija potječe od grčkih riječi *kriptos* (tajan, skriven) i *graphein* (pisati). Kriptografija je znanost o čuvanju podataka na sigurnom. Ona dopušta pohranu informacija ili komunikaciju s drugim strankama, a pritom onemogućuje neovlaštenim strankama razumijevanje pohranjene informacije ili komunikacije. Šifriranjem tekst pretvara u nečitljive podatke, a dešifriranjem se isti podaci vraćaju u razumljivi tekst. Oba procesa uključuju matematičku formulu ili algoritam i tajni slijed podataka (ključ). Kriptografija djeluje na dva načina. Pruža mehanizme za druge primjene kao što su elektronički potpis i digitalni novac, a postala je rasprostranjena i u svojoj uporabi od strane onih koji nemaju jake potrebe za tajnošću. Obično je ugrađena u računalnu i telekomunikacijsku infrastrukturu, a da korisnici nisu toga ni svjesni.

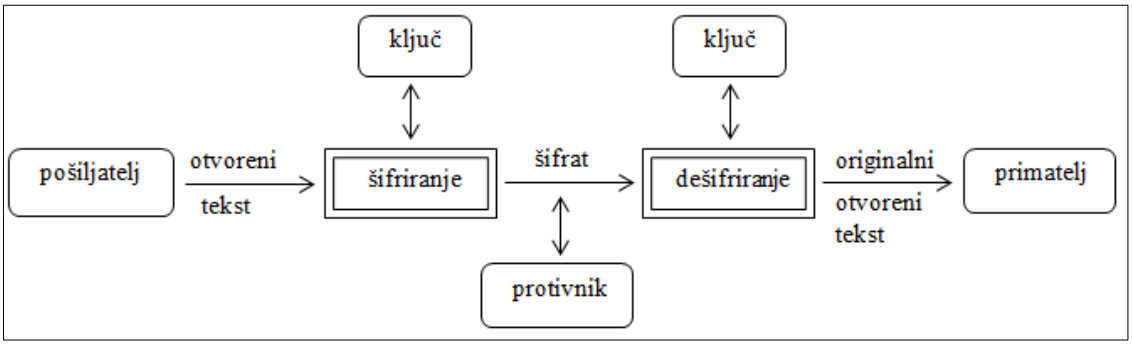
Postoje pet temeljnih funkcija kriptografije putem kojih se ostvaruje sigurnost:

1. Prva od pet funkcija je Privatnost/povjerljivost/tajnost (engl. *privacy*), svojstvo koje osigurava dostupnost informacije samo onoj osobi kojoj je informacija namijenjena. Samo ovlašteni primatelj može izvući sadržaj iz kriptirane poruke, a inače ne bi trebalo biti moguće doći do sadržaja kriptirane poruke.
2. Autentifikacija (engl. *authentication*) je proces kojim se utvrđuje identitet osobe. Ovaj proces je iznimno važan element u informacijskoj sigurnosti.
3. Integritet (engl. *integrity*) podataka je jedno od ključnih svojstava koje je potrebno očuvati. Podaci zadržavaju integritet samo ako nisu na neki način izmijenjeni. Kako bi

se osigurao integritet, pojedinac mora imati mogućnost otkrivanja raznih manipulacija podacima od strane neovlaštenog pojedinca.

4. Neporecivost (engl. *non-repudiation*) je svojstvo, ali i mehanizam putem kojeg se može dokazati da je pošiljatelj stvarno poslao poruku. Ovo svojstvo sprječava poricanje prijašnjih obveza ili akcija. Razni dogovori preko interneta kasnije ne mogu biti opovrgnuti.
5. Razmjena ključeva (engl. *key exchange*) je način na koji se ključevi dijele između pošiljatelja i primatelja.[15]

Osnovni zadatak kriptografije je omogućiti dvjema osobama (pošiljatelju i primatelju, za koje su često u literaturi rezervirana imena *Alice* i *Bob*) komuniciranje preko nesigurnog komunikacijskog kanala na način da treća osoba (njihov protivnik, u literaturi često *Eva* ili *Oskar*), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke. Poruka koju pošiljatelj želi poslati naziva se otvoreni tekst (engl. *plaintext*). Taj isti tekst pošiljatelj transformira koristeći unaprijed dogovoreni ključ (engl. *key*). Taj postupak se naziva šifriranje, a dobiveni rezultat je šifrat (engl. *ciphertext*) ili kriptogram. Taj šifrat pošiljatelj šalje preko komunikacijskog kanala, a protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od protivnika, primatelj zna ključ kojim je poruka šifrirana te na temelju toga može dešifrirati šifrat i odrediti otvoreni tekst. Shema klasične kriptografije prikazana je na slici 3.



Slika 3. Shema klasične kriptografije[16]

[15] Duđela, Andrej; Maretić, Marcel. Kriptografija. Zagreb: Element, 2007., str. 101.
[16] Duđela, Andrej; Maretić, Marcel. Kriptografija, n. dj., str. 2.

Za razliku od dešifriranja, kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito se radi o dvije funkcije od kojih je jedna za šifriranje, a druga za dešifriranje. One preslikavaju osnovne elemente otvorenog teksta (slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata i obratno. Funkcije se biraju iz određene skupine funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva naziva se *prostor ključeva*. Kriptosustav se tako sastoji od kriptografskog algoritma te svih mogućih otvorenih tekstova, šifrata i ključeva.

Kriptosustav (engl. *cryptosystem*) je uređena petorka (P, C, $\mathcal{K}$, $\mathcal{E}$, D) za koju vrijedi:

1. **P** (engl. *plaintext*) je konačan skup svih osnovnih elemenata otvorenog teksta;
2. **C** (engl. *ciphertext*) je konačan skup svih mogućih osnovnih elemenata šifrata;
3. $\mathcal{K}$ (engl. *key*) je konačan skup svih mogućih ključeva;
4. $\mathcal{E}$ (engl. *encryption method*) je skup svih funkcija šifriranja;
5. **D** (engl. *decryption method*) je skup svih funkcija dešifriranja;
6. Za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \rightarrow \mathcal{C}$ i $d_K : \mathcal{C} \rightarrow \mathcal{P}$ funkcije sa svojstvom da je $d_K(e_K(x))=x$ za svaki otvoreni tekst $x \in \mathcal{P}$.[17]

Kriptosustavi se obično dijele s obzirom na tri kriterija:

1. **Tip operacija koje se koriste pri šifriranju**
   Prema tipu operacija koje se koriste pri šifriranju postoji podjela na supstitucijske šifre u kojima se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje s nekim drugim elementom, te transpozicijske šifre u kojima se elementi otvorenog teksta permutiraju. Primjerice, šifriranjem riječi TAJNA u XIWOI, načinjena je supstitucija, a šifriranjem u JANAT transpozicija. Naravno, postoje i kriptosustavi koji kombiniraju ove dvije metode.
2. **Način na koji se obrađuje tekst**
   Ovdje je potrebno razlikovati blokovne (engl. *block cipher*) i protočne šifre (engl. *stream cipher*). Kod blokovnih šifri obrađuje se jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ *K*, dok se kod protočnih elementi

[17] Ibid.

otvorenog teksta obrađuju jedan po jedan koristeći pritom paralelno generirani niz ključeva (engl. *key-stream*).

3. **Tajnost i javnost ključeva**

   S obzirom na tajnost i javnost ključeva potrebno je razlikovati simetrične i asimetrične kriptosustave. Kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obrnuto. Najčešće su ta dva ključa identična. Ovaj tip kriptosustava ima jednu od važnih prednosti, a to je sigurnost koja leži u tajnosti ključa. Upravo zato se simetrični sustavi još zovu i kriptosustavi s tajnim ključem.

   Kod asimetričnih ili kriptosustava s javnim ključem, ključ za dešifriranje se ne može izračunati iz ključa za šifriranje. Ovdje je ključ za šifriranje javni ključ. Naime, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati poruku. Za samu ideju javnog ključa zaslužni su Whitfield Diffie i Martin Hellman koji su 1976. dali prijedlog rješenja problema razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala.[18]

Osnovna pretpostavka kriptoanalize je da kriptoanalitičar zna koji se kriptosustav koristi. Pretpostavka je poznata kao Kerckhoffsovo načelo, po Nizozemcu Augustu Kerckhooffsu, autoru važne knjige "Vojna kriptografija". Ukoliko kriptoanalitičar treba provjeriti i nekoliko mogućih kriptosustava, kompleksnost procedure se bitno ne mijenja. Dakle, za pretpostaviti je da tajnost šifre u potpunosti leži u ključu. Kako bi se smanjio rizik od napada na kriptosustav, kriptosustav može ostati tajan. Međutim, upitno je koliko je rizik od napada smanjen jer kriptoanalitičar može na razne načine otkriti koji se kriptosustav koristi. Kako bi se utvrdila sigurnost kriptosustava potrebno je poznavati ciljeve i sposobnosti kriptoanalitičara. Različiti kriptoanalitičari posjeduju različita znanja i sposobnosti pa s obzirom na to postoji nekoliko vrsta osnovnih razina kriptoanalitičkih napada:

1. **Samo šifrat** *(engl. ciphertext-only attack)*

   U ovome slučaju kriptoanalitičar posjeduje samo šifrat od nekoliko poruka šifriranih pomoću istog algoritma. Njegov je zadatak otkriti otvoreni tekst od što više poruka ili u najboljem slučaju otkriti ključ kojim su poruke šifrirane. Ova razina je ujedno i najslabija razina napada. Jednostavna verzija ovog napada je tzv. *executive search*, slučaj u kojemu kriptoanalitičar dekriptira šifrat sa svim ključevima iz prostora

[18] Duđela, Andrej; Maretić, Marcel. Kriptografija. Zagreb: Element, 2007., str. 3.

ključeva te pronalazi otvoreni tekst među nizom otvorenih tekstova koji ima smisla. Ovaj tip napada koristi se kod kriptosustava koji imaju poprilično male prostore ključeva. Drugi slučaj ovakvih napada je napad uz korištenje statističkih svojstava jezika otvorenog teksta. Upravo se putem tih svojstava mogu dekriptirati šifrat i otkriti ključevi.

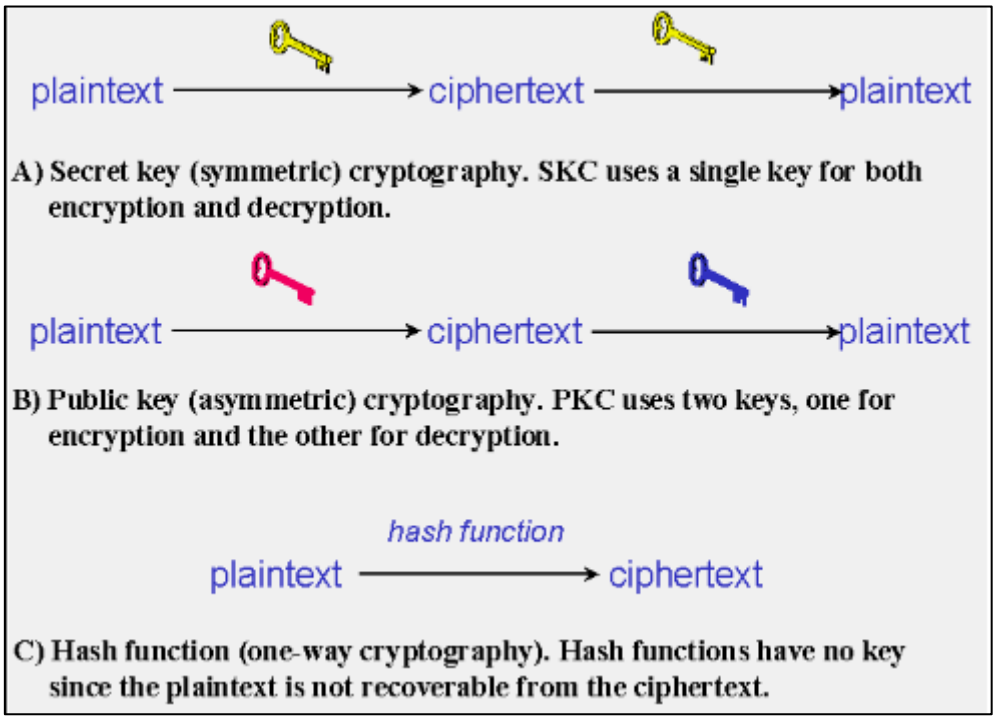
2. **Poznati otvoreni tekst** (engl. *known plaintext attack*)
   Ovdje kriptoanalitičar posjeduje šifrat neke poruke, ali i njemu odgovarajući otvoreni tekst. U prvome slučaju bilo je potrebno otkriti i otvoreni tekst i ključ, a ovdje je potrebno otkriti samo ključ ili neki algoritam za dešifriranje poruka šifriranih tim ključem. Kriptoanalitičar je upoznat s otvorenim tekstom i pripadajućim šifratom.
3. **Odabrani otvoreni tekst** (engl. *chosen plaintext attack*)
   Kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Ovaj napad je jači od prethodnoga, ali je manje realističan. Dakle, kriptoanalitičar može šifrirati otvoreni tekst, ali problem je ključ za dešifriranje s kojim nije upoznat te tako pokušava dešifrirati druge šifrate. Ovaj napad je uvijek moguć u asimetričnim kriptosustavima jer je ključ korišten za šifriranje javno poznat.
4. **Odabrani šifrat** (engl. *chosen ciphertext attack*)
   Kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može odabrati šifrat te dobiti odgovarajući otvoreni tekst. Zadatak je otkriti ključ za dešifriranje (tajni ključ). Ovaj napad je tipičan za kriptosustave s javnim ključem. Kriptoanalitičar može dešifrirati šifrat prema vlastitom izboru, ali mora otkriti ključ za dešifriranje. Ovakav napad je moguć kod kriptosustava koji se koriste za identifikaciju. Ono što kriptoanalitičar ovdje može je oponašati pošiljatelja. Umjesto slanja nasumično odabranih brojeva, kriptoanalitičar primatelju šalje poruke prema vlastitom izboru, a primatelj će u tom slučaju imati poteškoća pri dešifriranju.[19]

4.1.1. Osnovne vrste šifriranja

Kroz naredna poglavlja bit će detaljnije analizirane dvije osnovne vrste šifriranja, tj. dva osnovna sustava ključeva koji se koriste u kriptografiji, a koji su gradivni blokovi sigurnosti. Riječ je o simetričnoj kriptografiji (engl. *Secret Key Cryptography, SKC*) i asimetričnoj kriptografiji (engl. *Public Key Cryptography, PKC*). Također će biti predstavljena i hash funkcija (engl. *Hash Function*) koja u svom najjednostavnijem obliku ne koristi ključeve, te PGP mehanizam šifriranja koji je zapravo hibridni kriptosustav jer kombinira simetrično i

[19] Duđela, Andrej; Maretić, Marcel. Kriptografija, n. dj., str. 4.

asimetrično šifriranje. Simetrična i asimetrična kriptografija su i jedan od kriterija podjele kriptosustava. Iz slike 4 je vidljivo koje su to temeljne razlike između simetrične i asimetrične kriptografije te hash funkcije, a koje će biti analizirane u narednim poglavljima. Simetričnu i asimetričnu kriptografiju potrebno je razlikovati i prema tajnosti i javnosti ključeva. Jedna od temeljnih razlika između simetrične i asimetrične kriptografije je i broj ključeva. Simetrična koristi samo jedan ključ za šifriranje i dešifriranje, dok asimetrična koristi dva različita ključa.



Slika 4. Simetrična kriptografija, asimetrična kriptografija, hash funkcija[20]

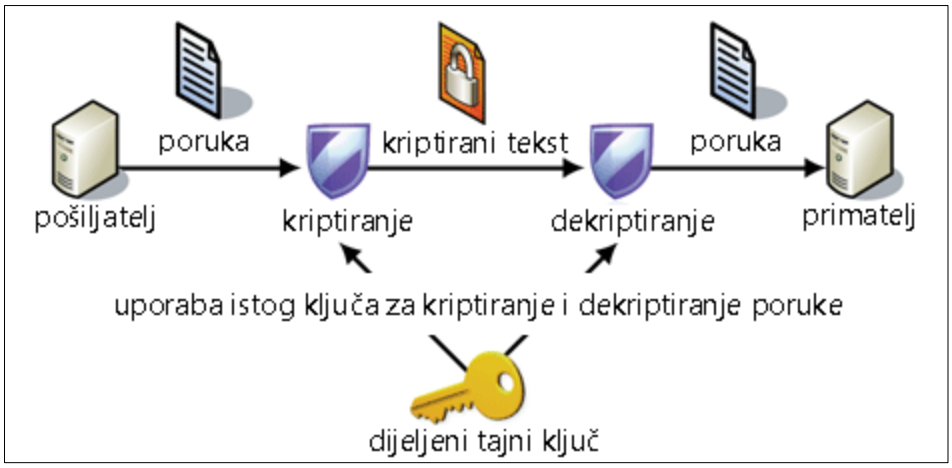
Svrha šifriranja je zaštiti podatke koje sadrži poruka koju pošiljatelj želi poslati. Potrebno je naglasiti da se za šifriranje podataka koristi algoritam i kriptografski ključ. U procesu sudjeluju dvije osobe, tj. pošiljatelj i primatelj poruke, a provode se dva osnovna koraka, šifriranje i dešifriranje poruke.

4.1.1.1. Simetrična kriptografija

Alice, tj. pošiljatelj želi poslati šifriranu poruku Bobu, tj. primatelju. U tom slučaju Alice koristi ključ za šifriranje (engl. *encryption key*), a Bob koristi odgovarajući ključ za dešifriranje (engl. *decryption key*) šifrata i određivanje otvorenog teksta. Ako je u

[20] Kessler, Gary C. An overview of criptography. 2018. URL: https://www.garykessler.net/library/crypto.html#why3

kriptosustavu ključ za šifriranje uvijek jednak ključu za dešifriranje ili se ključ za dešifriranje može jednostavno odrediti na temelju ključa za šifriranje, radi se o simetričnoj kriptografiji i simetričnom (konvencionalnom) kriptosustavu.



Slika 5. Proces šifriranja i dešifriranja tajnim ključem[21]

Proces koji se odvija u sklopu simetrične kriptografije uključuje nekoliko koraka, kao što je prikazano na slici 5:

1. Pošiljatelj i primatelj postignu dogovor oko tajnog ključa – pošiljatelj šifrira otvoreni tekst u šifrat koristeći algoritam za šifriranje i tajni ključ koji je poznat i jednoj i drugoj strani.
2. Pošiljatelj šalje šifrat primatelju.
3. Primatelj dešifrira šifrat u otvoreni tekst koristeći zajednički tajni ključ.

Treća osoba, u literaturi poznatija kao Eva ili Oskar, može presresti šifrat, međutim, neće biti u mogućnosti pročitati sadržaj poruke. Treća osoba može pročitati sadržaj poruke jedino ako ima ključ (koji može ukrasti ili pogađati dok ne otkrije odgovarajući ključ) koji i primatelj poruke koristi za dešifriranje ili ako otkrije određenu slabost algoritma koji je pošiljatelj koristio za šifriranje poruke. U slučaju otkrivanja slabosti algoritma, treća osoba može odrediti sadržaj poruke bez ključa.

Kod simetrične kriptografije za svaki par ključeva (e, d), na osnovu poznatog ključa e jednostavno je izračunati ključ d i obrnuto. To znači da je dovoljno znati samo jedan od dva ključa iz para ključeva jer se radi o jedno te istom ključu, tj. $e=d$. Zbog sigurnosnih razloga taj

[21] CARNet CERT. Nedostaci PKI infrastrukture. 2009., str. 6. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-02-255.pdf

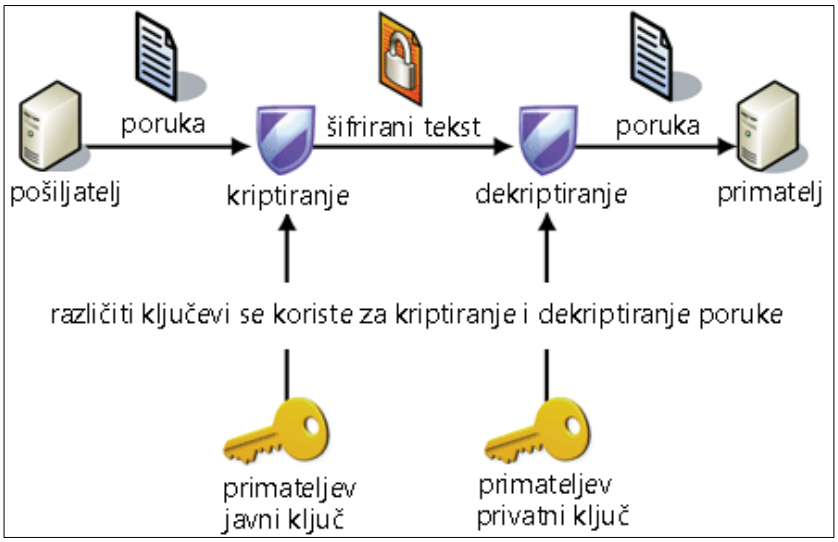
ključ mora ostati tajan, a također mora biti moguća i njegova česta promjena. Važno je napomenuti da su algoritmi koji se koriste prilikom šifriranja i dešifriranja javno poznati, ali dogovoreni ključ koji koristi jedna i druga strana mora ostati tajan. Najveća mana simetrične kriptografije je upravo dogovor oko tajnog ključa i njegova distribucija. Kako bi primatelj mogao dešifrirati šifrat, potrebno mu je nekako dostaviti ključ *e*. Međutim, problem nastaje kada nije moguće stvaranje sigurnog kanala do primatelja. U tom slučaju koriste se asimetrični algoritmi. Sigurni komunikacijski kanal potreban je za slanje tajnog ključa primatelju jer tek nakon toga obje strane mogu koristiti isti ključ za šifriranje i dešifriranje. Prijedlog u praksi je česta izmjena zajedničkog ključa *e* kako bi komunikacija bila sigurna. Simetrični algoritmi su s obzirom na svoje karakteristike potrebni za šifriranje i dešifriranje, dok se problem distribucije ključa često rješava upotrebom asimetričnih algoritama. Algoritme za simetrično šifriranje moguće je brzo i uspješno implementirati u hardver i softver, tako su oni prilagođeni za šifriranje velike količine podataka, dok asimetrična kriptografija nije toliko djelotvorna i prilagođena za velike količine podataka, ali zato uspješno rješava problem distribucije ključa kod simetrične kriptografije.

4.1.1.2. Asimetrična kriptografija

U asimetričnoj kriptografiji ključevi se razlikuju, a određivanje ključa za dešifriranje na temelju ključa za šifriranje nije isplativo. U ovom sustavu ključeva, ključ za šifriranje može biti javan. Ako primatelj želi primati šifrirane poruke, mora objaviti ključ za šifriranje, a odgovarajući ključ za dešifriranje će ostati tajan. U ovome slučaju, bilo tko može koristiti ključ za šifriranje poruka koje želi poslati primatelju, te se taj ključ naziva javnim ključem (engl. *public key*), ali samo primatelj može dešifrirati poruke, te se ključ za dešifriranje naziva još i privatnim ključem (engl. *private key*). Stoga se često asimetrična kriptografija naziva i kriptografija javnim ključem (engl. *Public Key Cryptography, PKC).*

Proces koji se odvija u sklopu asimetrične kriptografije također uključuje nekoliko koraka, kao što je prikazano na slici 6:

1. Primatelj stvara par ključeva od kojih je jedan privatan, a drugi šalje pošiljatelju – pošiljatelj upotrebom asimetričnog algoritma i javnog ključa primatelja šifrira otvoreni tekst u šifrat.
2. Pošiljatelj šalje šifrat primatelju.
3. Primatelj dešifrira šifrat u otvoreni tekst koristeći privatni ključ koji odgovara javnom ključu korištenom prilikom šifriranja otvorenog teksta.



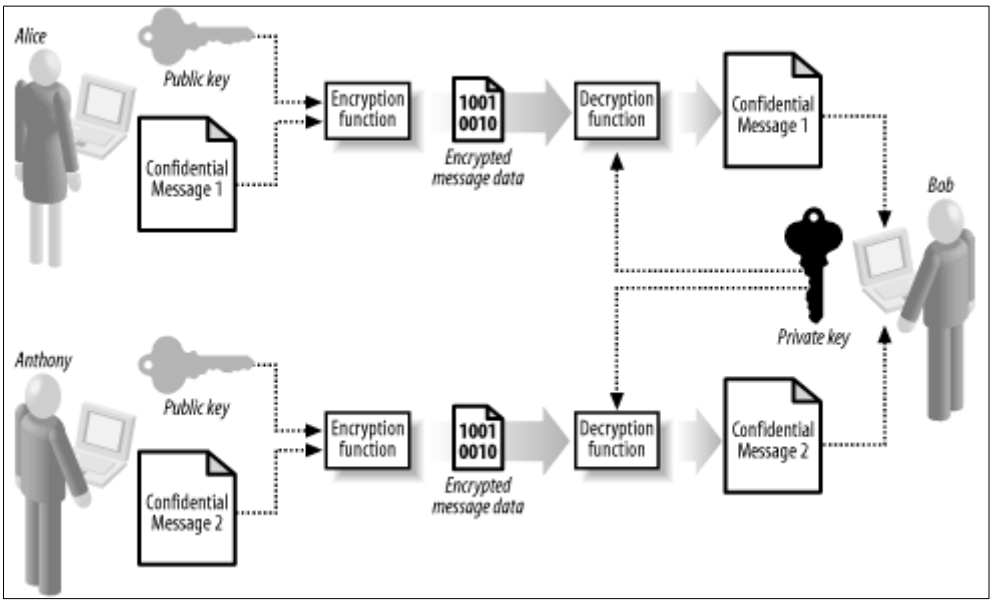
Slika 6. Proces šifriranja i dešifriranja primjenom dva različita ključa[22]

U asimetričnoj kriptografiji, pošiljatelj šifrira otvoreni tekst jednim ključem, a drugi ključ, koji nije identičan prvom ključu, kao što je to slučaj kod simetrične kriptografije, koristi se za dešifriranje. Ta dva ključa nisu identična, ali čine par ključeva koji jedan drugome odgovaraju i samo je njihovom kombinacijom moguće šifrirati i dešifrirati isti otvoreni tekst. Javni ključ primatelja mogu znati sve osobe koje tom primatelju žele poslati poruku, ali privatni ključ poznat je samo primatelju. Jedna od temeljnih razlika u odnosu na simetričnu kriptografiju je činjenica da primatelj apsolutno ne sudjeluje u stvaranju para ključeva, tj. primatelj prilikom stvaranja ključeva ne uzima u obzir prijedloge pošiljatelja, nego jednostavno nakon stvaranja ključeva, šalje javni ključ.

Kao što je već spomenuto, pošiljatelj prilikom šifriranja otvorenog teksta osim javnog ključa koristi i asimetrični algoritam. Asimetrični algoritam uključuje protokol stvaranja ključeva (engl. *key generation protocol*) koji koristi primatelj kako bi generirao novi par ključeva. Asimetrični algoritam zapravo uključuje dvije povezane funkcije od kojih svaka ima određeni zadatak. Funkcija šifriranja šifrira otvoreni tekst koristeći javni ključ, a funkcija dešifriranja koristi privatni ključ za dešifriranje šifrata. Funkcija šifriranja može samo šifrirati otvoreni tekst što znači da pošiljatelj ne može dešifrirati šifrat koji je nastao šifriranjem. Ovakva jednosmjerna priroda funkcije šifriranja ukazuje na činjenicu da poruke jednog pošiljatelja

[22] CARNet CERT. Nedostaci PKI infrastrukture. 2009., str. 7. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-02-255.pdf

nisu vidljive drugom pošiljatelju (slika 7). Ako primatelj posumnja da je netko otkrio privatni ključ, jednostavno će generirati novi par ključeva. Isto tako je važno istaknuti da primatelj ne može koristiti par ključeva za slanje poruke pošiljatelju zbog te jednosmjerne prirode funkcija. Ako primatelj želi poslati poruku, pošiljatelj mora generirati par ključeva.



Slika 7. Oba pošiljatelja koriste isti ključ za šifriranje, a šifrat može dešifrirati samo primatelj[23]

Asimetrično kriptiranje primjenjuje se na dva osnovna načina. Prvi je kriptiranje uporabom javnog ključa, postupak u kojem poruka kriptirana javnim ključem primatelja ne može biti dekriptirana bez privatnog ključa istog primatelja. Drugi način je elektronički potpis. Mehanizam u kojem poruku potpisanu privatnim ključem pošiljatelja svaki korisnik može provjeriti, ako ima pošiljateljev javni ključ.

Simetrična vs. asimetrična kriptografija

Nakon što je kroz prethodna dva poglavlja detaljnije objašnjeno kako funkcioniraju simetrična i asimetrična kriptografija, potrebno ih je usporediti i utvrditi po čemu se razlikuju i koje su to prednosti i mane jedne i druge. Simetrična kriptografija primjenjuje simetrične algoritme i tajni ključ koji se primjenjuje i kod šifriranja i kod dešifriranja, dok se u sklopu asimetrične

[23] etutorials. org. Asymmetric Encryption Explained. URL: http://etutorials.org/Programming/Programming+.net+security/Part+III+.NET+Cryptography/Chapter+15.+Asymmetric+Encryption/15.1+Asymmetric+Encryption+Explained/

koriste asimetrični algoritmi i dva različita ključa – od kojih je jedan za šifriranje, a drugi za dešifriranje. Također je potrebno naglasiti dva osnovna izazova prisutna i u jednom i u drugom sustavu ključeva. Prvi izazov je distribucija ključeva, tj. kako poslati ključ kako bi se ostvarila sigurna komunikacija i kako uspostaviti dovoljno siguran komunikacijski kanal za slanje ključeva. Drugi izazov se odnosi na upravljanje ključevima (engl. *key management*), tj. kako očuvati sigurnost ključeva i osigurati dostupnost kada su potrebni. Ovo je posebno izazov u sustavu koji sadrži puno ključeva. Ključevi u simetričnom kriptosustavu u većini slučajeva nemaju neka posebna svojstva, jednostavno ih je generirati i broj ključa je nasumično generiran, dok ključevi u sklopu asimetričnih kriptosustava imaju posebnu strukturu i njihovo generiranje je poprilično skupo.

Asimetrična kriptografija je potrebna za distribuciju tajnog ključa. Elektronički potpis je primjer forme koja zahtijeva primjenu asimetrične kriptografije pošto je jedan od glavnih ciljeva zadržati neporecivost i omogućiti provjeru identiteta korisnika. Asimetrična kriptografija se prvenstveno pojavila kako bi se riješili određeni problemi simetrične, tj. povjerenje i dogovor oko ključa koji će se koristiti. S obzirom da pošiljatelj i primatelj koriste isti ključ, mora biti prisutna visoka razina povjerenja, a dogovor oko ključa mora se odvijati u sigurnoj okolini.

4.1.2. Hash funkcije

Hash funkcija H je funkcija koja za ulazni podatak m (datoteku, poruku, ...) proizvoljne veličine računa vrijednost unaprijed određene veličine, koja je najčešće izražena u bitovima. Vrijednost $H(m)$ još se naziva i hash-code, hash-rezultat, hash-vrijednost ili jednostavno hash od m. Uobičajeno je vrijednosti hash funkcija zapisivati u heksadecimalnom obliku. Pod hash funkcijom podrazumijeva se hash funkcija bez ključa, osim ako nije drugačije navedeno. Hash funkcija služi za brzo dobivanje „digitalnog otiska prsta“ podataka. Osnovna ideja hash funkcije je da hash služi kao reprezentativna slika ili digitalni otisak ulazne vrijednosti i da se ne može dobiti pomoću neke druge ulazne vrijednosti. U literaturi se hash funkcije još nazivaju i funkcijama/algoritmima za izračunavanje sažetka poruke. Razlog tome je činjenica da hash funkcije uzimaju poruku kao ulaz i proizvode izlaz koji je zapravo sažetak poruke. Hash se često uspoređuje s otiscima prstiju i ta se ideja koristi u raznim kriptografskim shemama, a posebno kod elektroničkog potpisa gdje hash funkcija ima ulogu „vezivnog tkiva“ između poruke i potpisa.

Područja primjene

Hash funkcije imaju dva osnovna područja primjene:

- kriptografija / zaštita podataka,
- detekcija pogreške / provjera ispravnosti podataka.

Hash funkcije koje se primjenjuju u ovim područjima su poprilično različite. Glavno svojstvo funkcija koje se primjenjuju u kriptografiji je to što su jednosmjerne, tj. njihovim korištenjem se iz poznavanja sažetka poruke ne može matematičkim operacijama doći do originalnog podatka iz kojeg je sažetak izračunat. Kod kreiranja takvih algoritama osnovna pretpostavka je da postoji zlonamjerni korisnik koji ima namjeru naći podatak čiji će sažetak biti jednak nekom pronađenom sažetku kako bi taj podatak iskoristio za npr. lažiranje autentikacije. Hash funkcije koje se primjenjuju kod detekcije pogrešaka i provjere ispravnosti podataka koriste se za detekciju pogreške prilikom prijenosa podataka komunikacijskim kanalom ili za detekciju pogreške prilikom pohranjivanja podataka na medij. Kod takvih hash funkcija nije važno jesu li otporne na napade korisnika, a također se ne smatra nedostatkom ako je moguće iz dvije različite poruke generirati isti sažetak.

Hash funkcije primjenjuju se i kod elektroničkog potpisa te provjere integriteta podataka. U sklopu elektroničkog potpisa, dugačka poruka se hashira i samo se dobivena hash vrijednost digitalno potpisuje. Primatelj poruke tada hashira primljenu poruku i zapravo potvrđuje da elektronički potpis odgovara hash vrijednosti. Hash vrijednost koja odgovora određenoj ulaznoj vrijednosti bit će s vremenom izračunata. Integritet hash vrijednosti je do određene razine zaštićen, ali u određenom trenutku, bit će potrebno, u svrhu provjere mogućih promjena u podacima, ponovno izračunati hash vrijednost na temelju ulazne vrijednosti, te će se ta hash vrijednost usporediti s izvornom hash vrijednosti. Ovaj proces se primjenjuje kada je potrebno provjeriti integritet podataka.

Svojstva hash funkcija

Hash funkcija zadovoljava dva svojstva:

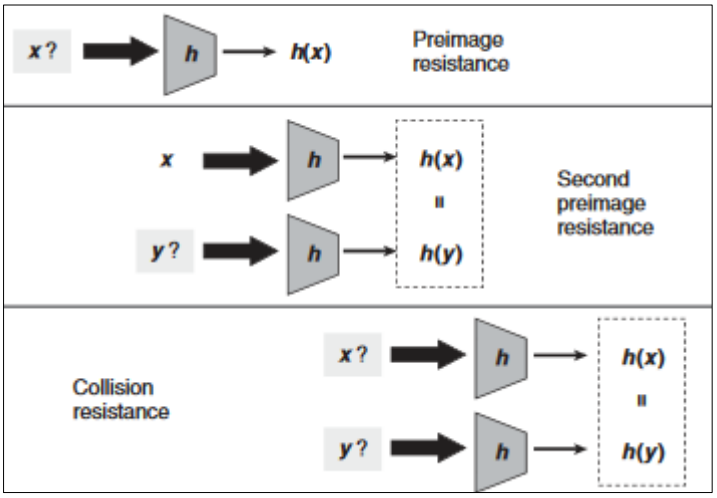
1. Kompresija – hash funkcija ulazu x proizvoljne konačne duljine pridružuje izlaz $h(x)$ fiksne duljine n;
2. Jednostavnost izračuna – zadani su h i ulaz x, $h(x)$ je jednostavno izračunati.[24]

[24] Menzes, J. Alfred; Oorschot, Paul C.;Vanstone, Scott A. Handbook of applied cryptography.USA: CRC Press, 1996., str. 322. URL: http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf. (24.06.2018.)

Osnovno svojstvo svih hash funkcija je zahtjev da za bilo koja dva izračunata različita hasha i ulazi iz kojih su oni izračunati moraju biti različiti. Drugo svojstvo bi bilo da za ta dva izračunata ista hasha ulazi iz kojih su izračunati ne moraju biti isti. Ako izračunamo hash vrijednost za jedan ulaz, a nakon toga promijenimo samo jedan *bit*, tada bi novi izračunati hash trebao biti potpuno različit od prethodnog. Tipična hash funkcija može prihvatiti bilo koju veličinu ulaznog podatka, a izlaz je obično niz bitova fiksne dužine, ali može biti i varijabilne. Neke hash funkcije će za istu dužinu ulaznih podataka uvijek dati jednaku dužinu izlaznog podatka – u tom slučaju riječ je o permutacijama.

U kriptografiji se koriste hash funkcije koje moraju zadovoljiti određena svojstva:

1. *H* radi s blokovima proizvoljne veličine;
2. izlaz od *H* je fiksne duljine (u bitovima);
3. za svaki *x* relativno je lako izračunati *H* (*x*) (važno za primjenu);
4. za zadanu vrijednost *h* nemoguće je naći *x* takav da je *H*(*x*)=*h* → **svojstvo jednosmjernosti** (engl. *one-way* ili *preimage resistant*);
5. za zadani *x* nemoguće je naći *y* tako da je *H*(*x*)=*H*(*y*) → **jednoznačnost** ili **slaba otpornost na koliziju** (engl. *weak collision resistance* ili *2nd-preimage resistance*);
6. nemoguće je naći par (*x*, *y*) tako da je *H*(*x*)=*H*(*y*) → **općenita jednoznačnost** ili **jaka otpornost na koliziju** (engl. *strong collision resistance* ili *collision resistance*).[25]



Slika 8. Svojstva sigurnosti[26]

[25] Dujela, Andrej; Maretić, Marcel. Kriptografija, n. dj., str. 143.
[26] Keith, Martin. Everyday Cryptography: Fundamental Principles and Applications. New York:Oxford University Press, 2012., str. 191, URL: https://bayanbox.ir/view/2880755982131658715/Oxford-Everyday-Cryptography-Fundamental-Principles-and-Applications-2014.pdf. (11.05.2018.).

Svojstva od 4. do 6. su kriptografski zahtjevi potrebni kako korištenje hash funkcije ne bi oslabilo sigurnost sheme elektroničkog potpisa. Hash funkcije koje zadovoljavaju svojstvo 1. do 6. su kriptografske hash funkcije.

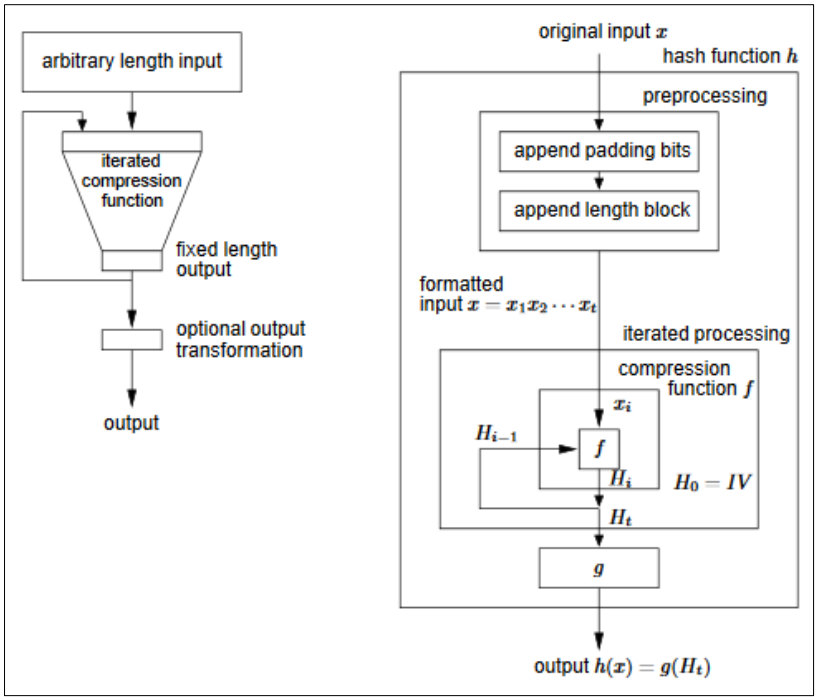
Također je potrebno promotriti veze između svojstava 4.-6. (slika 8). Svojstvo jednosmjernosti, jednoznačnosti i opće jednoznačnosti u literaturi se često naziva i svojstvom sigurnosti – s obzirom na to da je jedan od ključnih zadataka hash funkcija podići razinu sigurnosti podataka. Iako su ova tri svojstva povezana, zapravo su poprilično različita što je vidljivo ako se usporede različite primjene hash funkcija i identificiraju svojstva sigurnosti koja su u tim slučajevima primjene potrebna.

Također je važno napomenuti da hash funkcija koja zadovoljava svojstva 4.-6. može imati i neka neželjena svojstva. Hash algoritam se smatra nesigurnim ako je moguć pronalazak prethodno nepoznatog podatka za koji algoritam kao rezultat daje traženi sažetak ili nalaženje kolizija, tj. dva različita podatka koji za rezultat daju isti sažetak. „Idealni hash algoritam je onaj koji je maksimalno „dosadan“, tj. nema zanimljivih svojstava poput produživanja dužine i jedina razlika između algoritma i funkcije generiranja slučajnih brojeva je ta što je algoritam deterministčkog karaktera i što je efikasan za računanje.“[27]

Osnovna konstrukcija hash funkcija

Većina hash funkcija bez ključa *h* su dizajnirane kao iterativni procesi koji hashiraju ulaze proizvoljne duljine obrađujući uzastopne blokove fiksne veličine.

[27] CARnet CERT. Algoritmi za izračunavanje sažetaka. 2006., str. 6. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-166.pdf. (11.05.2018).



Slika 9. Opći model iterativne hash funkcije – jednostavni i detaljni prikaz[28]

Na slici 9 prikazan je opći model iterativne hash funkcije. Lijevi model je nešto jednostavniji, a desni model detaljniji prikaz hash funkcije. Hash ulaz *x* proizvoljne konačne veličine je podijeljen na *r*-bitne blokove x_i fiksne duljine. Predobrada se obično uključuje dodavanjem koliko god je potrebno blokova za postizanje cjelokupne duljine *bita* što se još naziva i *padding.* Svaki blok x_i tada služi kao ulaz unutarnjoj hash funkciji *f* fiksne veličine, funkciji kompresije od *h*, koja izračunava novi međurezultat duljine bita *n*, za neki fiksni *n*, kao funkcija od prethodnog *n*-bitnog međurezultata i sljedećeg ulaznog bloka x_i. Neka H_i u ovom slučaju označava djelomičan rezultat poslije faze *i*, opći proces za iterativnu hash funkciju s ulazom $x=x_1x_2...x_t$ može biti modeliran na sljedeći način:

$$H_0=IV;\ H_i=f(H_{i-1}, x_i),\ 1 \leq i \leq t;\ h(x)=g(H_t)$$

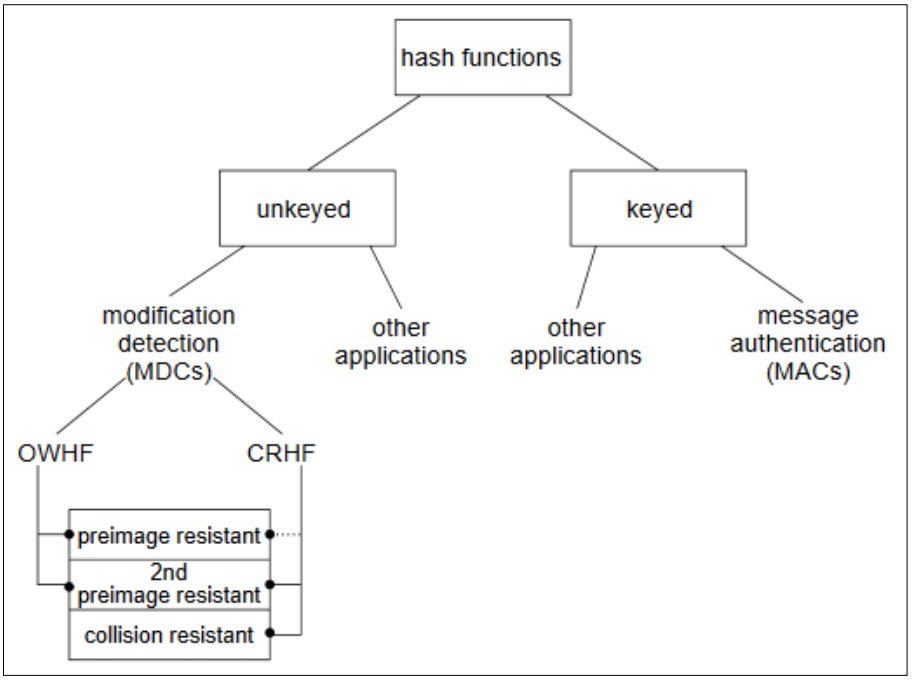
H_{i-1} predstavlja *n*-bitno ulančavanje između faze *i-1* i faze *i*, a H_0 je ranije definirana početna vrijednost ili inicijalna vrijednost (*IV*). Proizvoljan izlaz transformacije *g*, koristi se u konačnom koraku za pridruživanje *n*-bitnih ulančanih varijabli *m*-bitnom rezultatu $g(H_t)$, a *g* je često identiteta $g(H_t)=H_t$. Specifične hash funkcije imaju određene karakteristike po kojima se razlikuju, a to su narav predobrade, funkcija kompresije i transformacija izlaza.[29]

[28] Menzes, Handbook of applied cryptography, n. dj., str. 332.
[29] Menzes, Handbook of applied cryptography, n. dj., str. 332 – 333.

Klasifikacija hash funkcija

Hash funkcije mogu se u osnovi podijeliti na one s ključem i bez ključa. Kao što je već spomenuto, pod hash funkcijom podrazumijeva se ona bez ključa, osim ako nije drugačije navedeno. S obzirom na svojstva koja posjeduju i zahtjeve koje specifične aplikacije imaju, hash funkcije mogu se podijeliti na dva osnovna tipa (pojednostavljena klasifikacija prikazana je i na slici 10):

1. modificirano otkrivanje kodova ili hash funkcije bez ključa (engl. *Modification Detection Codes, MAC*)
    a. jednosmjerna hash funkcija (engl. *One-Way Hash Functions, OWHF*)
    b. hash funkcije s jakom otpornosti na koliziju (engl. *Collision Resistant Hash Functions, CRHF*)
2. kodovi autentičnosti poruke ili hash funkcije s ključem (engl. *Message Authentication Codes, MAC*)[30]



Slika 10. Pojednostavljena klasifikacija kriptografskih hash funkcija[31]

Kao što je već navedeno, u kriptografiji se koriste hash funkcije koje zadovoljavaju navedena svojstva 1.-6. i nazivaju se kriptografskim hash funkcijama. Te funkcije su specifične po tome

[30] Menzes, Handbook of applied cryptography, n. dj., str. 323.
[31] Menzes, Handbook of applied cryptography, n. dj., str.324.

što imaju dodatna sigurnosna svojstva kako bi ih se moglo koristiti za autentifikaciju i očuvanje integriteta podataka.

4.1.3. PGP-primjer hibridnog kriptosustava

Kroz poglavlja koja analiziraju simetričnu i asimetričnu kriptografiju, utvrđeno je kako kod simetrične kriptografije primatelj može pročitati poruku samo ako mu pošiljatelj dostavi svoj tajni ključ. Stoga je prednost jednostavnost, dok je mana nemogućnost čitanja poruke od strane pošiljatelja i primatelja ako se ključ izgubi i potreba za čestom promjenom ključa radi sigurnosti. S druge strane, asimetrična kriptografija povećava razinu sigurnosti primjenom dva različita ključa. Rješava problem gubljenja ključa pošiljatelja, ali ne rješava i problem brze zamjene postojećeg ključa novim. Kao rješenje pojavio se PGP (engl. *Pretty Good Privacy, PGP*) program za kriptografsku zaštitu podataka, koji se dosta primjenjuje u procesu digitalnog potpisivanja. PGP program poseban je po tome što kombinira ono najbolje iz područja simetrične i asimetrične kriptografije čime omogućuje kvalitetno i jako šifriranje. Osoba zaslužna za razvoj ovog programa je Philip Zimmermann koji je kao antinuklearni aktivist imao potrebu za sigurnom komunikacijom sa svojim istomišljenicima.
PGP mehanizam zapravo predstavlja hibridni kriptosustav koji se sastoji od nekoliko ključnih komponenti, a to su generator slučajnih ključeva, simetrični algoritam za šifriranje sadržaja poruke, asimetrični algoritam za šifriranje jednokratnog ključa te hash algoritam za stvaranje digitalnog otiska poruke. S vremenom je izašlo nekoliko verzija ovog programa, princip rada ostao je isti, a samo su se mijenjali korišteni algoritmi. Širenje softvera izvan SAD-a je i dalje bilo ilegalno zbog izvoznog zakona ITAR (engl. *International Traffic in Arms Regulations*), koji zabranjuje izvoz izvan SAD-a svake tehnologije koja se može upotrijebiti za proizvodnju oružja, a tu spadaju i algoritmi za enkripciju podataka. Međutim, PGP softver se brzo proširio putem interneta. Iz koda koji je ilegalno izvezen iz SAD-a je nastala nova verzija programa nazvana PGPi (engl. *PGP International*), koja se dalje samostalno razvijala u Europi. Brojni programeri su podržavali PGP sintaksu, stoga se javila potreba za standardizacijom, što je dovelo do OpenPGP standarda.

Princip rada

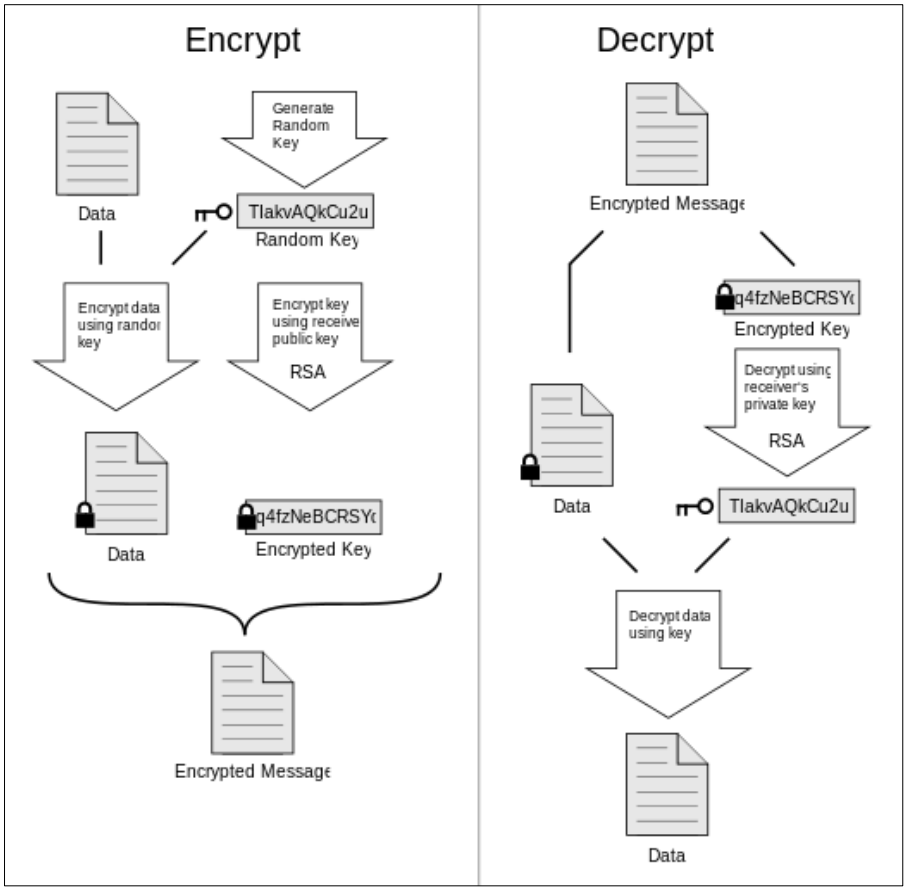
Programi PGP i GnuPG primjenjuju se kod šifriranja i digitalnog potpisivanja dokumenata. Princip rada je sličan i temelji se na kombinaciji algoritama za šifriranje kako bi se postigla što veća razina sigurnosti. Temelji se na hash algoritmu kao posebnom skupu matematičkih operacija kojima se iz dokumenta generira jedinstveni sažetak, tj. hash ili otisak poruke.

Nemoguće je za dva različita dokumenta proizvesti jednak otisak, a isto tako nije moguće niti iz poznatog otiska kreirati izvorni dokument. Tako je moguće dva puta generirati otisak nekog dokumenta i ako su otisci jednaki, dokazano je da su generirani iz istog dokumenta. Stoga se hash algoritmi ponajviše primjenjuju radi zaštite od neovlaštenih promjena dokumenta. Osim hash algoritma, princip rada obuhvaća i dvije ključne operacije, a to su simetrična i asimetrična kriptografija.

Princip rada PGP sustava, tj. operacije šifriranja i dešifriranja poruke prikazane su kroz sliku 11, a u ovom slučaju se koristi RSA kriptosustav javnog ključa. Svaki korisnik raspolaže asimetričnim parom ključeva od kojih je jedan privatni, a jedan javni. Sadržaj poruke štiti se jednokratnim simetričnim ključem koji se posebno generira za svaku poruku, a taj isti ključ potrebno je poslati pošiljatelju poruke zaštićen asimetričnim šifriranjem pomoću javnog ključa primatelja poruke. Jednokratni ključ generira upravo PGP sustav i složenost generiranja je sigurnosni čimbenik u postupku šifriranja. Što je vremensko razdoblje u generiranju slijeda ključeva dulje, time je teže otkriti način na koji se slijed generira temeljem „prisluškivanja“ njegovih dijelova.[32] Prvi korak koji je potrebno poduzeti prije korištenja PGP sustava je generiranje barem jednog para asimetričnih ključeva. U tome slučaju sustav nudi razne opcije, a potrebno je i odabrati veličinu ključa (1024, 2048 ili 4096 bitova). Generirani ključevi su poprilično dugački tako da ih korisnik ne može zapamtiti i upisati prilikom svakog šifriranja, stoga se privatni ključ šifrira pomoću posebne kratke šifre (engl. *passphrase*). Postoji i mogućnost probijanja PGP sustava, ali samo ako se zna početno stanje generatora pseudo-slučajnih brojeva jer je time moguće predvidjeti niz brojeva koji će se generirati. Jedino rješenje je skrivanje početnog stanja, o čemu brine sama PGP potpora. Za razliku od asimetričnog para ključeva simetrični ključ generira se automatski kao slučajna vrijednost i svaki puta je drugačiji. On se šifrira asimetričnim algoritmom pomoću javnog ključa primatelja poruke i dodaje na početak poruke.

Ono što PGP sustav radi prije samog šifriranja je sažimanje ZIP algoritmom, zbog čega poruka zauzima manje prostora i otpornija je na provale. Kako bi primatelj mogao pročitati poruku, potreban mu je privatni ili javni ključ kako bi dešifrirao jednokratni ključ poruke. Javni ključ je pošiljatelj ugradio u poruku ili se nalazi na nekom od PGP poslužitelja. Za čuvanje javnih ključeva koristi se PKS poslužitelj (engl. *Public Key Server*).

[32] Radić, Drago. " Informatička abeceda ". Kriptiranje – zaštita poruka u komunikaciji. https://informatika.buzdo.com/pojmovi/gpg-1.htm. (22.09.2018.).



Slika 11. Princip rada PGP sustava – šifriranje i dešifriranje[33]

Osim povjerljivosti koju osigurava zaštita podataka, PGP nudi i funkcionalnost kojom se omogućuje provjera autentičnosti koja je prvenstveno usmjerena na primatelja jer omogućava provjeru autentičnosti pošiljatelja. U svrhu provjere autentičnosti koristi se kombinacija šifriranja i potpisa. Razlog tome je što samo šifriranje nije dovoljno u svrhu otkrivanja osobe koja je šifrirala poruku pa se poruka još i digitalno potpisuje.

4.1.4. Kriptografski algoritmi

Kriptografski algoritmi dijele se u tri kategorije, a to su simetrični, asimetrični algoritmi i kriptografske hash funkcije. Glavni ciljevi koji su ispunjeni primjenom kriptografskih algoritama su povjerljivost, integritet podataka, autentifikacija i neporecivost. Nadalje će biti ukratko predstavljeni najznačajniji predstavnici svake kategorije.

[33] Information security. URL: https://security.stackexchange.com/questions/20134/in-pgp-why-not-just-encrypt-message-with-recipients-public-key-why-the-meta-e.(16.06.2018.).

Tablica 1. Simetrični i asimetrični algoritmi

PRIMJENA NA	SIMETRIČNI ALGORITMI	ASIMETRIČNI ALGORITMI
blokovne šifre	DES, 3DES, RC2, RC5, AES, CAST, IDEA, Skipjack, Safer, Blowfish, FEAL, Lucifer	RSA
protočne šifre	RC4, A5 (GSM), Rambutan	BBS

4.1.4.1. Simetrični

S obzirom na način na koji se obrađuje otvoreni tekst, postoje blokovne i protočne šifre. Simetrične algoritmi također se dijele u dvije grupe, algoritme koji se primjenjuju na blokovne šifre i one koji se primjenjuju na protočne šifre. Stream šifriranje funkcionira tako da se šifriranje poruke vrši bit po bit, dok se kod blok šifriranja vrši po blokovima podataka, tj. uzimaju se blokovi od više bitova te se šifriraju kao jedna cjelina. Simetrični algoritmi koji se primjenjuju u blok šifriranju su DES, 3ES, RC2, RC5, AES, CAST, IDEA, Skipjack, Safer, Blowfish, FEAL i Lucifer. U stream šifriranju primjenjuju se RC4, A5 (GSM) i Rambutan. Ovdje će biti predstavljeni neki od najznačajnijih simetričnih algoritama.

Lucifer

Prvi simetrični algoritam, prethodnik DES-a, je Lucifer. Osmislio ga je Horst Fiestel – razvio ga je IBM u 70-im godinama. Radi se o prvom simetričnom algoritmu s blok šifriranjem. Puno je jednostavniji od DES-a, enkriptira blok veličine 128 bita, a iste veličine je i ključ. Primjenjuje i 16 ključeva od 72 bita, a dešifriranje se vrši inverznim šifriranjem. Glavne slabosti ovog algoritma su pri korištenju ključeva (engl. *key scheduling*) i slaba otpornost na napade diferencijalne kriptoanalize.

DES (Data Encryption Standard)

Krajem 60-ih i početkom 70-ih godina 20. st. pojavila se potreba za šifrom koju će moći koristiti korisnici širom svijeta, a u koju će u isto vrijeme imati povjerenja, dakle pojavila se potreba za uvođenjem standarda u kriptografiji. Godine 1972. NBS (*National Bureau of Standards*) inicirao je program za zaštitu računalnih i komunikacijskih podataka, a jedan od ciljeva bio je i razvoj standarda, stoga je 1973. raspisan natječaj za kriptosustav koji je trebao zadovoljiti određene uvjete (visok stupanj sigurnosti, efikasnost, mogućnost provjere, specifikacija i razumijevanje algoritma itd.). Među prijavama istaknula se ona IBM-a čiji kriptosustav se temeljio na Feistelevoj šifri. Jedna od glavnih ideja je primjena supstitucije i

transpozicije kroz više iteracija. Predloženi algoritam je prihvaćen kao standard 1976. godine pod nazivom *Data Encryption Standard* (DES).[34]
DES šifrira otvoreni tekst koji je duljine 64 bita te pritom koristi ključ koji je duljine 56 bitova, čime se dobiva šifrat koji je opet 64 bita.

AES (Advanced Encryption Standard)
Još jedan od značajnijih algoritama iz ove skupine je AES. Godine 1997. *National Institute of Standards and Technology (NIST),* objavio je natječaj za kriptosustav koji bi trebao kao opće prihvaćeni standard zamijeniti DES. Prema NIST-u novi sustav bi trebao biti simetričan i blokovni, a upravo je AES zadovoljio te uvjete. AES šifrira blokove od 128 bitova=16 bajtova.

4.1.4.2. Asimetrični

Asimetrični algoritmi primjenjuju se u asimetričnoj kriptografiji, tj. kriptografiji javnog ključa. Iako je u simetričnoj kriptografiji nužna tajnost ključa, to je i veliki nedostatak simetričnog sustava budući da za razmjenu ključa mora postojati sigurni komunikacijski kanal. Godine 1976. Whitfield Diffie i Martin Hellman ponudili su moguće rješenje problema, a to je upravo kriptografija javnog ključa. Ideja se sastoji u tome da bi iz poznavanja funkcije šifriranja e_K bilo gotovo nemoguće izračunati funkciju dešifriranja d_K. Tada bi funkcija e_K mogla biti javna. U kriptografiji javnog ključa ključnu ulogu imaju tzv. jednosmjerne funkcije. Funkcija je jednosmjerna (engl. *one-way*) ako je f lako, a f^{-1} teško izračunati. Važno je napomenuti da se kriptografija javnog ključa ne koristi za šifriranje poruka, već za šifriranje ključeva, a glavni razlog za to je činjenica da su algoritmi s javnim ključem puno sporiji od modernih simetričnih algoritama. Najpoznatiji algoritmi koji se primjenjuju u asimetričnoj kriptografiji su RSA, Diffie-Hellman, ElGamal, Rabin i Eliptic Curves.

Najpoznatiji među njima je upravo RSA. RSA algoritam razvili su Rivest, Shamir i Adelman 1977. godine. Sigurnost ovog algoritma temelji se na složenosti izračunavanja vrlo velikih primarnih brojeva. Algoritam se sastoji od nekoliko koraka:

1. odabrati dva velika primarna broja: p i q,

2. izračunati $n=p*q$ i $z=(p-1) * (q-1)$,

3. izabrati broj d takav da su z i d relativno prosti,

4. pronaći e takav da je $(e*d)$ mod $z=1$,

[34] Duđela, Andrej; Maretić, Marcel .Kriptografija, n. dj., str. 67.

5. privatni ključ čini par (*n*, *d*), dok javni ključ čini par (*e*, *d*),

6. p i q ne smiju biti nikad otkriveni, poželjno ih je uništiti.[35]

4.1.5. Kriptografske hash funkcije

Bit će ukratko predstavljene najznačajnije hash funkcije, tj. algoritmi koji su se koristili ili se još uvijek koriste u praksi. Kriptografske hash funkcije su važne zbog dodatnih sigurnosnih svojstava, zbog čega ih se primjenjuje u autentifikaciji i očuvanju integriteta podataka. Najpoznatiji hash algoritmi su MD5 i SHA algoritam te MAC kodovi.

MD5 algoritam (engl. *Message-Digest algorithm 5*) za izračunavanje sažetka koristi 128-bitni sažetak. Definiran je *RFC 1312* standardom[36] i koristi se u raznim sigurnosnim aplikacijama za provjeru integriteta datoteka. Primjenjuje se i za enkripciju kod pohranjivanja zaporki. Razvio ga je 1991. godine Ronald Rivest kao nasljednika algoritma MD4, ali već 1996. godine dolazi do otkrivanja ranjivih strana ovog algoritma, pa se preporučuje korištenje drugih (SHA). Ostao je u uporabi sve do 2004. godine kada su otkrivene ozbiljne sigurnosne mane.

Prema NIST-u MD5 se pokazao kao algoritam koji ima određene mane te postoji nekoliko vrsta napada na isti i zbog toga nije siguran. Stoga je NIST 1993. godine predložio novi algoritam koji je poboljšanje MD5 algoritma. Riječ je o SHA algoritmu (engl. *Secure Hash Algorithm*). Prvi SHA algoritam, SHA-0 objavljen je 1993. godine, međutim ubrzo je povučen iz upotrebe zbog otkrivene mane. Godine 1995. objavljen je SHA-1 koji je samo izmijenjena varijanta SHA-0. Stoga se SHA-1 smatra nasljednikom MD5. Poboljšani nasljednik SHA-1 algoritma je SHA-2 koji sadrži određene izmjene i kao rezultat daje duži sažetak. Također ga je objavio NIST 2001. godine. Skupni je naziv za SHA-224, SHA-256, SHA-384 i SHA-512 algoritme kod kojih brojke u nazivu označavaju dužinu sažetka. Posljednji u SHA skupini je SHA-3 algoritam koji je objavljen 2015. godine. On nije zamijenio SHA-2 algoritam, nego će se oba algoritma nadopunjavati.

MAC algoritam je algoritam koji se primjenjuje za autentifikacija i provjeru integriteta poruka tako što se uz poruku šalje i dodatni podatak koji se naziva MAC sažetak, a dobiva se upotrebom MAC algoritma i tajnog ključa. Primatelj poruke može uz posjed identičnog tajnog

[35] CARNet CERT. Napadi na RSA. 2003., str. 4. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-04-19.pdf. (21.05.2018.).
[36] RFC 1312. The MD5 Message-Digest Algorithm URL: https://www.ietf.org/rfc/rfc1321.txt. (21.05.2018.).

ključa upotrebom istog algoritma provjeriti odgovara li MAC sažetak primljenoj poruci te time može verificirati integritet i autentičnost poruke.[37]

4.1.6. Algoritmi za generiranje elektroničkog potpisa

Potrebno je posebno izdvojiti algoritme koji se koriste za generiranje elektroničkog potpisa. DS algoritmi sastoje se od tri osnovna koraka – stvaranje javnog i tajnog ključa, stvaranje elektroničkog potpisa na temelju sažetka poruke i privatnog ključa te utvrđivanje vjerodostojnosti potpisane poruke korištenjem javnog ključa pošiljatelja. Riječ je o DSA/DSS (engl. *Digital Signature Algorithm*) i ECDSA (engl. *Elliptic Curve Digital Signature Algorithm*). DSA je dio NIST-ovog *Digital Signature Standarda*[38]. Osim navedenih algoritama, često se primjenjuje i RSA algoritam.

DSA algoritam je razvijen po uzoru na ElGamalov-om kriptosustavu elektroničkog potpisa. Ovaj algoritam ne prati obrazac šifriranja hash vrijednosti tajnim ključem, a umjesto cijele poruke *m* koristi samo hash vrijednost *H(m)*. ECDSA predstavlja analogon DSA algoritma. Godine 1999. prihvaćen je kao ANSI standard. Ovaj algoritam se sastoji od tri etape – generiranje ključeva, generiranje potpisa i provjera potpisa.

4.1.7. Upravljanje ključevima

Odgovarajuće upravljanje kriptografskim ključevima jamči sigurnost. Sigurnost informacije koja se štiti primjenom kriptografije ovisi upravo o kriptografskim ključevima te mehanizmima i protokolima na koje se ključevi oslanjaju. Svi ključevi bi trebali biti zaštićeni od neovlaštene zamjene ili modifikacije, a privatni ključevi bi trebali biti zaštićeni od neovlaštenog otkrivanja. Upravljanje ključevima omogućuje sigurnu generaciju, pohranu, distribuciju i uništavanje ključeva. Jedan od glavnih problema je nekoliko administratora koji su zaduženi za upravljanje samo svojim ključevima (administrator za baze podataka, administrator za pohranu, administrator za operacijske sustave itd.), čime isti postaju neovisni jedni o drugima i s vremenom razviju vlastiti sustav upravljanja ključevima. Zbog toga je potrebna primjena centraliziranog sustava koji će omogućiti svim administratorima koji su zaduženi za upravljanje ključevima na nekoj razini sustava, upravljanje u skladu s dogovorenim zadacima, pravilima, politikom i standardima.

[37] CARnet CERT. Algoritmi za izračunavanje sažetaka, n. dj., str. 14.
[38] NIST. Digital Signature Standard (DSS). URL: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf. (06.06.2018.).

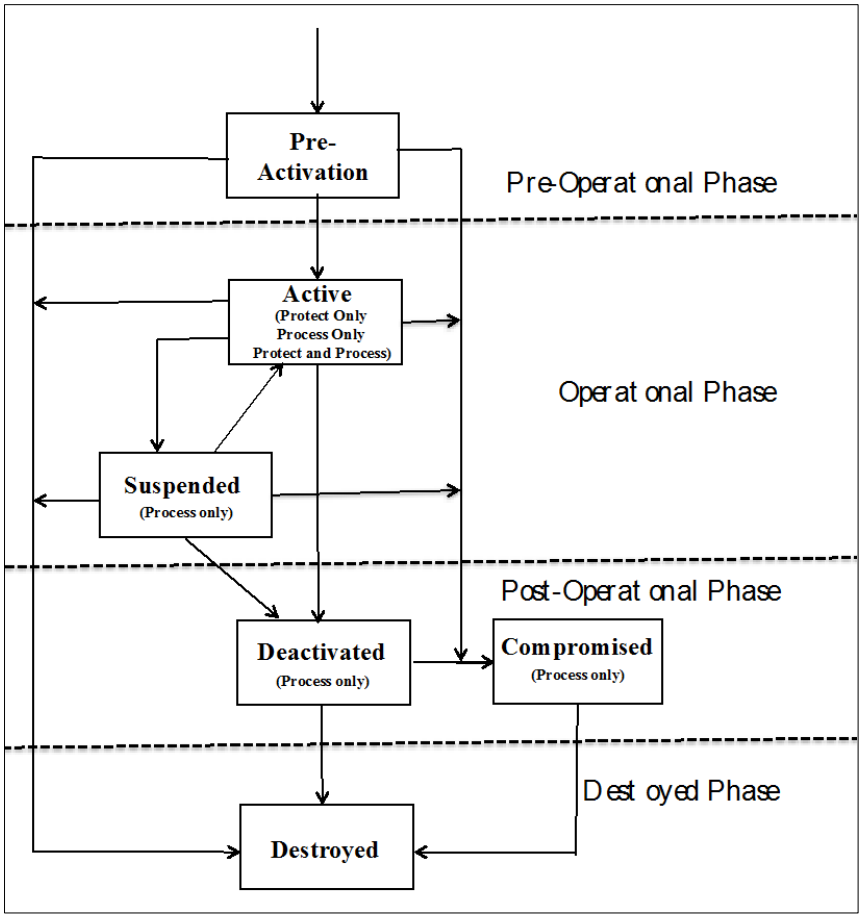
Upravljanje kriptografskim ključevima (engl. *Cryptographic Key Management*) je skup raznih operacija koje su potrebne za održavanje šifriranih podataka i ključeva koji su tim podacima pridruženi, tijekom životnog ciklusa podataka i pridruženih ključeva. Sustav za upravljanje ključevima (engl. *Key Management System, KMS*) predstavlja implementaciju svih dijelova, tj. operacija koje obuhvaća proces upravljanja ključevima.[39]

Operacije koje su dio procesa upravljanja ključevima proizlaze iz sigurnosnih zahtjeva organizacije i politike upravljanja ključevima. Također je važno napomenuti da je proces upravljanja ključevima puno više od šifriranja i dešifriranja. Usmjeren je ponajviše na upravljanje, primjenu i provjeru ključeva. Proces upravljanja ključevima jedan je i od ključnih aspekata PKI infrastrukture.

Životni ciklus upravljanja ključevima

U ovome radu bit će predstavljen životni ciklus upravljanja ključevima koji je dio smjernica za upravljanje ključevima koje je sastavio NIST[40]. Smjernice se sastoje od tri dokumenta - *SP 800-57 Part 1, General; SP 800-57 Part 2, Best Practices for Key Management Organizations* i *SP 800-57 Part 3, Application-Specific Key Management Guidance*. Životni ciklus je detaljno predstavljen u dokumentu *SP 800-57 Part 1, General*[41]. Životni ciklus predstavljen u smjernicama, osnovni je model koji svaka organizacija primjenjuje u skladu sa svojim zahtjevima i politikom rada. Podijeljen je u nekoliko faza upravljanja i nekoliko stanja koja će ključ proći kroz svoj životni ciklus (slika 12).

[39] Kwidama, Sevickson; Hassanmahomed, Taarik. Criptographyc Key Management. Academiyear 2008-2009. URL: https://www.os3.nl/_media/2008-2009/courses/lia/ckm_thassanmahomed_skwidama.pdf. (06.06.2018.).
[40] NIST. URL: https://www.nist.gov/
[41] NIST. Reccomendation for Key Management: Part 1: General.2016., URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf. (07.06.2018.).



Slika 12. Faze i stanja u procesu upravljanja ključevima[42]

Faze upravljanja ključevima:

- *Pre-operational* – Početna faza u kojoj su ključevi generirani, ali se još ne mogu primijeniti u kriptografskim operacijama. Ključevi možda još i nisu generirani ili se nalaze u *pre-activation* stanju.
- *Operational* – Faza u kojoj su ključevi spremni za primjenu u kriptografskim operacijama. U ovoj fazi ključ po svojim karakteristikama može biti Protect only (šifriranje), Process only (dešifriranje) i Protect and Process (simetrični ključ).
- *Post-operational* – Faza u kojoj ključ više nije u uobičajenoj upotrebi, međutim i dalje je moguće pristupiti materijalu koji ključ sadrži u svrhu daljnje obrade. U ovoj fazi ključevi se nalaze u deaktiviranom ili čak ugroženom stanju. Dok nisu u procesu obrade, mogu se pohraniti u arhivi.

[42] NIST. Recommendation for Key Management: Part 1: General, n. dj., str. 85.

- *Destroyed* – Posljednja faza u kojoj ključevi više nisu dostupni za primjenu. Prolaze postupak uništavanja. Zapisi o postojanju ključeva se također mogu obrisati. Iako su ključevi uništeni, metapodaci se mogu sačuvati.[43]

Stanja ključa tijekom životnog ciklusa:

- *Pre-activation state* – Stanje u kojem su ključevi generirani, ali još uvijek se ne mogu primijeniti u kriptografskim operacijama. Dok je u ovom stanju, ključ se može dostaviti certifikacijskom tijelu (engl. *Certification Authority, CA*) kako bi isto provelo certificiranje i registraciju. U ovoj fazi se također odvija i potvrda ključeva između primatelja i pošiljatelja.
- *Active state* – Ovo je stanje u kojemu je ključ aktivan i može se koristiti za šifriranje i dešifriranje podataka. U ovome stanju, po karakteristikama, ključ može biti *Protect only*, *Process only* ili *Protect and process*.
- *Deactivated state* – Stanje u kojem se ključ nalazi nakon što je završio proces kriptiranja podataka. Međutim, ključ se i dalje može koristiti za obradu šifrata. Ovo stanje traje sve dok više nije potrebna obrada informacija koje su tim ključem zaštićene.
- *Compromised state* – Ključ se nalazi u ugroženom stanju nakon što je isti otkrio entitet koji ne sudjeluje u komunikaciji, tj. nije dio sigurnog komunikacijskog kanala.
- *Destroyed state* – Ključ je uništen. Međutim, metapodaci se mogu sačuvati u svrhu daljnjih provjera.
- *Destroyed compromised state* – Ključ je također uništen, ali razlika između ovog i prethodno navedenog stanja je u tome što se ovdje sumnja da je ključ i ugrožen, tj. otkriven od strane neovlaštenog entiteta.[44]

Upravljanje kriptografskim ključevima je administracija zadataka u raznim aspektima primjene ključeva u kriptografiji (generiranje, razmjena, distribucija, pohrana, zamjena, uporaba ključeva). Svaki ključ bi trebao biti zaštićen od mogućeg otkrivanja, modifikacije, zamjene i neadekvatnog korištenja.

4.1.8. Generiranje, verifikacija i validacija elektroničkog potpisa

Elektronički potpis služi za potpisivanje podataka te njihovu provjeru. Zapravo se elektroničkim potpisom može potvrditi da je određena osoba potpisala neki dokument, a osim

[43] NIST. Recommendation for Key Management, n. dj., str. 84.
[44] Kwidama, Criptographyc Key Management, n. dj., str. 9.

toga moguće je i ustanoviti je li došlo do promjene podataka nakon što je dokument digitalno potpisan. Uz pravilnu implementaciju algoritma elektroničkog potpisa moguće je ostvariti ulogu elektroničkog potpisa. Životni ciklus elektroničkog potpisa sastoji se od tri osnovna procesa – generiranje, verifikacija i validacija. Ovo su tri procesa koja prolazi svaki elektronički potpis. Za proces generiranja zadužena je osoba koja digitalno potpisuje dokument, služba zadužena za verifikaciju potpisa potvrđuje valjanost potpisa i identitet osobe koja je generirala taj elektronički potpis. Potpisnik ima dva ključa, javni i privatni i vlasnik je tog para ključeva. Vlasnik para ključeva je jedini entitet ovlašten za korištenje privatnog ključa u svrhu generiranja elektroničkog potpisa. Za potrebe generiranja i verifikacije poruka se transformira u sažetak poruke primjenom hash funkcije. Služba zadužena za verifikaciju također mora imati potvrdu da javni ključ koji se koristi za verifikaciju stvarno pripada entitetu koji je generirao elektronički potpis. Isto tako mora imati i potvrdu da vlasnik para ključeva stvarno posjeduje privatni ključ koji je povezan s javnim ključem i da je javni ključ matematički ispravan.

Životni ciklus elektroničkog potpisa, tj. proces generiranja, verifikacije i validacije objašnjen je u standardu pod nazivom *Digital Signature Standard (DSS)*[45] koji je sastavio NIST, a objavljen je 2013. godine. Standard je dio *Federal Information Processing Standards Publications (FIPS PUBS).*

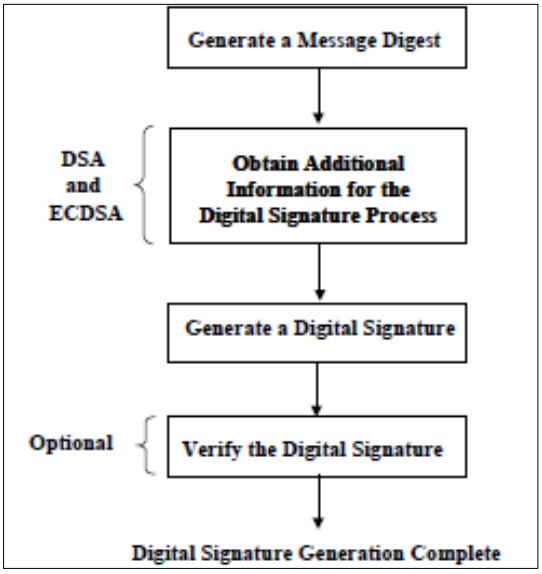
Prije samog procesa generiranja i verifikacije elektroničkog potpisa postoji niz koraka koje je potrebno poduzeti. Zajednički naziv za te korake je početno podešavanje (engl. *initial setup*).

Početno podešavanje uključuje nekoliko koraka koji su nužni za daljnje procese – potpisnik ili neki drugi entitet trebao bi za DSA i ECDSA algoritme definirati parametre domene i imati potvrdu o valjanosti tih domena, potpisnik također mora generirati par ključeva. Kao vlasnik para ključeva mora potvrditi valjanost javnog ključa i potvrditi da stvarno posjeduje odgovarajući privatni ključ. Entitet zadužen za verifikaciju također od potpisnika zahtjeva i potvrdu o identitetu.

Nakon početnog podešavanja slijedi proces generiranja elektroničkog potpisa (slika 13). Prije svega potrebno je uz primjenu odgovarajuće hash funkcije dobiti sažetak poruke. Zbog sažetka poruke potpisivanje će biti puno brže. Osim sažetka poruke potrebno je i prikupiti dodatne informacije za algoritam koji se primjenjuje za generiranje potpisa. Primjenom odabranog algoritma za generiranje, privatnog ključa, sažetka poruke i drugih važnih

[45] NIST. Digital Signature Standard (DSS), n. dj.

informacija, elektronički potpis je generiran. Proces bi se trebao odvijati u skladu sa DSS standardom.



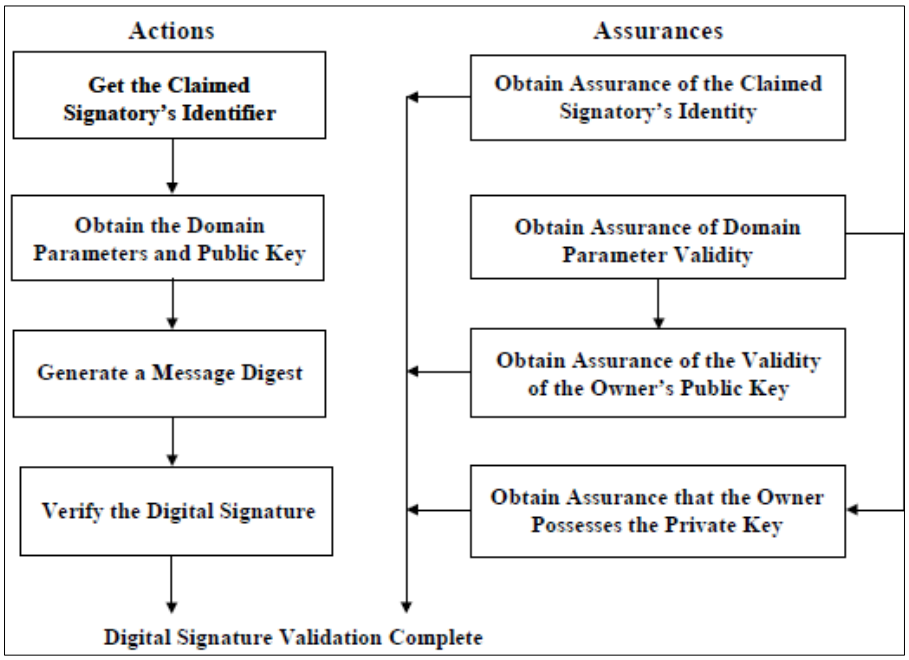
Slika 13. Generiranje elektroničkog potpisa[46]

Na slici 14 prikazan je proces verifikacije i validacije elektroničkog potpisa. Riječ je o procesima koji također podrazumijevaju niz koraka koje je potrebno poduzeti. Procese provodi entitet zadužen za verifikaciju i validaciju, tj. entitet koji je primatelj digitalno potpisane poruke. Rezultat svakog koraka je određena potvrda, a sve uspješne potvrde na kraju rezultiraju uspješnom verifikacijom i validacijom. Kako bi se elektronički potpis mogao verificirati, entitet zadužen za verifikaciju mora imati javni ključ iz para ključeva potpisnika. Ako su u procesu generiranja korišteni DSA ili ECDSA algoritam, potrebno je utvrditi i parametri domene. Javni ključ i parametre domene moguće je dobiti od treće strane od povjerenja ili direktno od potpisnika. Zatim je potrebno generirati sažetak poruke i to sažetak poruke onih podataka čiji elektronički potpis je u postupku verifikacije, a primjenom hash funkcije koja je korištena i tijekom generiranja elektroničkog potpisa. Uz odgovarajući DS algoritam, parametre domene, javni ključ i sažetak poruke provodi se postupak verifikacije.
Potvrda valjanosti elektroničkog potpisa moguća je samo ako: je provjeren i potvrđen identitet potpisnika, potvrđena je valjanost parametara domene, potvrđena je valjanost javnog ključa i potvrđeno je da potpisnik stvarno posjeduje privatni ključ iz generiranog para ključeva. Ovo

[46] NIST. Digital Signature Standard (DSS), n dj., str.12.

su zapravo jamstva (engl. *assurances*) koja potvrđuju valjanost elektroničkog potpisa. Za potvrđivanje ovih jamstava također postoje metode koje se primjenjuju.

Ako su postupak verifikacije i potvrđivanje jamstava uspješni, elektronički potpis je valjan, a ako je ishod negativan, elektronički potpis nije valjan. U slučaju elektroničkog potpisa koji nije valjan, primjenjuje se politika organizacije.



Slika 14. Verifikacija i validacija elektroničkog potpisa[47]

[47] NIST. Digital Signature Standard (DSS), n. dj., str. 12.

5. Upravljanje elektroničkim potpisom

Politika upravljanja elektroničkim potpisom je imenovani skup pravila koja navode primjenjivost elektroničkog potpisa unutar određene zajednice ili za određeni skup primjena s uobičajenim sigurnosnim zahtjevima. Politika se kreira za korištenje u točno određenim situacijama i definira prava i obaveze svih strana. Politika upravljanja elektroničkim potpisima definira se na razini organizacije, pojedinih tvrtki te vladinih i nevladinih agencija i odjela. Sadrži pravila upravljanja i korištenja certifikata s javnim ključevima. Politikom upravljanja elektroničkim potpisima propisuje se korištenje određene infrastrukture javnih ključeva i normi sigurnosti.[48]

5.1. PKI- infrastruktura javnog ključa

Jedno od ključnih pitanja koje se može postaviti prilikom komunikacije pomoću kriptosustava javnim ključem je pitanje vjerodostojnosti ili autentičnosti poruke. Naime, osoba B ne može biti sigurna da joj je upravo osoba A poslala poruku. Obzirom da svatko ima pristup funkciji za šifriranje e_B, može se lažno predstaviti kao osoba. Diffie i Hellman su 1976. godine opisali ideju elektroničkog potpisa poruke. Ideja je da se pomoću originalne poruke i tajnog ključa osobe A generira elektronički potpis za osobu A. Imajući na raspolaganju poruku, elektronički potpis i javni ključ osobe A, osoba B može verificirati autentičnost potpisa. Nedostatak potpisivanja elektroničkim potpisom je udvostručena duljina poruke, čime i postupak potpisivanja duže traje. Stoga se umjesto originalne poruke koristi sažetak poruke koji se dobije primjenom hash funkcije. Kod digitalnog potpisivanja postoji problem identiteta ključa. Jedna od mogućnosti je da će se protivnik Oskar predstaviti lažnim pseudonimom Bob. U takvoj situaciji Alice može misliti da je šifrirala poruku za Boba, a ustvari je tu poruku pročitao protivnik Oskar. Stoga nas uspješna provjera elektroničkog potpisa ne uvjerava da je poruku potpisala Alice, već samo da je poruka potpisana tajnim ključem koji odgovara javnom ključu za koji je vjerojatno da pripada Alice.

Jedno od rješenja problema identiteta je PKI (engl. *Public Key Infrastructure*), tj. infrastruktura javnog ključa. PKI infrastruktura predstavlja skupinu programa, ljudi, sigurnosnih politika i procedura potrebnih za kreiranje, upravljanje, pohranjivanje te povlačenje digitalnih certifikata.[49] Ključna komponenta je treća strana od povjerenja koja

[48] CARNet CERT. Digitalni potpis. 2007., str. 13. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf. (10.06.2018.).
[49] CARNet CERT. Digitalni potpis, n. dj., str. 10.

jamči za identitet osobe, tj. ključeva. PKI povezuje javne ključeve s pojedinačnim korisnikom pomoću središnjeg autoriteta, a povezivanje je omogućeno kroz procese registracije i izdavanja certifikata koji, ovisno o razini sigurnosti, mogu biti izvedeni programima u CA entitetima ili pod ljudskim nadzorom. Središnji autoritet zamjenjuje ulogu javnog bilježnika u digitalnom svijetu. Ponekad se za središnji autoritet koristi i izraz TTP (engl. *trusted third party*). Djelovanje središnjeg autoriteta temelji se upravo na izdavanju certifikata, tj. digitalno potpisanih poruka koje sadrže osobne podatke nositelja javnog ključa i sam javni ključ. Javni ključ središnjeg autoriteta je jedini ključ u koji bi osoba trebala imati povjerenja. Javni ključ se smatra valjanim ako postoji lanac certifikata koji doseže do središnjeg autoriteta. Infrastruktura je definirana unutar ITU-T standarda pod nazivom *X. 509*[50], a temelji se na strogoj hijerarhijskoj organizaciji.

Osnovne značajke

Osnovne značajke PKI infrastrukture su ujedno i obilježja koja bi digitalno potpisani zapisi trebali zadržati prilikom dugotrajnog očuvanja. Riječ je o povjerljivosti, integritetu, vjerodostojnosti i nemogućnosti poricanja.

Povjerljivost je svojstvo koje osigurava tajnost i privatnost podataka uporabom kriptografskih algoritama. Integritetom se osigurava da podaci nisu ugroženi ili izmijenjeni, a prijenos podataka također nije promijenjen. Osnovni podaci kojima se osigurava svojstvo integriteta su javni ključevi, certifikati i elektronički potpisi. Sama provjera identiteta odvija se u sklopu procesa autentifikacije uporabom certifikata i elektroničkih potpisa. Primjer korištenja autentifikacije su usluge stvaranja i prodaje proizvoda preko elektroničkih sustava. Posljednje svojstvo je nemogućnost poricanja koje je zapravo iznimno važno u procesu dugotrajnog očuvanja digitalno potpisanih zapisa. Riječ je o svojstvu koje osigurava nemogućnost poricanja i odbijanja prijenosa podataka uporabom kriptografije javnim ključevima i elektroničkih potpisa. Ovo svojstvo se također primjenjuje u sustavima za elektroničko poslovanje (engl. *e-commerce*).

Primjena PKI infrastrukture

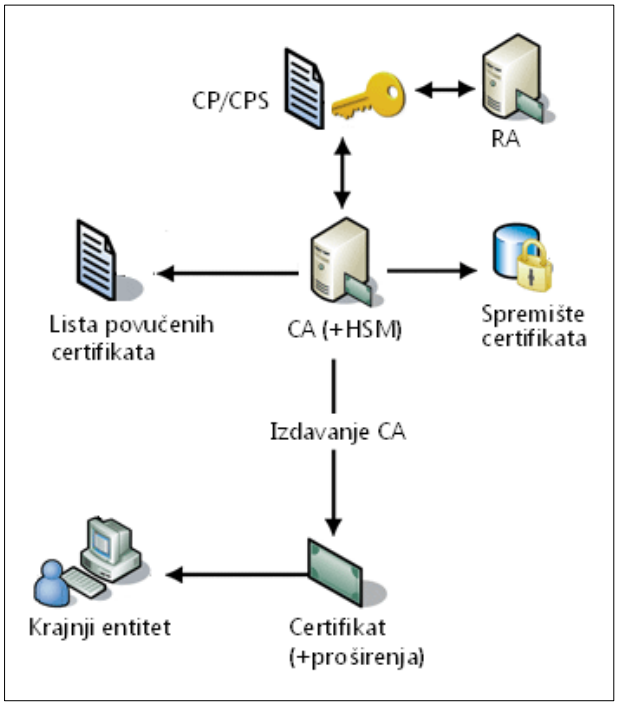
Osnovna funkcija PKI infrastrukture je omogućavanje distribucije i korištenje javnih ključeva i certifikata osiguravajući sigurnost i integritet. Sustavi koji zahtijevaju primjenu PKI-a su

[50] X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 2016. URL: http://www.itu.int/rec/T-REC-X.509-201610-I/en

poruke elektroničke pošte, usluge e-poslovanja, razne aplikacije, online bankarstvo itd. PKI također omogućava osnovne sigurnosne usluge – SSL, IPsec i HTTP protokol za komunikaciju i sigurnost, SET protokol za razmjenu vrijednosti i drugo. Što se tiče prednosti PKI-a, potrebno je izdvojiti smanjenje troškova obrade transakcijskih pristupa, smanjenje i odjeljivanje rizika, povećanje efikasnosti i performansa sustava.

PKI arhitektura

PKI infrastruktura sastoji se od nekoliko međusobno povezanih objekata, aplikacija i usluga.



Slika 15. Komponente PKI infrastrukture[51]

Osnovne komponente sustava su (slika 15) :

- Krajnji entitet za potpisivanje – svaki korisnik ili objekt koji treba digitalni certifikat iz nekog razloga. Mora imati sposobnost generiranja javnog ključa te pohrane i korištenja privatnog ključa.
- CA (engl. *Certificate Authority*) – središnji autoritet koji predstavlja javnog bilježnika u digitalnom svijetu ili treću stranu od povjerenja. Tijelo kojemu korisnici vjeruju i koje je zaduženo za kreiranje i dodjelu javnih ključeva certifikata. Razina povjerenja

[51] CARNet CERT. Nedostaci PKI infrastrukture, n. dj., str. 12 .

CA ovisi o razini suglasnosti drugih entiteta u tom CA. CA ključ se dostavlja svim entitetima koji vjeruju tom CA. Osnovne zadaće CA su generiranje i povlačenje certifikata.

- CP (engl. *Certificate Policy*) – skup pravila koja uključuju primjenjivost javnih ključeva certifikata za određenu zajednicu ili klasu aplikacija s osnovnim sigurnosnim zahtjevima.
- CPS (engl. *Certificate Practices Statement*) – prakse koje CA uključuje u izdavanje ključeva. Potrebno je definirati sve procese uključene u generiranje, izdavanje, upravljanje, pohranu, dostavljanje i povlačenje javnih ključeva.
- HSM (engl. *Hardware Security Modules*) – osnovna komponenta CA entiteta koja omogućava uspostavu povjerenja klijenta određenog CA, ali i svima koji ovise o certifikatima izdanim od krajnjih entiteta.
- Javni ključ certifikata (engl. *Public Key Certificates*) – služi kao potvrda povezivanja identiteta krajnjeg korisnika i njegovog javnog ključa. Sadrži dovoljno informacija kako bi drugi entitet mogao provjeriti i potvrditi vlasnika certifikata.
- Proširenje certifikata (engl. *Certificate Extensions*) – pruža dodatne informacije o certifikatu i dopušta njegovu uporabu za posebne potrebe organizacije. Informacije koje proširenje najčešće sadrži su politika, uporaba i povlačenje.
- RA (engl. *Registration Authorities*) – provodi određene zadatke u korist CA. Osnovna uloga je provjera identiteta krajnjeg entiteta i određivanje ovlasti za dodjelu javnog ključa. RA mora provesti politike i procedure definirane u CP i CPS kako bi ispitala zahtjev za certifikatom.
- Spremište certifikata (engl. *Certficate Depositories*) – služi za distribuciju certifikata na način da je svaki objavljeni certifikat spremljen u spremište koje kontrolira CA i RA. Tada je proces distribucije pojednostavljen jer je prilikom izdavanja novog certifikata potrebno samo obnoviti zapise u spremištu.
- Lista povučenih certifikata (engl. *Certificate Revocation List, CRL*) – popis svih povučenih i nevažećih certifikata koji obnavljaju RA i CA.[52]

Osim navedenih komponenti važno je spomenuti i službe koje imaju važnu ulogu u slučaju kompromitiranih certifikata, tj. onih koji su izdani lažno predstavljenoj osobi. Kako bi se to spriječilo na nivou države osnivaju se TRA (engl. *Trusted Registration Authority*) i TCA

[52] CARNet - CERT. Nedostaci PKI infrastrukture, n. dj., str. 12-13.

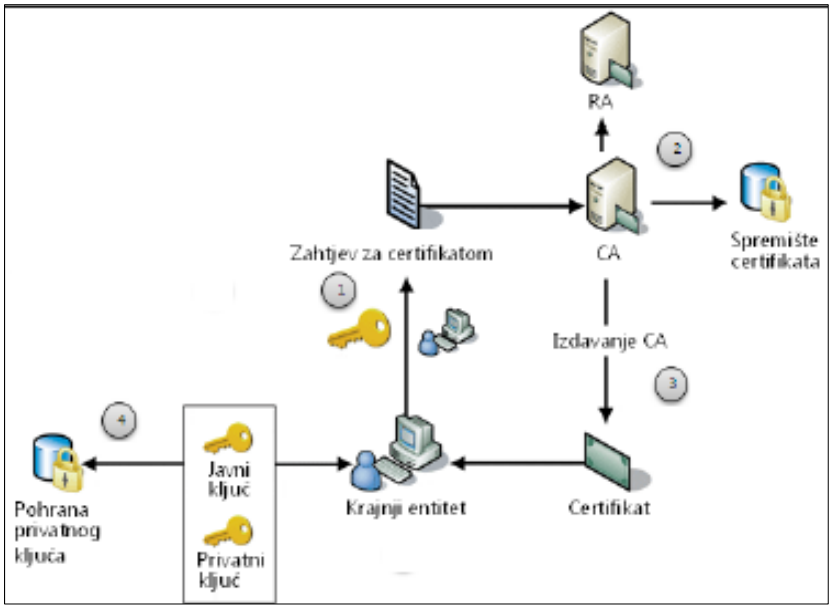
(engl. *Trusted Certificate Authority*) tijela kao institucije od najvišeg povjerenja. U slučaju kompromitiranja tajnog ključa korisniku se izdaje novi par ključeva i certifikat, a stari certifikat dospijeva na listu opozvanih certifikata.

Modeli

U implementaciji PKI infrastrukture postoje tri modela koja se mogu primijeniti, a to su hijerarhijski, distribuirani i izravni model. Hijerarhijski model predstavlja tipičnu implementaciju PKI-a te dopušta CA organizaciji potpisivanje certifikata krajnjih entiteta. Distribuirani model ne uključuje CA niti neki drugi oblik organizacije za provjeru identiteta te se primjenjuje kod PGP sustava. Posljednji je izravni model koji se primjenjuje unutar postupak temeljenih na kriptografiji tajnog ili simetričnog ključa te također ne uključuje središnji autoritet kao treću povjerljivu stranu.

Funkcionalnosti

Osnovne funkcije PKI infrastrukture su – kriptografija uporabom javnog ključa te izdavanje, provjera i povlačenje certifikata. Kriptografija uporabom javnog ključa uključuje generiranje, distribuciju, administraciju i kontrolu kriptografskih ključeva. Izdavanje certifikata (slika 16) provodi se u nekoliko koraka – prvenstveno je potrebno povezati javni ključ jednog korisnika sa samim entitetom, entitet zatim može poslati zahtjev za certifikatom, zahtjev provjeravaju CA i RA te vrše provjeru identiteta, CA formira certifikat i potpisuje ga privatnim ključem te zapisuje u spremište certifikata, dok krajnji entitet sprema privatni ključ i javni distribuira. Provjera certifikata utvrđuje postoji li certifikat i je li valjan, a povlačenje certifikata je potrebno ako je certifikat istekao ili je iz nekog razlog ugrožen.



Slika 16. Izdavanje certifikata[53]

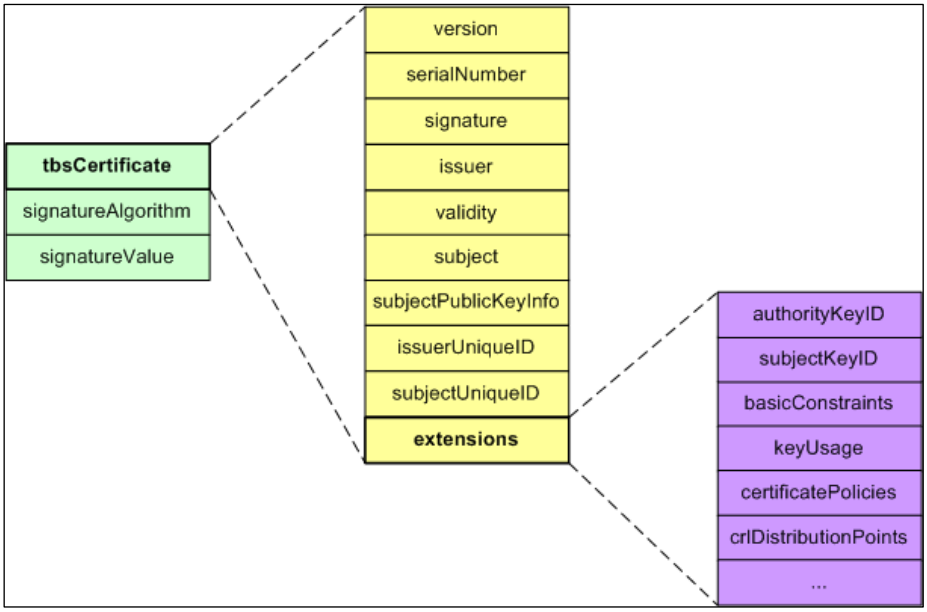
5.2. Digitalni certifikat

„Digitalni certifikat je potvrda u elektroničkom obliku koja predstavlja elektronički identitet u elektroničkim transakcijama te omogućuje sigurnu i povjerljivu komunikaciju internetom. Digitalnim certifikatom dokazuje se da je informacija primljena iz nekog izvora autentična. Certifikat predstavlja elektroničku identifikacijsku iskaznicu koja sadrži ključ i informacije o imatelju, svom vijeku trajanja, izdavatelju, te ovjeru, tj. potpis izdavatelja“.[54]

Digitalni certifikat omogućuje utvrđivanje povezanosti ključa kojeg posjeduje određeni entitet i pripadajućeg mu javnog ključa. U digitalnom certifikatu pohranjen je identitet entiteta zajedno s javnim ključem, a cijelu strukturu digitalno potpisuje treća strana od povjerenja. Certifikat se izdaje na određeno vrijeme, a njegova valjanost može biti ukinuta i prije isteka vremenskog roka na koji je certifikat izdan. Valjanost certifikata entitet provjerava provjerom elektroničkog potpisa, uz uvjet da postoji direktno povjerenje ili lanac povjerenja do autoriteta koji je ovjerio odgovarajući digitalni certifikat. Format digitalnog certifikata definiran je X.509 standardom, odnosno v3 inačica koja je preuzeta i u RFC dokumentima 2459 i 3280 – „*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*

[53] CARNet - CERT. Nedostaci PKI infrastrukture, n. dj., str.15.
[54] Fina. Digitalni cerifikati. URL: https://www.fina.hr/Default.aspx?art=10751(12.06.2018.)

Profile"[55]. X.509 standard također definira i strukturu digitalnog certifikata koja je prikazana na slici 17.



Slika 17. Prikaz strukture digitalnog certifikata[56]

Struktura certifikata ima tri obavezna polja:

- *tbsCertificate* – predstavlja niz koji sadrži ime entiteta kojem se izdaje digitalni certifikat i ime izdavača (CA), pripadajući javni ključ, period valjanosti;
- *signatureAlgorithm* – predstavlja polje koje sadrži identifikator algoritma koji središnji autoritet koristi za digitalno potpisivanje;
- *signatureValue* – polje koje sadrži elektronički potpis izračunat nad ASN.1 DER enkodiranom tbsCertificate strukturom korištenjem algoritma za digitalno potpisivanje.[57]

Ovo su informacije koje identificiraju osobu ili aplikaciju za koju se izdaje digitalni certifikat i izdavača tog istog certifikata.

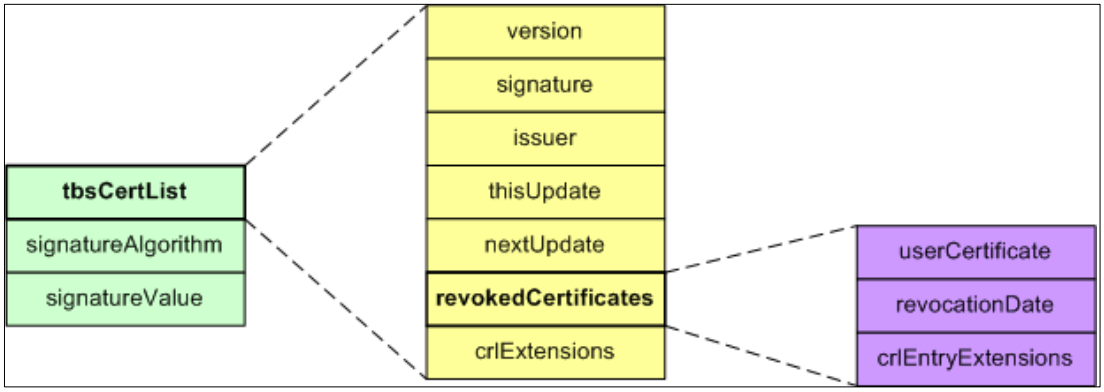
X.509 certifikat se tako sastoji o dva osnovna dijela: dio koji je potrebno „potpisati" – serijski broj, vrijeme valjanosti, ime izdavatelja, ime entiteta, javni ključ te osnovna polja sa zahtjevima; dio s potpisom – potpis preko svih dijelova koje treba „potpisati", koristi se za generiranje privatnog ključa

[55] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. URL: https://tools.ietf.org/html/rfc5280
[56] CARNet - CERT. Metode povlačenja digitalnih certifikata. 2005., str. 5. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-03-115.pdf
[57] CARNet - CERT. Metode povlačenja digitalnih certifikata, n. dj., str. 5.

Certifikati također zadovoljavaju određenu hijerarhijsku strukturu. Potpis podataka može se provjeriti pomoću ključa entiteta koji potpisuje podatke. Javni ključ povezan je s korisnikovim identitetom preko certifikata, što je moguće provjeriti upravo preko potpisa certifikata. Pritom se koristi javni ključ CA koji izdaje određeni certifikat. Javni ključ pohranjen je unutar CA certifikata koji je sloj više u hijerarhiji. Na vrhu te hijerarhije nalazi se korijenski CA entitet.

5.2.1. Metode povlačenja digitalnih certifikata: CRL i OCSP

Osnovne metode koje se primjenjuju u povlačenju digitalnih certifikata su CRL liste i OCSP protokol/zahtjevi. Ovo su također i metode koje se primjenjuju kao potpora dugotrajnom očuvanju digitalnih zapisa koji imaju pridodane elektroničke potpise ili digitalne pečate. CRL liste su jedan od uobičajenih načina povlačenja digitalnih certifikata. Mehanizam je opisan u već navedenim RFC dokumentima 2459 i 3280 – „*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*“. CRL lista predstavlja običnu datoteku koja se sastoji od niza serijskih brojeva. Svaki digitalni certifikat koji se nalazi na toj listi ima svoj jedinstveni broj i taj broj označava povučeni certifikat. CRL listu objavljuje vodeći CA u unaprijed definiranim vremenskim intervalima, a dosta rješenja omogućava i ručnu objavu. Klijentske aplikacije trebale bi dohvatiti CRL liste putem nekog komunikacijskog protokola, ali se pokazalo da to u praksi i nije baš tako, tj. aplikacije ne dohvaćaju liste i time ne rade provjeru je li certifikat povučen ili ne. S vremenom se pokazalo kako CRL liste imaju određene nedostatke zbog kojih je potrebno razviti novu metodu kojom će se barem neki od nedostataka ukloniti. Na slici 18. prikazana je struktura CRL liste koja se pohranjuje u ASN. 1 DER enkodiranom obliku, a na temelju tog enkodinga izračunava se i elektronički potpis cijele CRL liste.



Slika 18. Prikaz strukture CRL liste[58]

[58] CARNet - CERT. Metode povlačenja digitalnih certifikata, n. dj., str. 10.

Struktura CRL liste se sastoji od tri obavezna polja:

- *tbsCertList* predstavlja niz koji sadrži ime CA, datum izdavanja, datum izdavanja iduće CRL liste, popis povučenih certifikata i opcionalne CRL ekstenzije;
- *signatureAlgorithm* je polje koje sadrži identifikator algoritma koji je CA koristio za digitalno potpisivanje liste;
- *signatureValue* polje sadrži elektronički potpis izračunat nad ASN.1 DER enkodiranom tbsCertList strukturom korištenjem algoritma čiji je identifikator naveden u signature Algorithm polju[59].

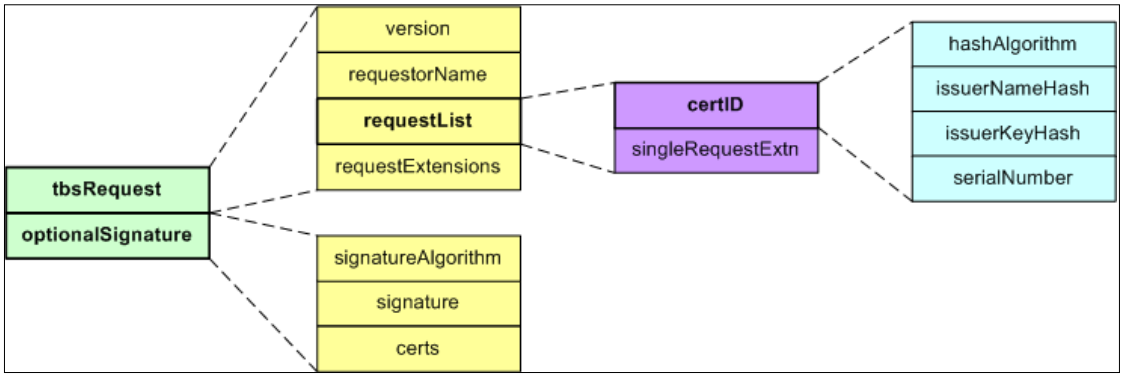
RFC 2459 opisuje i delta CRL mehanizam. Pri ovom mehanizmu koristi se diferencijalna metoda koja rješava jedan od osnovnih nedostataka CRL liste. Smanjuje veličinu liste koju klijentska aplikacija mora dohvaćati i skraćuje vrijeme potrebno za obradu kod aplikacija koje povučene digitalne certifikate pohranjuju lokalno. Delta CRL sadrži samo promjene koje su nastale između osnovne i trenutne CRL liste.

OCSP (engl. *Online Certificate Status Protocol*) predstavlja protokol koji je razvijen kako bi se zaobišli određeni nedostaci koji su uočeni uporabom CRL liste. To se ponajviše odnosi na obavljanje transakcija u realnom vremenu, za koje PKI infrastruktura s CRL listama nije dovoljno dobro rješenje.

Primjenom OCSP-a javlja se još jedan entitet u PKI arhitekturi – VA (engl. *Validation Authority*), tj. OCSP responder koji je odgovoran za provjeru valjanosti digitalnog certifikata. CA šalje revokacijske podatke OCSP responderu. Prilikom slanja mogu se koristiti CRL liste ili slanje može biti direktno. U svakom slučaju OCSP responder mora vjerovati u CA koji objavljuje revokacijske podatke. Dok klijent ili aplikacija mora vjerovati OCSP responderu. Primjenom respondera, klijent ne provjerava valjanost certifikata direktnom provjerom CRL liste, već šalje upit responderu. Tri su moguća odgovora OCSP respondera – „dobar“ (engl. *good*), „povučen“ (engl. *revoked*) ili „nepoznat“ (engl. *unknown*). Odgovor dobar nije znak da je certifikat valjan, nego samo potvrda da nije povučen u trenutku slanja upita. Kod OCSP-a također postoje određeni nedostaci koji će biti navedeni u poglavlju koje se bavi postojećim tehnologijama i pristupima u dugotrajnom očuvanju digitalnih zapisa s pridruženim elektroničkim potpisom.

[59] Ibid.

OCSP zahtjev formiran je također korištenjem ASN.1 notacije, a oblik zahtjeva ovisi o komunikacijskom protokolu koji se koristi.



Slika 19. Sadržaj OCSP zahtjeva[60]

Struktura OCSP sastoji se od dva osnovna polja:

- *tbsRequest* – sadrži informacije o inačici protokola i zahtjev(e) za verifikacijom digitalnog certifikata;
- *optionalSignature* – sadrži opcionalni digitalni popis zahtjeva.

Posebno je važna *requestList* koja sadrži popis zahtjeva za verifikacijom digitalnih certifikata, a sastoji se od dva polja:

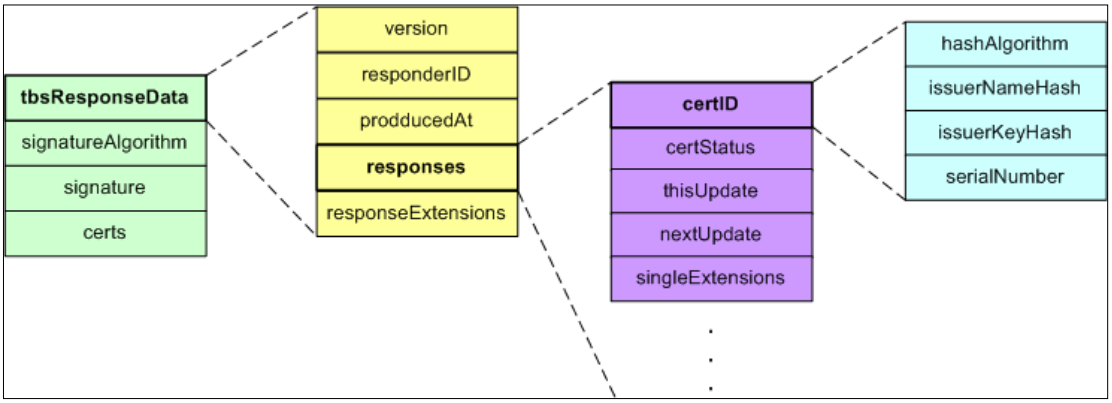
- *CertID* – polje koje se sastoji od četiri polja koja jednoznačno određuju digitalni certifikat:
  - *hashAlgorithm* – sadrži identifikator algoritma koji se koristi za računanje hash vrijednosti u zahtjevu,
  - *issuerNameHash* – sadrži hash vrijednost ASN.1 DER enkodiranog issuerName polja digitalnog certifikata koji se verificira,
  - *issuerKeyHash* – sadrži hash vrijednost ASN.1 DER enkodiranog javnog ključa izdavača digitalnog certifikata koji se verificira,
  - *serialNumber* – sadrži jedinstveni serijski broj digitalnog certifikata;
- *singleRequestExtensions* – sadrži opcionalne ekstenzije vezane uz pojedini zahtjev.

OCSP odgovor je odgovor na OCSP zahtjev te njegov oblik također ovisi o komunikacijskom protokolu koji se koristi, a sam zahtjev oblikovan je u ASN.1 enkodiranu strukturu. OCSPResponse struktura sastoji se od dva osnovna polja:

[60] CARNet - CERT. Metode povlačenja digitalnih certifikata, n. dj., str. 12.

- *responseStatus* – označava status OCSP odgovora, a ako je status pogreška responseBytes polje se ne postavlja. Ovo polje može poprimiti nekoliko vrijednosti:
  - *successful* – odgovor je uspješan i postavljeno je responseBytes polje,
  - *malfoormedRequest* – pogrešno oblikovan zahtjev,
  - *internal Error* – interna pogreška kod izdavača,
  - *sigRequired* – OCSP responder zahtijeva elektronički potpis OCSP zahtjeva,
  - *unauthorized* – OCSP zahtjev je neovlašten;
- *responseBytes* – sastoji se od dva polja, a to su responseType i response[61].

Obični OCSP responder će generirati OCSP odgovor tipa BasicOCSPResponse (slika 20).



Slika 20. Struktura OCSP odgovora[62]

Aplikacije koje primjenjuju OCSP verifikaciju digitalnih certifikata moraju podržavati provjeru *extendedKeyUsage* polja certifikata OCSP respondera te odbaciti OCSP odgovor ako digitalni certifikat kojim je potpisan ne ispunjava određene uvjete (npr. digitalni certifikat je certifikat CA koji je objavio certifikat čija verifikacija se traži u zahtjevu). Osim toga, CA mora i definirati na koji način OCSP klijent može provjeriti status certifikata OCSP respondera.

[61] CARNet - CERT. Metode povlačenja digitalnih certifikata, n. dj., str. 13.
[62] CARNet CERT. Metode povlačenja digitalnih certifikata, n. dj., str. 14.

6. Istraživanje – analiza Fina okruženja

S obzirom da je Fina prvi davatelj usluga certificiranja u Hrvatskoj koji izdaje digitalne certifikate za javnost te je upisana u *Evidenciju davatelja usluga certificiranja u Hrvatskoj*, bilo je logično analizirati upravo sustav certificiranja koji provodi Fina. Osim toga, Fina je i jedan od partnera projekta pod nazivom *TRUSTER Preservation Model (31) - Model for Preservation Of Trustworthiness of Digitally Signed, Timestamped and /or Seald Digital Records*[63] koji je samo jedan u nizu projekata koji se provode u sklopu međunarodnog *InterPARES Trust* projekta. Ovaj projekt bavi se upravo pitanjem *„Kako dugotrajno očuvati digitalne zapise koji imaju pridružene elektroničke potpise, certifikate, vremenske žigove ili elektroničke pečate, a da takav digitalni zapis u procesu dugotrajnog očuvanja zadrži osnovne karakteristike, dakle autentičnost, pouzdanost, integritet i upotrebljivost?"*

U ovom interdisciplinarnom istraživačkom radu provedena je analiza sadržaja. Analizirana je usluga certificiranja koju pruža Fina, a dostupni su i brojni dokumenti koji će korisniku olakšati razumijevanje cijelog procesa izdavanja digitalnog certifikata. Također je objašnjeno koja su prava i obveze osobe kojoj je potrebna usluga certificiranja, a koja Fine kao davatelja usluge certificiranja.

6.1. Analiza usluge certificiranja u Fini

E-poslovanje danas predstavlja jednostavan način komuniciranja između poslovnih partnera elektroničkim putem. Međutim, elektroničko poslovanje ima i brojne rizike koji su lako ostvarivi bez napredne elektroničke zaštite i platforme povjerenja. Fina omogućuje smanjenje potencijalnih rizika zato što su sve usluge koje Fina nudi i razvija u sferi e-poslovanja usklađene sa zakonima o elektroničkom potpisu, elektroničkoj trgovini, elektroničkoj ispravi, zakonom o zaštiti osobnih podataka te svjetskim i europskim poslovnim praksama. Uvođenjem same kriptografije javnog ključa (PKI) te zakonskim reguliranjem elektroničkog potpisa nestale su zapreke za korištenje interneta i e-poslovanja. Zapravo je omogućena potpuna eliminacija papira uz znatnu uštedu vremena u poslovnoj komunikaciji.[64]

Fina kao *Trusted Third Party* (*TTP*) ili povjerljiva treća strana jamči ispravan i nepristran rad sukladan javno objavljenim pravilnicima rada. U elektroničkom svijetu TTP je kao osobna

[63] TRUSTER Preservation Model (31) - Model for Preservation Of Trustworthiness of Digitally Signed, Timestamped and /or Seald Digital Records. URL: https://interparestrust.org/trust/about_research/studies. (16.06.2018.).
[64] Fina. Elektroničko poslovanje. URL: http://www.fina.hr/Default.aspx?sec=940. (17.06.2018.)

iskaznica, tj. organizacija koja će potvrditi i garantirati identitete korisnika. To je organizacija kojoj se može vjerovati, koja svojim radom, veličinom i stabilnošću i utjecajem ulijeva povjerenje kod sudionika e-poslovanja. Svi sudionici se mogu s povjerenjem obratiti trećoj strani i prihvaćati njezine garancije o identitetu sudionika komunikacije. Kao davatelj usluge certificiranja upisan u Evidenciju davatelja usluga certificiranja u Hrvatskoj, Fina jedina u Hrvatskoj posjeduje dozvolu za izdavanje kvalificiranih digitalnih certifikata.

Pored zaštite integriteta podataka i autentifikacije potpisnika u e-poslovanju često je potrebno na siguran način označiti vrijeme u kojem su podaci nastali, bili potpisani ili bili uspješno validirani. Vremenski žig kojeg izdaje FINA TTP osigurava pouzdan dokaz postojanja tih podataka u određenom vremenu. Tradicija, obavljanje pouzdanih usluga i orijentiranost prema pružanju elektroničkih usluga za poslovne subjekte i tijela javne vlasti glavni su razlozi zbog kojih je Fina prepoznata kao treća strana od povjerenja u e-poslovanju i e-upravi.

Fina kao *Time Stamp Authority* (*TSA*) je pružatelj usluge/servisa ovjere elektroničkog potpisa. TSA vremenskim žigom ovjerava potpis potpisnika. Vremenskim se žigom potvrđuje da su podaci i elektronički potpis postojali prije izdavanja (stavljanja) vremenskog žiga. Vremenska ovjera je podrška za pravno valjanu upotrebu kvalificiranog elektroničkog potpisa. Servise vremenske ovjere je moguće primijeniti u bilo kojoj aplikaciji koja zahtijeva dokaz da je određeni podatak postojao prije nekog određenog vremena. Dakle, servisi vremenske ovjere osiguravaju pouzdanost elektroničkog potpisa i poslije isteka valjanosti/opoziva certifikata potpisnika/subjekta. Vremenska ovjera može se koristiti za zaštitu dugotrajnih elektroničkih potpisa. TSA je davatelj usluga vremenske ovjere, koja izdaje pouzdane potvrde o vremenu neke transakcije, sukladno Zakonu o elektroničkom potpisu RH, direktivama EU o kvalificiranom elektroničkom potpisu i vremenskoj ovjeri.[65]

Kao i mnogi drugi izdavatelji kvalificiranih certifikata, Fina se nalazi na *EU Trusted listi*.[66] Fina kao *Archiving Authority* je pružatelj usluge sigurne elektroničkog arhiva. Uslugom Arhiviranja FINA TTP mora osigurati sigurno arhiviranje dokumenata, odnosno transakcija. TTP primitak u arhivu se ovjerava vremenskim žigom i mora svim sudionicima osigurati pristup arhivu. Upravljanje arhivskom građom predstavlja uslugu kojom TTP osigurava "izvadak iz arhiva" na zahtjev sudionika, izvadak može sadržavati sve informacije ili samo dio informacija u transakciji/dokumentu. Izvadak digitalno potpisuje TTP, odnosno Fina.

[65] Isto.
[66] Trusted List Croatia. Trust service providers. URL: https://webgate.ec.europa.eu/tl-browser/#/tl/HR . (22.09.2018.)

Kroz daljnju analizu predstavit će se i pojasniti Finina produkcijska okolina za izdavanje digitalnih certifikata i naprednih vremenskih žigova (od kojih dijelova se sastoji, vrste certifikata, napredni vremenski žig, ...), a također će biti riječi i o aplikativnim rješenjima koja su nužna za elektroničko potpisivanje dokumenta, a Fina ih je razvila nekoliko za svoje poslovne subjekte.

Na slici 21 i 22 prikazano je sučelje web stranice Fine. Klikom na „Digitalni certifikati“ korisniku će se otvoriti novo sučelje koje sadrži sve potrebne informacije o Fininoj produkcijskoj okolini. Prvi dio sadrži sve informacije o digitalnim certifikatima i naprednom vremenskom žigu koji Fina izdaje, drugi i treći dio su posebno bitni za korisnika jer pružaju informacije koje korake je potrebno poduzeti kako bi korisnik dobio Finin digitalni certifikat i gdje se uopće certifikati primjenjuju. Četvrti dio obuhvaćaju „Obavijesti” gdje se objavljuju sve važne i aktualne promjene i događanja vezana uz digitalne certifikate, dok se peti dio odnosi na „Često postavljana pitanja” gdje korisnici mogu pronaći odgovore na većinu nedoumica i nejasnoća.

Slika 21. Sučelje web stranice Fine – Digitalni certifikati[67]

[67] Fina. Poslovni subjekti/građani. URL: http://www.fina.hr/Default.aspx?sec=1714.

Slika 22. Sučelje web stranice Fine – Digitalni certifikati[68]

Finina produkcijska okolina za izdavanje digitalnih certifikata i naprednog vremenskog žiga

Na slici 23 prikazana je Finina produkcijska okolina za izdavanje digitalnih certifikata i naprednog vremenskog žiga. Fina je od 7. prosinca 2015. godine počela izdavati digitalne certifikate i napredne vremenske žigove na novoj dvorazinskoj arhitekturi Fininih CA-ova.

Kao glavne karakteristike nove produkcijske okoline mogu se izdvojiti:

- dvorazinska arhitektura certifikacijskih tijela (CA-ova);
- korištenje sigurnijih kriptografskih algoritama i duljih kriptografskih ključeva;
- novi servis za provjeru statusa certifikata;
- servis izdavanja naprednih vremenskih žigova[69].

Važno je napomenuti da su svi digitalni certifikati i napredni vremenski žigovi koje Fina izdaje na novoj produkcijskoj okolini usklađeni s važećim EU i međunarodnim normama iz

[68] Fina. Poslovni subjekti/građani. URL: http://www.fina.hr/Default.aspx?sec=1714.
[69] Fina. Fina PKI sustav. URL: http://www.fina.hr/Default.aspx?sec=1799. (19.06.2018.).

područja izdavanja digitalnih certifikata i vremenskih žigova te normama iz područja elektroničkog potpisa.

Nova produkcijska okolina značajna je zbog dvorazinske arhitekture Fininih produkcijskih certifikacijskih tijela. Novi sustav za izdavanje certifikata sastoji se od novog korijenskog certifikacijskog tijela (engl. *Root Certification Authority, Root CA*) koje izdaje certifikate za subordninirana certifikacijska tijela (engl. *Subordinate Certification Authority, Subordinate CA*), a subordinirana certifikacijska tijela izdaju certifikate krajnjim korisnicima. Stoga u novoj produkciji digitalnih certifikata Fina ima jedno korijensko certifikacijsko tijelo (*Fina Root CA*) i dva subordinirana certifikacijska tijela (*Fina RDC 2015* i *Fina RDC TDU 2015*). CA je certifikat kojeg je izdalo i potpisalo certifikacijsko tijelo (CA), a koji sadrži javni ključ i naziv CA koji je izdao certifikat. Na web stranici Fine dostupan je i dokument pod nazivom „Uputa za instalaciju Fina Root CA i Subordiniranih digitalnih certifikata".

Fina Root CA preuzeo je ulogu prijašnjeg FINA RDC CA te izdaje kvalificirane, normalizirane i *lightweight* certifikate za fizičke osobe (građane), prilikom čega je riječ o osobnim certifikatima, zatim za fizičke osobe povezane s poslovnim subjektom te su radi o poslovnim certifikatima i na kraju za IT opremu povezanu s poslovnim subjektom što su onda poslovni certifikati za IT opremu. Fina RDC-TDU 2015 CA preuzeo je ulogu prijašnjeg FINA RDC-TDU CA te izdaje kvalificirane i normalizirane certifikate državnim dužnosnicima i zaposlenicima u tijelima državne uprave, dok je Fina Root CA izdao i potpisao certifikate za subordinirane Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove. Fina za izračun sažetka prilikom potpisivanja certifikata, CRL i vremenskih žigova koristi algoritam SHA-246, RSA. Što se tiče duljina kriptografskih RSA parova ključeva koriste se CA parovi ključeva duljine 4096 bitova, RSA i korisnički parovi ključeva duljine 2048 bitova, RSA. Fina Root CA certifikat je root CA za sve Finine produkcijske certifikate. Root CA nosi i naziv „sidro povjerenja" (engl. *trust anchor*) Finine dvorazinske arhitekture te izdaje i potpisuje certifikate za Finine subordinirane CA-ove. Fina Root certifikat sadrži RSA javni ključ duljine 4096 bita. Certifikati za Fina RDC 2015 i Fina RDC-TDU 2015 sadrže RSA javni ključ duljine 4096 bitova. Kasnije u analizi bit će detaljnije opisani root, subordinirani i korisnički certifikati. Root i subordinirani certifikati su detaljnije opisani u dokumentu „Opća pravila davanja usluga certificiranja Fina Root CA", dok su korisnički certifikati detaljnije objašnjeni u dokumentu „Opća pravila davanja usluga certificiranja". Tablica 2 prikazuje osnovne vrste digitalnih certifikata u novoj dvorazinskoj okolini, tj. skraćenicu, puni naziv i objašnjenje.

Tablica 2. Vrste digitalnih certifikata u novoj dvorazinskoj okolini

Skraćenica	Puni naziv	Objašnjenje
Fina Root CA	Korijenski certifikat izdavatelja	Certifikat kojim su subordinirani certifikati izdavatelja
Fina RDC 2015	Subordinirani CA certifikat	Certifikat kojim su potpisani RDC certifikati
Fina RDC-TDU 2015	Subordinirani CA certifikat	Certifikat kojim su potpisani TDU certifikati

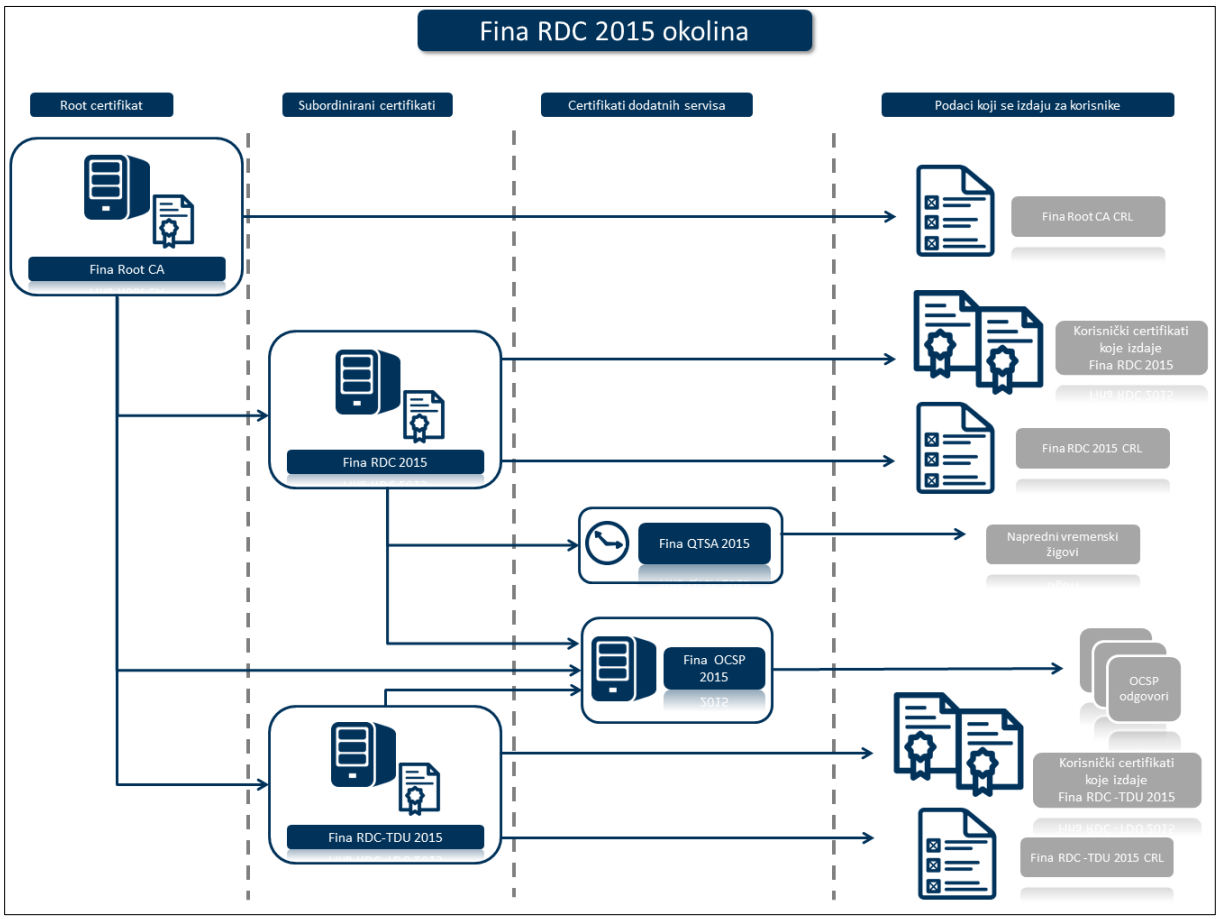
U sklopu Finine produkcijske okoline potrebno je još pojasniti i postojeće servise, a to su *Fina OCSP*, tj. uslugu za online provjeru statusa certifikata te *Fina QTSA 2015*, tj. servis za izdavanje naprednih vremenskih žigova.

OCSP servis temelji se na klijent-server modelu u kojem OCSP klijent šalje OCSP serveru upit o statusu certifikata, a OCSP servis vraća odgovor o statusu. Finin OCSP servis pod nazivom Fina OCSP 2015 pruža informacije o statusima certifikata koji su izdani od Fina Root CA, Fina RDC 2015 i Fina RDC-TDU 2015. Adresa koja omogućuje pristup servisu nalazi se u *Authority Information Access* ekstenziji svakog Fininog certifikata, dok je sam rad ovog servisa usklađen s preporukom IETF RFC 6960. Preporuka IETF RFC 6960 predstavlja dokument koji određuje protokol koji je jako koristan prilikom utvrđivanja trenutnog statusa digitalnog certifikata, a da prilikom utvrđivanja nije potrebno konzultirati CRL.[70] Fina OCSP 2015 servis potpisuje odgovore RSA privatnim ključem duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA. Pored korištenja Fina OCSP 2015 servisa, provjera statusa certifikata može se i dalje obavljati dohvatom CRL. Preporuka je da se za provjeru statusa certifikata koristi OCSP servis, a provjera statusa dohvatom CRL može se koristiti kao alternativna metoda provjere u slučaju nedostupnosti OCSP servisa.

Fina je također uspostavila i *Fina QTSA servis* koji izdaje napredne vremenske žigove sukladno zakonskoj regulativi iz područja elektroničkog potpisa. Početkom rada ovo servisa s radom je prestao prijašnji servis koji je imao istu zadaću, „Servis vremenske ovjere TSA1". Mogućnost korištenja Fina QTSA 2015 servisa imaju autorizirani korisnici koji se na servis prijavljuju Fininim digitalnim certifikatom. Certifikat za Fina QTSA 2015 izdao je Fina RDC 2015, a napredni vremenski žigovi potpisuju se RSA privatnim ključem Fina QTSA 2015 servisa, duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.[71] Podaci o certifikatu Fina QTSA 2015 kojim ovaj servis potpisuje napredne vremenske žigove kao i

[70] Fina. RFC Editor. URL: https://www.rfc-editor.org/info/rfc6960. (19.06.2018.).
[71] Fina. Fina PKI sustav. URL: http://www.fina.hr/Default.aspx?sec=1799. (19.06.2018.).

podaci o profilu vremenskih žigova koje izdaje ovaj servis dostupni su u „Općim pravilima davanja usluga izdavanja naprednih vremenskih žigova".



Slika 23. FINA RDC 2015 okolina[72]

Fina PKI sustav

Za potrebe pružanja usluge certificiranja Fina preko Registra digitalnih certifikata vodi infrastrukturu javnog ključa (engl. *Public Key Infrastructure*, *PKI*). Osnovna namjena PKI-a je zaštićena komunikacija nesigurnim kanalima.[73] Infrastrukturu vodi s već navedenim certifikacijskim tijelima (CA), a to su Fina Root CA, Fina RDC CA 2015 za građane i poslovne subjekte, Fina RDC-TDU CA 2015 za tijela državne uprave, Fina Demo Root CA za potrebe testiranja i Fina Demo CA 2014 za potrebe testiranja. PKI infrastruktura omogućuje uporabu kriptografije javnog ključa u poslovnim procesima. Zbog svoje uloge jako je važna

[72] Ibid.
[73] Ibid.

za elektroničke servise koji se koriste preko interneta, odnosno intraneta. Elektroničke transakcije koje su zaštićene primjenom PKI-a bazirane na digitalnom certifikatu i elektroničkom potpisu zadovoljavaju osnovne zahtjeve, a to su autentikaciija, integritet, tajnost i neporecivost. Ono što PKI tehnologija omogućuje je tajnost elektroničkih transakcija, provjera identiteta, integritet informacija, sigurniji procesi razmjene podataka, pristup javnosti državnim i drugim e-servisima, prihvat različitih elektronički ispunjenih dokumenata, sigurna komunikacija sa zaposlenicima na udaljenim lokacijama, razmjena tajnih podataka i smanjenje operativnih troškova uvođenjem elektroničkog poslovnog procesa.[74]

Vrste digitalnih certifikata koje izdaje Fina

Certifikati koje izdaje Fina usklađeni su s normom *X.509 v3*[75], a što onda omogućuje korištenje Fininih certifikata u svim rješenjima. Certifikat koji je usklađen s ovom normom sadrži informacije o identitetu za koji je certifikat izdan, ali i o identitetu koji je izdao certifikat, tj. povjerljivoj trećoj strani. Standardne informacije koje sadrži X.509 certifikat su verzija X.509 norme koja se primjenjuje na certifikat, serijski broj, informacija o algoritmu, naziv CA, vrijeme trajanja certifikata, ime korisnika kojem je izdan certifikat, javni ključ koji se veže uz korisnika kojem je izdan certifikat i na kraju ekstenzije, koje nisu obvezne.

Kao što je već navedeno, za elektroničko potpisivanje potrebno je uz aplikativno rješenje imati i digitalni certifikat. Dvije osnovne vrste certifikata prema namjeni koje izdaje Fina su autentifikacijski (normalizirani certifikat) i potpisni (kvalificirani certifikat). Svrha pojedinog certifikata objašnjena je u tablici 3.[76]

Tablica 3. Certifikati prema namjeni

Autentifikacijski (normalizirani) certifikat	koristi se za autentifikaciju, odnosno enkripciju (zaštitu tajnosti podataka), te za njihovu kombinaciju. Taj certifikat i uporaba ključa od strana uključenih u e-poslovanje osigurava autentičnost, cjelovitost, izvornost i tajnost. Može se izdati na FINA e-kartici ili USB tokenu ili kao certifikat za aplikacije koji se instalira na serveru na kojemu se nalazi aplikacija.
Potpisni (kvalificirani) certifikat	koristi se za elektroničko potpisivanje dokumenata ili transakcija naprednim elektroničkim potpisom u

[74] Ibid.
[75] National Security Agency; Queensland University of Technology. X.509v3 Certificates for Secure Shell Authentication. 2011. URL: https://tools.ietf.org/html/rfc6187. (04.07.2018.).
[76] Fina. e-Potpis. URL: http://www.fina.hr/Default.aspx?sec=960. (20.06.2018.).

	skladu sa Zakonom o elektroničkom potpisu. Jamči autentičnost, cjelovitost i izvornost te priskrbljuje i neporecivost zamjenjujući u cijelosti vlastoručni potpis ili vlastoručni potpis i otisak pečata. Obzirom da je vezan za osobu, izdaje se na FINA e-kartici ili USB tokenu.

Osim podjele prema namjeni, certifikati se mogu podijeliti i prema subjektu certificiranja. U tom slučaju certifikati se dijele na certifikate za poslovne subjekte (poslovni certifikati), certifikate za fizičke osobe/građane i certifikate za državna tijela uprave (TDU).

Certifikate za poslovne subjekte izdaje Fina RDC CA. Poslovni subjekt može zatražiti jednu od dvije glavne vrste certifikata od kojih svaki ima nekoliko podvrsta.

1. Certifikat za fizičku osobu povezanu s poslovnim subjektom/ organizacijom:
    - certifikat na kripto uređaju (Fina e-kartica ili USB token),
    - poslovni soft certifikat,
    - poslovni soft certifikat (engl. *Lightweight Certificate Policy*, *LCP*).
2. Certifikat za IT opremu povezanu s poslovnim subjektom/organizacijom:
    - SSL certifikat za web poslužitelj,
    - certifikat za aplikaciju.[77]

Poslovni certifikati za fizičke osobe unutar pojedinog poslovnog subjekta, a koji se izdaju na kripto uređaju, mogu biti normalizirani certifikati ili kvalificirani certifikati. Namjena normaliziranih je elektronički potpis, jaka autentifikacija i enkripcija, a namjena kvalificiranih je isključivo za napredni elektronički potpis. Elektronički potpis se izrađuje korištenjem normaliziranog certifikata, a napredni elektronički potpis korištenjem kvalificiranog certifikata i kripto uređaja koji posjeduje potpisnik certifikata. Poslovni soft certifikati su zapravo normalizirani certifikati standardne razine sigurnosti, a namijenjeni su fizičkim osobama unutar poslovnog subjekta za elektronički potpis i autentifikaciju na elektroničke servise koji prilikom pristupa zahtijevaju standardnu razinu sigurnosti, a isto tako mogu služiti i za enkripciju podataka. Ovakvi certifikati mogu se pohraniti na računalo ili na mobilni uređaj korisnika. Osim toga, usklađeni su s već spomenutom najzastupljenijom normom za

[77] Fina. Certifikati za poslovne subjekte. URL: http://www.fina.hr/Default.aspx?art=10752. (21.06.2018.).

digitalne certifikate X.509 v3, preporukom RFC 5280 koja regulira uporabu navedene norme, te s normom HRN ETSI/EN 319 411-3 koja regulira pravila za izdavanje certifikata za elektronički potpis. Zbog takve usklađenosti, ove certifikate je moguće koristiti na svim šire zastupljenim platformama.

Poslovni soft certifikat (LCP) je certifikat standardne razine sigurnosti čiji način izdavanja zadovoljava uvjete za *lightweight* certifikate. Sukladno tome, za izdavanje ovakvih certifikata identifikacija se provodi posredno. Identifikacija potpisnika i poslovnog subjekta te utvrđivanje njihove povezanosti, obavlja se metodom koja ne zahtjeva fizičku identifikaciju, a ostvaruje povjerenje u identitet potpisnika i poslovnog subjekta u skladu s pravilima za izdavanje LCP certifikata. S obzirom na to da se pri registraciji ne vrši fizička identifikacija potpisnika, ovakav je certifikat pogodan za elektroničke servise koji ne zahtijevaju razinu autentifikacije korisnika i potpisa kakvu pružaju normalizirani i kvalificirani certifikat, ali koja je dovoljna za elektronički potpis i koja omogućuje razinu autentifikacije višu od one koju pruža korištenje korisničkog imena i lozinke. Ovaj certifikat može služiti i za enkripciju podataka.[78]

Kada je riječ o certifikatima za IT opremu povezanu s poslovnim subjektom, postoje SSL certifikat za web poslužitelje i aplikacijski certifikat. SSL certifikat izdaje se za web poslužitelj i služi za uspostavu sigurnog komunikacijskog kanala. Pomoću takvog certifikata može se identificirati poslužitelj na mreži i kriptirati sadržaj na komunikacijskom kanalu. Fina razlikuje SSL certifikat srednje i visoke razine sigurnosti. Kod certifikata srednje sigurnosti, ovisno o zahtjevima web poslužitelja, skrbnik certifikata može generiranje para ključeva za web poslužitelj obaviti na svojoj lokaciji ili zatražiti da par ključeva poslužitelj generira Fina.

Fizička osoba može zatražiti osobni certifikat srednje razine sigurnosti koji je na kripto uređaju ili osobni soft certifikat. Prvi certifikat je kvalificirani certifikat koji je izdaje na kripto uređaju, a to može biti Fina e-kartica ili USB token. Namijenjen je za pristup e-servisima za građane koji će ih koristiti za vlastite potrebe, a koji zahtijevaju autentifikaciju, elektronički ili napredni elektronički potpis. Osobni soft certifikat je certifikat standardne razine sigurnosti, a namijenjen je za vlastite potrebe. Pogodan je za autentifikaciju na elektroničke servise namijenjene onima koji prilikom pristupa zahtijevaju određenu razinu sigurnosti. Mogu se pohraniti na računalu ili mobilnim uređajima. Također moraju biti usklađeni s već prije navedenim normama.

[78] Ibid.

Za izdavanje certifikata za državne dužnosnike i zaposlenike u tijelima državne uprave zadužena je Fina RDC-TDU CA. Izdani certifikati su vlasništvo TDU i pod nadzorom su potpisnika, tj. korisnika certifikata, a izdaju se na kripto uređaja.

Fina aplikativna rješenja za elektroničko potpisivanje

Ono što je važno upravo za sigurnost i povjerenje u elektroničkom poslovanju je elektronički potpis koji osigurava vjerodostojnost izvora i zaštitu integriteta sadržaja. Uz digitalne certifikate za elektroničko potpisivanje potrebno je imati i aplikativno rješenje. Fina je razvila nekoliko aplikativnih rješenja koja omogućuju elektroničko potpisivanje dokumenta. Moguće je potpisivanje jednog ili više dokumenata, što ovisi o potrebama klijenta. Fina je tako razvila aplikaciju pod nazivom „*Web e-Potpis*" [79] koja omogućuje elektroničko potpisivanje dokumenta, provjeru valjanosti potpisa na elektronički potpis anim dokumentima, enkripciju, dekripciju, ovjeru vremenskim žigom te dugoročnu validaciju (što zahtijeva ugradnju CRL liste ili OCSP servisa).

Ova aplikacija dostupna je putem interneta, stoga ju nije potrebno instalirati na računalo. Korisnikom aplikacije može se postati jedino ako klijent ima Finine digitalne certifikate na FINA e-kartici/USB tokenu ili CoBranded kartici/tokenu banke s kojom Fina ima ugovor o poslovnoj suradnji, a također je potrebna i registracija za korištenje aplikacije. Registracija se vrši online, prijavom na aplikaciju i korištenjem digitalnog certifikata. Nakon što se korisnik prijavi u aplikaciju potrebno je popuniti podatke za registraciju. Nakon toga korisniku će stići e-mail koji sadrži potvrdu o uspješnoj prijavi, nakon čega može početi koristiti aplikaciju. Na web stranici je dostupan dokument pod nazivom „Opći uvjeti korištenja aplikacije Web e-Potpis" koji sadrži osnovne informacije o tehničkim uvjetima koje bi korisnik trebao osigurati za korištenje aplikacije. Osim dokumenta, dostupni su i video isječci koji mogu biti od velike pomoći korisniku prilikom potpisivanja dokumentacije kroz aplikaciju. Ukoliko korisnik želi samo provjeriti valjanost potpisa na elektronički potpis anim dokumentima, tj. verificirati potpis, nije mu potreban digitalni certifikat niti registriranje kako bi mogao koristiti aplikaciju. Za verifikaciju potpisa postoji posebna aplikacija te se sama verifikacija ne naplaćuje. Ukoliko se verifikacija vrši bez digitalnog certifikata, preporučeno je instalirati verifikacijski root certifikat koji se može besplatno preuzeti preko web stranice Fine. Instalacijom root certifikata uspostavit će se povjerenje u certifikate kojima je dokument potpisan, a ukoliko

[79] Fina. Web e-Potpis. URL: https://www.fina.hr/Default.aspx?sec=960. (22.06.2018.).

korisnik ne instalira root certifikat, prilikom svake verifikacije dobit će poruku da je izdavatelj certifikata nepoznat i postavit će se pitanje vjeruje li korisnik tom certifikatu.

Osim ove aplikacije, Fina je razvila i klijentsko rješenje za potpisivanje u AdES potpisnim formatima. Klijentsko rješenje podrazumijeva komponentu za korištenje u Web aplikacijama za potpisivanje gdje potpisivanje naprednim elektroničkim potpisom provode krajnji korisnici. Riječ je o rješenju koje se koristi za potpisivanje podataka naprednim elektroničkim potpisom, dakle, rješenje je pogodno za poslovni proces u kojemu na dokumentu treba implementirati napredni elektronički potpis. Ovdje je važno spomenuti eIDAS uredbu prema kojoj elektroničke usluge koje priznaju tijela javnog sektora trebaju zadovoljiti zahtjeve za kvalificirana sredstva za izradu elektroničkih potpisa te se sukladno tome donosi provedbena odluka komisije (EU) 2015/1506 od 8. rujna 2015. godine o utvrđivanju specifikacija koje se odnose na formate naprednih elektroničkih potpisa i naprednih pečata. U tom dodatku propisuju se AdES formati za izradu naprednih elektroničkih potpisa i pečata, odnosno skupinu standarda CadES, XadES i PadES Baseline profile. Od dana stupanja na snagu Uredbe, sva rješenja za pružanje elektroničkih usluga trebala bi zadovoljavati uvjete iz Specifikacija koje se odnose na formate naprednih elektroničkih potpisa i naprednih pečata kako bi bila usklađena s drugim rješenjima na unutarnjem tržištu EU. Upravo zbog specifikacija koje su navedene u Uredbi, Fina je morala razviti ovakvo rješenje.

Posljednje od aplikativnih rješenja je samostojeća aplikacija za „e-Potpis“[80]. Namijenjena je izradi i provjeri elektroničkog potpisa na datotekama različitih formata te njihovoj enkripciji i dekripciji. Putem ove aplikacije moguće je interaktivno potpisivanje pojedinačnih dokumenata i automatski način rada za potpisivanje velike količine dokumenata. Nakon što se definiraju ulazni i izlazni direktoriji u kojima se pohranjuju dokumenti na kojima je potrebno implementirati elektronički potpis.

Opoziv, suspenzija, reaktivacija i oporavak certifikata

Korisnik može zatražiti opoziv, suspenziju, reaktivaciju ili oporavak certifikata.

Opoziv certifikata je postupak kojim certifikat nepovratno postaje nevažećim.

Zahtjev za opoziv certifikata podnosi se:

- u slučaju kompromitiranja privatnog ključa ili ako se pojavi osnovana sumnja da je privatni ključ kompromitiran,

[80] Fina. e-Potpis, n. dj.

- ako se pojavi sumnja da korisnički kriptografski uređaj, odnosno privatni ključ ili aktivacijski podaci nisu više u jedinstvenom posjedu potpisnika,
- u slučaju gubitka ili trajne nedostupnosti privatnog ključa,
- ako pripadajuća osoba više nije povezana s poslovnim subjektom,
- ako neka od informacija sadržana u certifikatu više nije točna,
- u slučajevima kada to nalaže zakon ili drugi potpis.

Suspenzija certifikata je postupak kojim certifikat privremeno, na vrijeme od najdulje 60 dana, postaje nevažećim. Ukoliko se sumnja koja je bila razlog za suspenziju potvrdi, korisnik je dužan zatražiti opoziv certifikata, a ako se sumnja opovrgne, korisnik može zatražiti reaktivaciju certifikata.

Reaktivacija certifikata je postupak ponovnog aktiviranja suspendiranog certifikata nakon prestanka postojanja razloga za suspenziju.

Oporavak certifikata je postupak ponovnog izdavanja certifikata s istim korisničkim podacima u slučaju da je certifikat čiji se oporavak traži važeći te ne postoji potreba za promjenom korisničkih podataka.[81]

Fina može suspendirati ili opozvati certifikat. Ako korisnik raskine Ugovor o obavljanju usluga certificiranja, Fina će opozvati sve certifikate na koje se taj ugovor odnosi.

Kroz ovo istraživanje analizirana je usluga certificiranja koju pruža Fina kao prvi izdavatelj kvalificiranih certifikata u Hrvatskoj koji izdaje digitalne certifikate za javnost. Na službenim stranicama Fine nalaze se osnovne informacije vezane uz usluge certificiranja te upravljanje životnim ciklusom certifikata. Detaljnije informacije, temeljna pravila te načela za davanje usluge certificiranja koja su usklađena sa zakonskom regulativom dostupne su u dokumentu Opća pravila davanja usluga certificiranja (engl. *Certificate Policy, CP*).

[81] Fina. Opoziv, suspenzija, reaktivacija i oporavak certifikata. URL: https://www.fina.hr/Default.aspx?art=10740 (24.06.2018.)

7. Izazov dugotrajnog očuvanja digitalno potpisanih zapisa

Primjena elektroničkog potpisa, a posebno arhiviranje jedna je od značajnijih tema u području arhivistike. Arhivisti se suočavaju s dugotrajnim očuvanjem digitalno potpisanih dokumenata, a u postupku digitalnog potpisivanja primjenjuje se napredni elektronički potpis koji će osigurati integritet i vjerodostojnost digitalnog zapisa. S vremenom je postalo jasno kako arhiviranje digitalno potpisanih zapisa predstavlja izazov zbog kojeg se arhivisti suočavaju s brojnim pitanjima i poteškoćama. Dva posebno važna koncepta su upravo vjerodostojnost i integritet koji su već spomenuti nekoliko puta kao jedna od ključnih karakteristika digitalno potpisanog zapisa koju je potrebno očuvati kroz proces dugotrajnog očuvanja. Ovo su dvije osnovne karakteristike pouzdanog digitalnog zapisa. Zapis je vjerodostojan ako je ono što tvrdi da jest i ako ga je kreirala ili poslala osoba koja je potpisnik. Digitalni zapis zadržava integritet ako nije došlo do neželjenih izmjena u sadržaju digitalnog zapisa. Dakle, izmjene jesu moguće, ali nepoželjne su sve one izmjene koje će negativno utjecati na integritet. Zapravo je integritet očuvan ako izvorna namjena te temeljne karakteristike ili komponente digitalnog zapisa nisu promijenjene.

Dva ključna pitanja s kojima se arhivistika susreće u kontekstu očuvanja digitalnih zapisa koji imaju pridružene elektroničke potpise/certifikate/pečate/vremenske žigove je dugotrajna validacija i dugotrajno očuvanje elektroničkog potpisa. Za dugotrajnu validaciju nije dovoljno imati u trenutku validacije samo elektronički potpis sadržaj dokumenta. Za potrebe validacije, također je potrebno imati certifikat koji je potpisnik koristio, a valjanost tog certifikata u vrijeme nastanka potpisa također mora biti potvrđena. Certifikat je možda bio valjan u vrijeme nastanka elektroničkog potpisa, ali je s vremenom istekao ili je povučen. Stav arhivista je da arhiviranje elektroničkih potpisa nije dovoljno kako bi se uspostavila vjerodostojnost i integritet digitalnog zapisa. Potrebno je rješenje za takve zapise koje će očuvati izvorni dokument s izvornim elektroničkim potpisom. Važno je istaknuti da su elektronički potpisi vremenski ograničeni, bitstreamovi digitalnih zapisa mogu „migrirati“ (do ovoga dolazi u slučaju rješavanja problema zastarjele tehnologije) i lanac valjanosti (engl. *validation chain*) mora biti dostupan – za verifikaciju je potrebna struktura koja je izvan PKI infrastrukture, a kompletan lanac valjanosti mora sadržavati i digitalne certifikate, a posebno korijenske digitalne certifikate. Osim problema arhiviranja digitalno potpisanih zapisa i njima pridruženih potpisa, problem s kojim se arhivistika suočava je i verifikacija elektroničkog potpisa u kombinaciji s osiguranjem dostupnosti dokumenta. U nastavku će biti prikazan

napredni elektronički potpis, zakonsko okruženje elektroničkog potpisa i postojeći pristupi u dugotrajnom očuvanju digitalno potpisanih zapisa.

7.1. Napredni elektronički potpis

Dvije nove razine elektroničkog potpisa su napredni elektronički potpis (engl. *Advanced Elctronic Signature – AdES*) i kvalificirani elektronički potpis (engl. *Qualified Electronic Signature – QES*). Već je navedeno koje to zahtjeve ispunjava napredni i kvalificirani elektronički potpis, a osim zahtjeva koje ispunjavaju, temelje se i na digitalnom certifikatu. Tehnologija naprednog elektroničkog potpisa koristi asimetrični par ključeva, tj. privatni i javni ključ. Privatni ključ koristi se za generiranje elektroničkog potpisa ili za dešifriranje šifriranih informacija. Taj ključ mora ostati tajan, a javni ključ se može objaviti. Par ključeva potpisniku dostavlja središnji autoritet – CA koji verificira i registrira identitet potpisnika. Potpisnik može i sam generirati par ključeva.

Osnovne tri funkcije naprednog elektroničkog potpisa:

- autentifikacija (engl. *authentication*) – provjera je li elektronički potpis doista kreiran privatnim ključem pošiljatelja/potpisnika,
- integritet (engl. *integrity*) – dokaz izvorna namjena ili ključne komponente/karakteristike dokumenta nisu promijenjene,
- neporecivost (engl. *non-repuditation*) – potpisnik ne može opovrgnuti da je poslao ili potpisao određeni dokument.[82]

ETSI (engl. *European Telecommunications Standards Institute*, *ETSI***)** je formirala tehnički odbor pod nazivom *Electronic Signatures an Infrastructures (ESI)* koji je bio zadužen za razvoj standarda za napredni i kvalificirani potpis – AdES i QES. Rezultat su standardi za PadES (engl. *PDF Advanced Electronic Signature*, *PadES*)[83], XadES (engl. *XML Advanced*

[82] Boudrez, Filip. Digital signatures and electronic records//Archival Science 7, 2(2007), str. 179-193. URL: http://www.edavid.be/docs/digitalsignatures.pdf. (24.06.2018.).

[83] ETSI. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES. URL: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf. (25.06.2018.).

Electronic Signatures, XadES) [84] i CadES (engl. *CMS Advanced Electronic Signature, CadES*)[85].

AdES formati uključuju skupinu standarda PadES, XAdES i/ili CAdES. PAdES je napredni elektronički potpis PDF dokumenta, XAdES je napredni elektronički potpis napravljen za XML elektronički potpis, a CAdES je napredni elektronički potpis napravljen za CMS potpis. Fina također podržava Baseline profile naprednih elektroničkih potpisa. Baseline profili osiguravaju 4 vrste sukladnosti, odnosno 4 razine potpisa (B, T, LT i LTA) koje omogućuju izradu i/ili nadogradnju elektroničkog potpisa uz proces dodavanja informacija (vremenski žig, CRL lista ili OCSP odgovor, lanac povjerenja) u potpis s ciljem zadržavanja valjanosti potpisa u dugom vremenskom roku.

Prilikom razvoja ovih standarda ponajviše se razmišljalo o mogućnosti validacije elektroničkih potpisa godinama nakon nastanka potpisa što je poznato kao koncept dugotrajne validacije (engl. *long-term validation, LTV*). Ako je dokument bio ili može biti validiran nakon što je digitalno potpisan, onda je dovoljno prikupiti informacije koje su u tom trenutku bile potrebne za validaciju i pohraniti te informacije zajedno s dokumentom ili elektroničkim potpisom. Time bi se nakon pedeset ili sto godina mogao ponoviti taj proces validacije uz iste podatke čime bi se potvrdilo da je potpis bio valjan u trenutku nastanka.

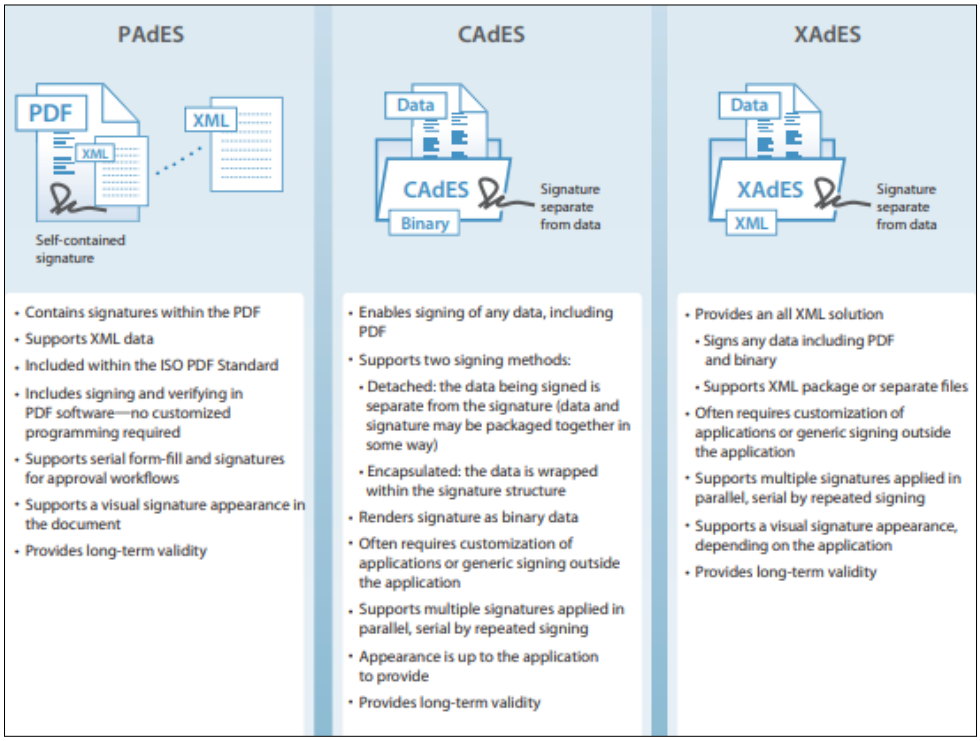
Usporedba formata elektroničkog potpisa

CadES se temelji na CMS-u[86] (engl. *Criptographic Message Syntax, CMS*). Riječ je o IETF-ovom (engl. *Internet Engineering Task Force, IETF)* standardu čija sintaksa se primjenjuje u procesu digitalnog potpisivanja, pregleda, potvrde ili šifriranja sadržaja poruke. CMS također predstavlja osnovni gradivni blok za elektroničke potpise koji se temelji na PKI infrastrukturi. Ono što CAdES dodaje CMS infrastrukturi je skup standarda za elektroničke potpise koji se mogu primijeniti na bilo koju vrstu digitalnih podataka. Osnovne karakteristike i sposobnosti digitalnog potpisivanja definiraju CAdES-BES (*Basic Electronic Signatures*) i CAdES-EPES (*Explicit Policy Electronic Signatures*), dok naprednija verzija ovog formata potpisa podržava LTV.

[84] ETSI. ML Advanced Electronic Signatures (XAdES). URL: https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf. (25.06.2018.).
[85] ETSI. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). URL: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf. (25.06.2018.).
[86] IETF. Cryptographic Message Syntax (CMS). URL: https://tools.ietf.org/html/rfc5652. (26.06.2018.).

XAdES se temelji na *XML Digital Signatures* (*XML-DSIG*) standardu za elektroničke potpise koji su prikazani u XML-u. XAdES-BES (*Basic Electronic Signatures*) i XAdES-EPES (*Explicit Policy Electronic Signatures*) definiraju osnovne sposobnosti potpisivanja ovim formatom potpisa, a XML-DSIG je naprednija verzija ovog formata koja također podržava LTV.

PAdES sadrži sve one karakteristike koje sadrže CadES i XAdES. Glavna razlika je u tome što se ovaj format primjenjuje samo na PDF dokumente te definira zahtjeve koje moraju ispuniti softveri koji se koriste za pregled i uređivanje PDF dokumenata kada ti dokumenti imaju pridružene elektroničke potpise.



Slika 24. Usporedba PAdES, CAdES i XAdES formata[87]

CAdES, XAdES i PAdES u upotrebi

Glavna razlika između ova tri formata je u tome što PAdES definira kako bi se trebao ponašati softver koji podržava digitalno potpisane PDF dokumente, dok druga dva formata

[87] The AdES family of standards: CAdES, XAdES, and PAdES. Implementation guidance for using electronic signatures in the European Union, White paper, Adobe Systems, 2009. URL: http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf

definiraju tehnologiju koja će se koristiti u razvijanju aplikacije koja treba obraditi elektronički potpis.

Korištenjem formata CAdES ili XAdES, izvorni podaci mogu biti bilo koje vrste, pa čak i PDF dokument, a stvaranje i provjera elektroničkog potpisa mogu se provesti neovisno o softveru koji obrađuje izvorne podatke. Međutim, potrebno je imati dva softvera. Jedan softver je zadužen za obradu izvornih podataka, a drugi je softver za digitalno potpisivanje koji podržava elektronički potpis ili format. PDF pruža elektroničku verziju dokumenta, ali i bogatiji digitalni sadržaj koji se može pohraniti i kasnije prezentirati korisniku. Zbog toga je toliko raširena primjena PDF-a. Prelazak s papira na PDF nije bio toliki šok upravo zbog mogućnosti PDF-a da elektronički prezentira bilo koju formu papirnatog dokumenta i to uz potporu PAdES formata elektroničkog potpisa.

PAdES Baseline Profile

S obzirom da se PDF dokumenti mogu pohraniti i čuvati kroz duže vremensko razdoblje, potrebno je imati alate koji će osigurati valjanost digitalno potpisanih dokumenata u PDF formatu kroz duže vremensko razdoblje. Elektronički potpis bi trebao ostati valjan bez obzira na ključ ili certifikat koji je istekao ili je povučen, središnji autoritet koji više ne postoji ili kriptografski algoritam koji više nije pouzdan. U svrhu rješavanja ovih problema razvijeni su određeni standardi pa tako i ETSI standard, tj. tehničke specifikacije pod nazivom *ETSI TS 103 172 – Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile*[88], koje definiraju kako bi se trebao arhivirati PDF koji koristi PadES standard, tj. format. U standardu je opisan PAdES osnovni profil koji razlikuje nekoliko tipova PadES elektroničkih potpisa:

- **B-Level** – definira profil za kratkoročne elektroničke potpise te mora sadržavati elektronički potpis potpisni certifikat;
- **T-Level** – kao i B-Level, ali još sadrži i vremenski žig koji je zapravo dokaz da je elektronički potpis bio valjan u trenutku nastanka;
- **LT-Level** – kao T-Level, ali sadrži i VRI (*Verification Related Information*) podatke i DSS (*Document Security Store*). Ovaj profil zapravo omogućava validaciju elektroničkog potpisa nakon dužeg vremenskog razdoblja koje je prošlo od nastanka potpisa. Ovaj profil preporučuje se za napredni elektronički potpis;

[88] ETSI. Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf. (27.06.2018.).

- **LTA-Level** – kao LT-Level, ali dodaje vremenski žig i VRI podatke za TSA (*Time Stamp Authority*) DSS-u. Ovaj profil može pomoći u validaciji elektroničkog potpisa bez obzira na bilo koji događaj ili vremensko razdoblje koje je prošlo od nastanka potpisa, tj. sve ono što bi moglo ograničiti njegovu valjanost.

7.2. Pravno i normativno okruženje vezano uz elektroničke potpise

Tijekom dugotrajnog očuvanja digitalno potpisani zapisi moraju zadržati svoje temeljne karakteristike, dakle vjerodostojnost, pouzdanost, integritet i upotrebljivost. Očuvanje navedenih karakteristika zahtijeva složeno rješenje digitalnog arhiva. Potrebno je uzeti u obzir relevantne norme na koje se potrebno osloniti ili one koje mogu pripomoći te važeći pravni okvir u kojem će digitalni arhiv djelovati.

Uredba eIDAS

Uredba eIDAS, punog naziva "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", svojom primjenom je izvan snage stavila Zakon o elektroničkom potpisu koji se primjenjivao u Republici Hrvatskoj. Ovom uredbom utvrđuju se uvjeti pod kojima države članice priznaju sredstva elektroničke identifikacije fizičkih i pravnih osoba koja su obuhvaćena prijavljenim sustavom elektroničke identifikacije druge države članice, zatim se utvrđuju pravila za usluge povjerenja, i to posebno za elektroničke transakcije te se uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica. Uredba donosi brojne novitete, a jedan od njih se odnosi i na korištenje e-potpisa. Tako će se certifikati za e-potpis moći dodijeliti samo fizičkim osobama koje će njime moći potpisivati dokumente, koji će služiti za dokazivanje identiteta potpisnika. Pravne osobe će koristiti certifikate za e-pečate koji služe za potvrđivanje cjelovitosti (integriteta) i izvornosti dokumenta. Ona propisuje i obvezu korištenja pouzdanog popisa kvalificiranih poslužitelja usluge povjerenja na europskoj razini (*EU Trusted List*). Kada je u pitanju dugotrajno čuvanje digitalno potpisanih zapisa, Uredba eIDAS definira e-vremenske žigove kao podatke u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i tako dokazuju da su ti podaci postojali u to vrijeme. Stupanjem na

snagu ove Uredbe tržište bi trebalo profitirati od stvaranja kvalificiranih usluga povjerenja, a korisnici bi se trebali osjećati sigurnije i jednostavnije se koristiti online uslugama.[89]

ISO 15489 Informacije i dokumentacija – Upravljanje spisima

Važno je izdvojiti i međunarodnu normu ISO 15489 Informacije i dokumentacija – Upravljanje spisima. Godine 2001. Međunarodna organizacija za normiranje (ISO) objavila je dva teksta, tj. dva dijela nove međunarodne norme za upravljanje dokumentima. Prvi dio odnosi se na opći dio norme, a drugi dio su smjernice koje su u ranijim fazama izrade norme bile poznatije kao tehničko izvješće. Primjenom ISO 15489-1:2016 Informacije i dokumentacija – Upravljanje spisima – 1. dio: Koncepti i načela, izvan snage je stavljen ISO 15489 iz 2001. godine. Prema ISO 15489, e-zapisi moraju ostati vjerodostojni, što znači da nakon svakog provedenog postupka digitalnog očuvanja i dalje moraju biti autentični, pouzdani, cjeloviti i upotrebljivi te moraju zadržati sadržaj, strukturu i kontekst s ostalim očuvanim zapisima.[90]

ISO 14721:2012 Otvoreni arhivski informacijski sustav (OAIS)

S obzirom da je jedno od mogućih tehničkih rješenja za dugotrajno očuvanje upravo referentni model za otvoreni arhivski informacijski sustav (engl. *Open Archival Information System Reference Model, OAIS RM*), potrebno je spomenuti i postojeću normu koja definira ovaj model. Model je razvio *Consultative Committee for Space Data Systems* (CCSDS) pri američkoj agenciji NASA 1999. godine. Model je u siječnju 2002. postao ISO standardom. Najnovija verzija je iz 2012. godine[91] i ona je trenutno u procesu osuvremenjivanja. OAIS referentni model može se primijeniti u svakom digitalnom arhivu, ali ga je potrebno razraditi i prilagoditi s obzirom na specifičnost stvaratelja i digitalnog arhiva. OAIS model govori o dugotrajnom očuvanju digitalnih zapisa u obliku objekata i informacijskih paketa (SIP, AIP, DIP). Kroz ovaj model detaljno su objašnjeni svi koraci u postupku očuvanja, dijelovi sustava digitalnog arhiva te njihova međusobna povezanost. Također su istaknuti glavni zadaci OAIS arhiva, okolina te struktura referentnog modela.

[89] Uredba eIDAS, n. dj.
[90] ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles URL: https://www.iso.org/standard/62542.html. (28.06.2018.).
[91] ISO 14721:2012 Space data and information transfer systems – Open archival information system (OAIS) – Reference model. URL: https://www.iso.org/standard/57284.html. (28.06.2018.).

7.3. Postojeći pristupi dugotrajnom arhiviranju i očuvanju digitalno potpisanih zapisa

Digitalno potpisani digitalni zapisi ili oni kojima je pridodan digitalni pečat su jedan od izazova za arhivsku struku. Takve digitalne zapise nije jednostavno očuvati i to ne samo zbog neprestanog napretka tehnologije, nego i zbog toga što certifikati na koje se oslanjaju imaju ograničeno vrijeme trajanja. Tako, primjerice, Fina izdaje certifikate na dvije godine, a AKD (Agencija za komercijalnu djelatnost) na pet godina. Vršni (engl. *root*) certifikati izdavatelja u pravilu traju duže, npr. deset godina. Nakon isteka perioda na koji je certifikat izdan, neće više biti moguće provjeriti valjanost elektroničkog potpisa, ali će se moći i dalje provjeravati cjelovitost i nepromjenjivost samog zapisa. Trenutno postoji nekoliko pristupa koji predstavljaju rješenje za dugotrajno očuvanje digitalnih zapisa koji imaju pridodane elektroničke potpise ili pečate. Riječ je o OAIS-u i TDR-u kao digitalnim arhivima od povjerenja, te CRL listama i OCSP servisu gdje oboje imaju više ulogu potpore dugotrajnom očuvanju. Potrebno je istaknuti i posebnu vrstu žiga koji je namijenjen dugotrajnom očuvanju, a od standardnog se razlikuje po obuhvatu.

OAIS i TDR – digitalni arhivi od povjerenja

Ovaj pristup, tj. uspostavljanje digitalnih arhiva prema OAIS referentnom modelu u načelu predstavlja tehnički najmanje zahtjevno rješenje. OAIS model doprinosi što boljem razumijevanju problematike očuvanja na dulji vremenski rok, a u isto vrijeme i očuvanja autentičnosti digitalnih objekata. *Consultative Committee for Space Data Systems* (CCSDS) započeo je s radom na razvoju formalnih standarda za dugotrajno pohranjivanje digitalnih podataka generiranih iz svemirskih misija. Osim na formalnim standardima, radilo se i na razvoju referentnog modela za „Otvoreni arhivski informacijski sustav“ (OAIS). Referentni model je zamišljen kao sveobuhvatan i dosljedan okvir za opis i analizu problema vezanih uz digitalno očuvanje, kao model koji će osigurati korake za razvoj budućih standarda i poslužiti kao referenca svima onima koji su zainteresirani za razvoj proizvoda i usluga u području digitalnog očuvanja. Dakle, u središtu pozornosti referentnog modela je otvoreni arhivski informacijski sustav. Dvije temeljne funkcije digitalnog arhiva uspostavljenog prema OAIS referentnom modelu su dugotrajno očuvanje informacije i osiguranje pristupa pohranjenoj informaciji i to u skladu s potrebama primarnih korisnika/ciljnih korisničkih skupina. OAIS referentni model sastoji se od 3 odvojene, ali povezane komponente. Prva je vanjsko okruženje u kojem OAIS djeluje, zatim funkcionalne komponente/unutarnji mehanizmi koji

zajednički ispunjavaju OAIS-ovu zadaću očuvanja i treća je komponenta su informacijski objekti koje OAIS pohranjuje, upravlja njima i dijeli ih s korisnicima. Tako se referentni model sastoji od informacijskog, modela transformacija informacijskih paketa i funkcionalnog modela. Posebno je izdvojena okolina OAIS arhiva u kojoj arhiv djeluje.

OAIS digitalni arhiv se nalazi u okolini koja ima utjecaj na njega, ali i on na nju. Okolinu čine četiri entiteta, a to su stvaratelji gradiva, korisnici/ciljna korisnička skupina, menadžment i, naravno, OAIS arhiv. Ova četiri entiteta konstantno surađuju te svaki od njih ima određene uloge i zadaće koje mora provoditi kako bi ovakva okolina uspješno funkcionirala. Pa je tako menadžment zadužen za formuliranje, reviziju, a ako je potrebno i provođenje političkih okvira koji upravljaju aktivnostima OAIS-a. Stvaratelji gradiva su pojedinci, organizacije ili sustavi koji šalju informaciju OAIS-u radi pohrane i dugotrajnog očuvanja. S druge strane su potrošači/korisnici, tj. pojedinci, organizacije ili sustavi. Referentni model definira i posebnu skupinu korisnika, ciljnu korisničku skupinu (engl. *Designed Community*). Radi se o podskupini od koje se očekuje neovisnost po pitanju razumijevanja arhivirane informacije u obliku u kojem je očuvana i stavljena na raspolaganje od strane OAIS-a.[92]

Referentni model definira i opisuje osnovni skup mehanizama koji OAIS arhivu omogućuju ispunjenje temeljnih zadaća, tj. dugotrajno očuvanje informacija i osiguranje dostupnosti istih ciljnoj korisničkoj skupini. Ovi mehanizmi su sažeti u funkcionalnom modelu. Dakle, radi se o uslugama/funkcionalnim entitetima koji mogu biti implementirani i prilagođeni u skladu sa zahtjevima i okolnostima pojedinog arhiva. Funkcionalni model se tako sastoji od prihvata, arhivske pohrane, upravljanja podacima, administracije, planiranja procesa očuvanja i pristupa.

Osim funkcionalnih komponenti, referentni model opisuje i informacijske objekte kojima OAIS upravlja. Informacijski model temelji se na konceptu informacijskog paketa. Informacijski paket sastoji se od objekta koji je u središtu očuvanja, a uz objekt dolaze i metapodaci koji su potrebni kao podrška dugotrajnom očuvanju, pristupu i razumijevanju objekta. Objekt i metapodaci zajedno čine jedan logički paket. Postoje tri vrste informacijskih paketa od kojih svaki ima određenu funkciju u procesu očuvanja. Dostavljeni informacijski paket (engl. *Submission Information Package, SIP*) je vrsta paketa koji stvaratelj gradiva dostavlja OAIS arhivu na čuvanje. Koncept SIP-a naglašava činjenicu da informacija možda

[92] CCSDS. Reference model for an open archival information system (OAIS), 2012., str. 2-2. URL: https://public.ccsds.org/pubs/650x0m2.pdf. (28.06.2018.).

neće biti očuvana u onom obliku u kojem ju je stvaratelj predao OAIS arhivu. Također je moguć slučaj neispravnih ili nepotpunih metapodataka pri čemu je iste potrebno ispraviti/poboljšati prilikom prihvata. Vrsta paketa koji je pohranjen i čuva se u OAIS arhivu je arhivski informacijski paket (engl. *Archival Information Package, AIP*). AIP se sastoji od informacije koja je predmet očuvanja, koja je popraćena i metapodacima koji su sada nadopunjeni ili ispravljeni i kao takvi dovoljni za OAIS-ove usluge očuvanja i pristupa. Diseminacijski informacijski paket (engl. *Dissemination Information Package, DIP*) je onaj koji se isporučuje korisniku kao odgovor na zahtjev za pristup. DIP koncept naglašava činjenicu da se informacijski paket koji je OAIS isporučio korisniku može razlikovati oblikom ili sadržajem od onoga koji je pohranjen u arhivu. Ono po čemu bi se DIP i AIP mogli razlikovati je format i količina sadržaja te metapodaci. Iako OAIS arhiv upravlja svim vrstama paketa, AIP je informacijski paket koji je u središtu pozornosti što se tiče dugotrajnog očuvanja.[93]

Digitalni arhiv uspostavljen prema OAIS modelu koji zaprima digitalno potpisane zapise ima šest glavnih zadataka koje mora ispuniti, a to su:

1. Pregovaranje o preuzimanju i preuzimanje odgovarajuće informacije od stvaratelja (engl. *Information Producers*).
2. Ostvarivanje dovoljne razine kontrole nad preuzetim informacijama radi dugotrajnog očuvanja.
3. Odrediti, samostalno ili konzultirajući se s drugima, koje skupine trebaju postati ciljnim korisničkim skupinama radi razumijevanja isporučenih informacija. Definiranjem ciljne korisničke skupine, definira se i baza znanja.
4. Osiguranje nezavisnosti razumijevanja informacija od strane ciljnih korisničkih skupina, tj. ciljna korisnička skupina trebala bi biti u mogućnosti razumjeti informacije bez potrebe za posebnim resursima, kao što je pomoć stručnjaka.
5. Praćenje dokumentiranih politika i procedura, a u svrhu čuvanja informacija od raznih nepredviđenih situacija.
6. Osiguranje dostupnosti očuvanih informacija ciljnim korisničkim skupinama, a također i osiguranje diseminacije autentificiranih kopija izvornika.[94]

[93] CCSDS. Reference model for an open archival information system (OAIS), n. dj., str.4-34 – 4-40.
[94] CCSDS. Reference model for an open archival information system (OAIS), n. dj., str. 3-1.

Ovaj referentni model osigurava okvir za razumijevanje i podizanje svijesti o arhivskim konceptima koji su potrebni za dugotrajno očuvanje i pristup informacijama, navodi i koncepte koji su potrebni od strane drugih institucija kako bi bile učinkoviti sudionici procesa očuvanja. Također je i okvir koji uključujući terminologiju i koncepte opisuje i uspoređuje arhitekturu i djelatnosti postojećih i budućih arhiva, a omogućuje i opis i usporedbu drugih strategija i tehnika za dugotrajno očuvanje.

Ulaskom dokumenta s pridodanim elektroničkim potpisom u digitalni arhiv, provjerava se valjanost elektroničkog potpisa, ta informacija se bilježi u metapodatke i arhivira dokument kao arhivski zapis s pripadajućim metapodacima. Na taj način više nije važno što će certifikat isteći jer će se informacija o njegovoj valjanosti prilikom zaprimanja čuvati u samom digitalnom arhivu. No, da bi se povjerenje u digitalni arhiv uspostavljen prema OAIS-u moglo ostvariti, on treba biti uspostavljen po načelima i sukladan normi ISO 16363:2012 za uspostavu digitalnih repozitorija od povjerenja (engl. *Trusted Digital Repositories, TDR*)[95], koja propisuje kako brojni koraci koji se poduzimaju prilikom dugotrajnog očuvanja trebaju odvijati, a da ne ugroze vjerodostojnost digitalnih zapisa koji su u tom arhivu pohranjeni. Drugim riječima, tek kada je neki digitalni arhiv uspostavljen prema OAIS-u i usklađen s TDR-om, povjerenje u valjanost nekog elektroničkog potpisa može se prenijeti sa samog zapisa na digitalni arhiv.

CRL liste i OCSP servis kao potpora dugotrajnom očuvanju

U kontekstu pristupa koji doprinose dugotrajnom očuvanju svoje mjesto našle su i već spomenute CRL liste te OCSP servis. S obzirom na karakteristike i zadaće, CRL liste i OCSP servis potpora su dugotrajnom očuvanju. Dodavanjem podataka o statusu valjanosti certifikata na CRL liste ili odgovora OCSP servisa te uključivanjem lanca certifikata radi povjerenja u potpisni certifikat moguće je uspješno potvrditi elektronički potpis nakon što je prošlo dosta vremena od isteka potpisnog certifikata.

Objava CRL lista je uobičajeni način za opoziv certifikata. Sama CRL lista predstavlja običnu datoteku s nizom serijskih brojeva, a svaki digitalni certifikat ima jedinstveni broj. Ukoliko se certifikat nalazi na listi, znači da je opozvan. Listu objavljuje odgovarajuća certifikacijska služba (CA) u unaprijed određenim vremenskim intervalima. Međutim, CRL liste imaju i

[95] ISO 16363:2012 Space data and information transfer systems – Audit and certification of trustworthy digital repositories. URL: https://www.iso.org/standard/56510.html. (28.06.2018.).

potencijalne nedostatke. Jedan od nedostataka je veličina CRL datoteka. Zbog neprestane objave novih serijskih brojeva povučenih digitalnih certifikata, CRL datoteke mogu poprilično narasti. Dobra strana je mogućnost njihova korištenja bez uspostavljanja internetske veze (eng. *offline*). Neka od obveznih polja koja su ključna za kasniju mogućnost provjere elektroničkog potpisa su serijski broj, datum i vrijeme opoziva digitalnog certifikata.

OCSP servis temelji se na OCSP protokolu, koji je razvijen zbog potrebe zaobilaženja nedostataka vezanih uz CRL liste. OCSP u PKI infrastrukturi dodaje i entitet službe potvrđivanja (engl. *Validation Authority, VA*), koja je odgovorna za provjeru valjanosti digitalnog certifikata. U tom slučaju CA šalje podatke o opozivu službi potvrđivanja. Osoba koja želi provjeriti valjanost nekog digitalnog certifikata, šalje upit službi potvrđivanja i dobiva odgovor „valjan“, „opozvan“ ili „nepoznat“. U ovom slučaju nije potrebno preuzimati CRL liste i pohranjivati ih uz arhivirane zapise, već se uspostavom direktne komunikacije provjerava je li neki digitalni certifikat valjan ili nije. To je, naravno i glavni nedostatak – gubitak mogućnosti provjere valjanosti bez uspostavljene internetske veze, a osim toga mogući problem predstavlja i kašnjenje između trenutka opoziva i objave o opozivu digitalnog certifikata. U Hrvatskoj Fina nudi mogućnost provjere valjanosti certifikata putem Fina OCSP 2015 servisa i putem dohvata CRL lista, a preporuka je korištenje OCSP servisa.[96]

Arhivski digitalni vremenski žig

Uredba eIDAS definira digitalne vremenske žigove koji dokazuju da su određeni podaci postojali u određeno vrijeme. Međutim, postoji i posebna vrsta vremenskog žiga koji je namijenjen za dugotrajno očuvanje. Takav se arhivski digitalni vremenski žig od standardnog razlikuje samo po svojem obuhvatu koji se odnosi na veći broj hash vrijednosti svakog podatka koji je potrebno dugotrajno očuvati. Ono što se želi ostvariti primjenom arhivskog digitalnog vremenskog žiga je produljenje valjanosti kratkotrajnog vremenskog žiga elektroničkog potpisa te ostvarenje mogućnosti pozitivnog OCSP i CRL odgovora na upit o valjanosti elektroničkih potpisa i nakon isteka valjanosti potpisnih certifikata. Dakle, ideja je da se u elektronički potpis prilikom izrade ili naknadno uključe dodatne informacije koje će omogućiti uspješno potvrđivanje u skladu s očekivanim vremenskim rasponom u kojem će ga biti potrebno potvrditi. Ovo rješenje je i detaljnije objašnjeno u normi za izradu i potvrđivanje naprednih elektroničkih potpisa, ETSI EN 319 102-1 v1.1.0. te u normama za pojedine

[96] Fina. Digitalni certifikati. URL: http://www.fina.hr/Default.aspx?sec=1799. (29.06.2018.).

formate naprednih elektroničkih potpisa, definiranjem četiriju temeljnih razina elektroničkog potpisa koje omogućuju interoperabilnost i dulji životni vijek zapisa. Primjer je ETSI tehnička specifikacija za PAdES Baseline Profile (*PDF Advanced Electronic Signature - PAdES*),ETSI TS 103172 V2.1.1. Ova tehnička specifikacija tako definira četiri vrste sukladnosti, tj. četiri razine potpisa.

Razine potpisa su B, T, LT i LTA, a omogućuju izradu i/ili nadogradnju elektroničkog potpisa uz proces dodavanja informacija u potpis s ciljem zadržavanja valjanosti potpisa u drugom vremenskom roku. Prilikom izrade svake sljedeće razine obuhvaća se i prethodna. LTA razina uključuje ugradnju tokena vremenskog žiga što omogućava validaciju elektroničkog potpisa nakon dužeg vremenskog perioda. Upravo je ova razina odgovorna za dugotrajnu valjanost i integritet dokumenta. Važno je izdvojiti B-LTA (engl. *Baseline-Long-Term Archiving*) razinu koja omogućuje periodička dodavanja arhivskih vremenskih žigova prethodne razine.[97] U stvarnosti ovo znači da će se s vremena na vrijeme tijekom dugotrajnog očuvanja ipak morati stariji zapisi ovijati dodatnim arhivskim vremenskim žigovima. To se neće moći izbjeći, a trebat će se voditi računa o tome kada svakom pojedinom zapisu istječe njegov arhivski vremenski žig kako bi se ovio novim.

[97] Više o ovoj temi u: Volarević, Ira; Stančić, Hrvoje, Norme za elektroničke vremenske žigove i mogućnosti njihove primjene u arhivskoj struci, u: Babić, Silvija (ur.), Arhivi i domovinski rat, Zagreb: Hrvatsko arhivističko društvo, 2016., str. 425-435.

8. Blockchain tehnologija kao novi pristup dugotrajnom očuvanju digitalno potpisanih zapisa

Osim navedenih tehnologija, jedno od mogućih rješenja kada je u pitanju dugotrajno očuvanje digitalno potpisanih zapisa je i tehnologija ulančanih blokova (engl. *blockchain*). Kroz dio rada koji je posvećen ovoj tehnologiji, koristit će se termin blockchain. Ova tehnologija je najpoznatija kao tehnologija koja se nalazi u podlozi digitalnih valuta (kriptovaluta), a koja se danas već primjenjuje u različitim drugim područjima i u različite svrhe. Ova tehnologija je upravo po svojoj prirodi prava arhivska tehnologija jer sve što se njome zabilježi više se ne može promijeniti niti izbrisati. Blockchain predstavlja bazu podataka ili bazu zapisa transakcija za spremanje sažetaka (hash vrijednosti) podataka, informacija, transakcija, dokumenata ili zapisa. Često se uz blockchain veže i pojam tehnologija distribuirane glavne knjige (engl. *Distributed Ledger Technologies, DLT*). Sam naziv tehnologije na engleskom jeziku sastoji se od dva pojma – pojam "block" odnosi se na zaokruženu cjelinu sadržaja, a pojam "chain" odnosi se na međusobno nadovezivanje blokova jedan na drugi. Ova tehnologija je realizirana kroz decentraliziranu (engl. *peer-to-peer*) mrežu u kojoj svako priključeno računalo pohranjuje podatke o svim transakcijama (u blockchain se ne pohranjuju podaci, već samo njihove hash vrijednosti).

U kontekstu dugotrajnog očuvanja digitalno potpisanih zapisa, blockchain može se iskoristiti tako da se prilikom zaprimanja takvih zapisa u digitalni arhiv informacija o valjanosti elektroničkog potpisa zabilježi u blockchain. S obzirom da se jednom upisana informacija više ne može mijenjati niti brisati, jednom kad istekne vrijeme valjanosti nekog potpisnog certifikata moći će se provjeriti je li on vrijedio u trenutku zaprimanja i bilježenja u blockchain tehnologiju, pa ako je vrijedio i ako se arhivirani zapis u međuvremenu nije promijenio onda se taj zapis može tretirati kao da mu je elektronički potpis dalje valjan. PKI infrastruktura koja se trenutno primjenjuje i u Fini ima svoje prednosti, ali također i određene mane i rizike poput brzog (iz arhivske perspektive) isteka certifikata i potrebe za njihovim neprestanim ovijanjem novim (arhivskim) vremenskim žigovima zbog kojih je bilo logično razmotriti mogućnost primjene upravo ove tehnologije koja olakšava cijeli proces provjere valjanosti elektroničkog potpisa te uklanja brojne spomenute rizike PKI infrastrukture.

Ova tehnologija je u postupku normiranja. Hrvatski zavod za norme aktivno se uključio u razvoj norme ISO/TC 307 Ulančani blokovi i tehnologije distribuirane glavne knjige (engl.

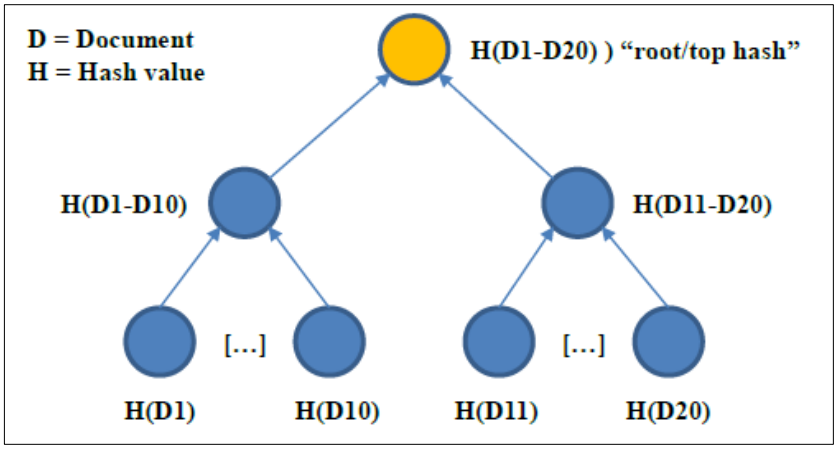
Blockchain and Distributed Ledger Technologies)[98] i formirao zrcalni tehnički odbor (TO) koji se time bavi. Korištenjem blochchain tehnologije u području arhivistike bavi se i InterPARES Trust projekt kroz istraživanje *Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31)*[99].

Osnovni koncepti i princip rada

Kako bi princip rada ove tehnologije i općenito distribuiranih tehnologija bio jasniji, potrebno je pojasniti određene koncepte na kojima se temelji blockchain. Hash funkcije su već detaljno pojašnjene, tako da će se u sklopu ovog poglavlja pojasniti ostali važni koncepti, a to su Merklovo stablo (engl. *Merkle tree*), distribuirani konsenzus (engl. *Distributed consensus*) i, naravno, koncept blockchaina.

Merklovo stablo je pristup koji je prvi puta predstavio Ralph C. Merkle 1980. godine. Struktura ovog pristupa oponaša strukturu stabla, stoga je bilo logično nazvati pristup *Merkle tree*. Blockchain primjenjuje strukturu ovog pristupa, stoga je važno pojasniti kako ovaj pristup funkcionira. Princip rada bit će pojašnjen na primjeru tvrtke koja kreira deset dokumenata ujutro i deset dokumenata popodne (slika 25). Za svaki dokument potrebno je izračunati hash vrijednost. U podne, deset hash vrijednosti je objedinjeno u jednu hash vrijednost koja se odnosi samo na dokumente nastale ujutro. Zatim je na kraju dana izračunata jedna hash vrijednost za sve dokumente koji su nastali poslijepodne. Nakon toga obje hash vrijednosti su objedinjene kako bi se dobila jedna hash vrijednost koja će predstavljati sve dokumente koji su nastali u jednom danu. Ta hash vrijednost se još naziva i *root hash* ili *top hash*, odnosno korjenski hash.

[98] Razvoj norme pokrenut je u travnju 2017. godine. Više na: ISO/TC 307 Blockchain and Distributed Ledger Technologies. URL: https://www.iso.org/committee/6266604.html.(29.06.2018.).
[99] InterPARES Trust – Research Studies. URL: https://interparestrust.org/trust/about_research/studies. (30.06.2018.).

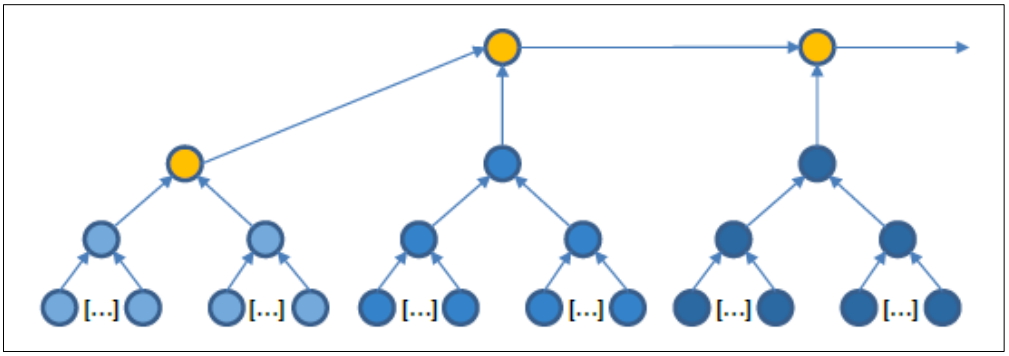


Slika 25. Merkleovo stablo[100]

Blockchain primjenjuje distribuiranu *peer-to-peer* mrežu. Postoje tri osnovna tipa mrežne topologije- centralizirana, decentralizirana i distribuirana. Centralizirana mreža ima jedan centralni server s kojim su spojena ostala računala iz mreže. Decentralizirana mreža ima nekoliko servera koji su spojeni s računalima iz mreže. Ovaj tip mreže ima decentraliziranu kontrolu i znatno je sigurniji, ali serveri su i dalje izloženi mogućim napadima. Distribuirana mreža nema jedan centralni server jer su sva računala međusobno povezana i jednako važna tako da ova mreža nema tu jednu centralnu točku koja je izložena napadima. Primjenom distribuirane mreže, nema potrebe za trećom stranom od povjerenja. Primjenom načela distribuiranog konsenzusa svaki sudionik (čvor) provjerava svaki događaj u glavnoj knjizi/bazi transakcija.

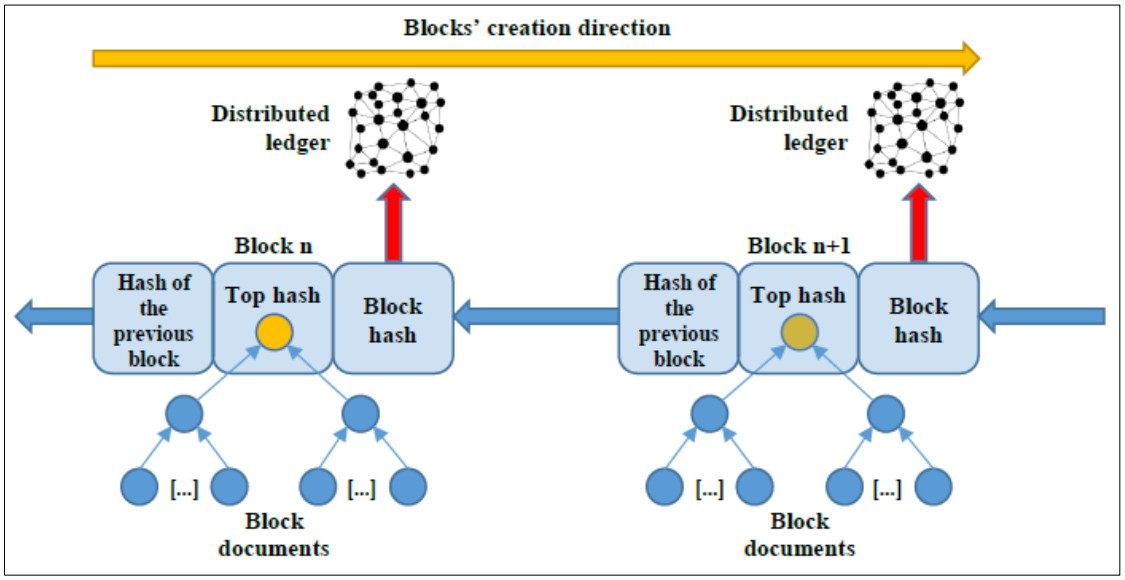
Blockchain kreira lanac povezanih blokova što će biti objašnjeno na istom primjeru na kojem je pojašnjeno i Merkleovo stablo. Tvrtka može ponoviti proces stvaranja korjenskog hasha naredni dan. Rezultat će biti dva hasha – jedan za npr. ponedjeljak i jedan za utorak. Za te dvije vrijednosti može biti izračunat novi korjenski hash koji ujedinjuje dva hasha od dva različita dana. Taj jedan hash se može dalje povezati s hashom od srijede kako bi se opet izračunao novi korjenski hash. Svaki novi korjenski hash izračunava se kombinacijom hasha trenutnog dana i prethodnog korjenskog hasha, a čime svi oni međusobno povezuju (slika 26).

[100] Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report, 2018., str. 11. URL: https://interparestrust.org/assets/public/dissemination/TRUSTERPreservationModel(EU31)-Finalreportv_1_3.pdf. (03.07.2018.).



Slika 26. Povezivanje hash vrijednosti[101]

Blockchain traži od svih čvorova potvrdu o nastanku novog korjenskog hasha (slika 27). S obzirom na primjenu distribuirane mreže, novi blok je potvrđen kada se kvalificirana većina mrežnih čvorova s time složila.

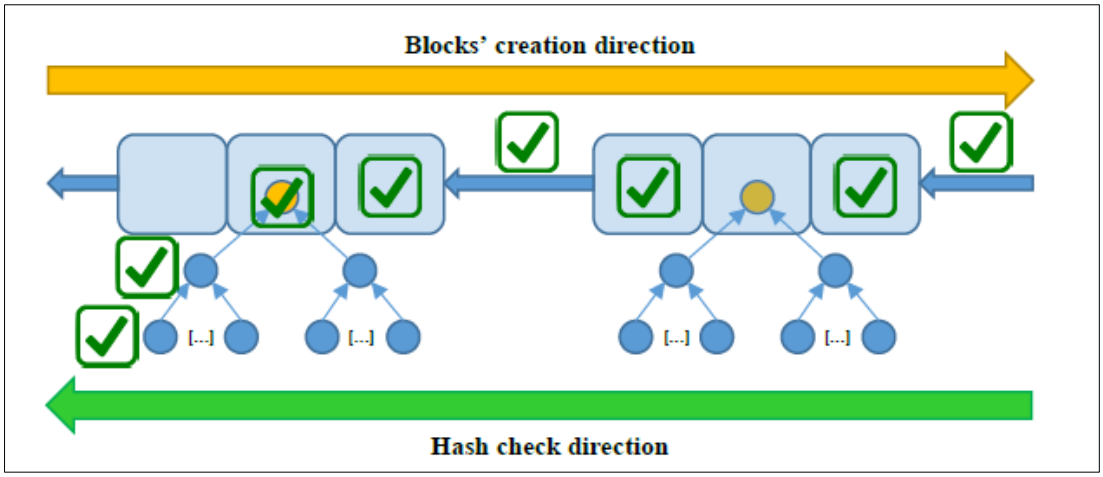


Slika 27. Nastanak blockchain tehnologije[102]

Postoji niz prednosti ove tehnologije. Iako se u blockchain mogu pohraniti podaci, većinom se pohranjuje samo hash vrijednost. Dodavanjem svakog novog bloka, jača prethodni blok jer se lanac i sastoji od blokova koji su povezani. Svaki pokušaj izmjene bloka uzrokovat će lančanu štetu, tj. svi naredni blokovi postaju nevažeći. Upravo zato izmjene nad već nastalim

[101] Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report, n. dj., str. 12.
[102] Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report, n. dj., str. 13.

blokovima nisu moguće. Blockchain sadrži dokaz da je hash, a time i određeni dokument, bio dio izvornog skupa hash vrijednosti od kojeg je lanac izgrađen (slika 28).



Slika 28. Provjera hash vrijednosti u blockchainu[103]

Za svaku distribuiranu tehnologiju ulančanih blokova ključno je da dosegne određenu veličinu, tj. određeni broj čvorova kako bi se zaštitio od potencijalnih napada. Koji je to broj čvorova, ovisi o implementaciji tehnologije ulančanih blokova injegovoj privlačnosti da ga se napadne. Postoje četiri osnovna tipa implementacije – javni i privatni blockchain (iz perspektive upravljanja) te nezaštićeni (engl. permissionless) i zaštićeni (engl. permissioned) iz perspektive zaštite pristupa). Javni je onaj koji ne pripada nikome i nitko njime ne upravlja, a privatni onaj koji je uspostavila jedna institucija (ili više njih) i njime upravlja. Nezaštićeni je onaj u koji svaka osoba može, zapisivati podatke kao što je na primjer kod kriptovaluta Bitcoin i Ethereum. Zaštićeni je onaj u koji samo sudionici od povjerenja mogu zapisivati podatke u lanac, a primjer primjene može biti zajednica arhiva koji su partneri.

Prednosti blockchaina u kontekstu dugotrajnog očuvanja predstavljaju potvrdu integriteta zapisa, potvrda da je zapis postojao ili je nastao u određenom trenutku (ali prije nego što je zapisan u blockchain tehnologiju), potpora neporecivosti, unaprjeđenje mogućnosti validacije tijekom dugotrajnog očuvanja te onemogućavanje manipuliranja procesima.

Blockchain se danas primjenjuje u raznim područjima. U početku je njezina primjena bila ograničena samo na kriptovalute. Danas se tako primjenjuje u ekonomiji, zdravstvu, online glasanju i mnogim drugim. Mogla bi u potpunosti transformirati svijet ekonomije i bankarstva.

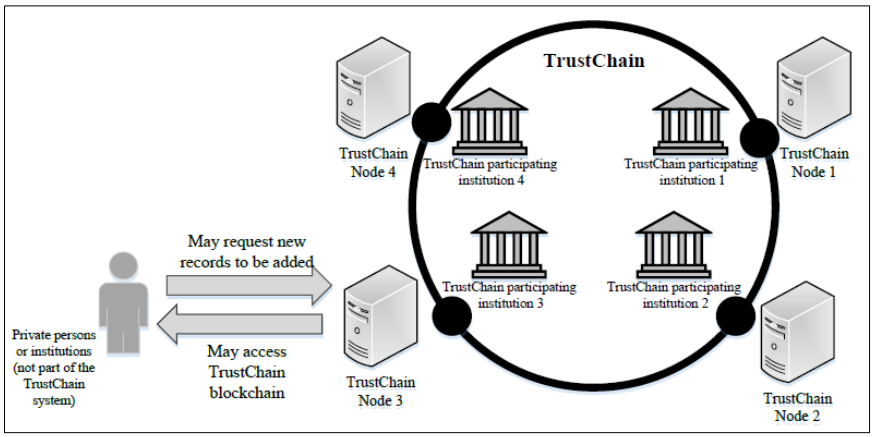
[103] Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report, n. dj., str. 14.

Također, postoji niz primjena ove tehnologije u siromašnim zemljama pa je zbog toga riječ o tehnologiji koja bi mogla u potpunosti transformirati društvo.

8.1. TrustChain model

U slučaju arhiviranja digitalno potpisanih dokumenata problem se javlja kada istekne certifikat koji je korišten prilikom digitalnog potpisivanja ili je središnji autoritet koji izdaje certifikate izvan funkcije. Kada dođe do ovakve situacije, elektronički potpis više ne može biti potvrđen. Jedno od mogućih rješenja u svrhu rješavanja problema dugotrajnog očuvanja valjanosti elektroničkog potpisa je TrustChain model, tj. model za dugotrajno očuvanje digitalno potpisanih dokumenata primjenom tehnologije blockchain. Ovaj model razvija se u sklopu projekta pod nazivom *TRUSTER Preservation Model (EU31*), a koji je dio međunarodnog projekta InterPARES Trust.

Model je jedno od mogućih rješenja problema koje je istraživački tim razmotrio. Ovaj model primjenjuje blockchain kako je opisano u dokumentu BitcoinWhitepaper (Nakamoto, 2008), ali u ovaj model nije uključen *proof-of-work* koncept. Jezgra ovog modela je blockchain koja sadrži hash elektroničkog potpisa. Bilo koja osoba ili institucija može zatražiti dodavanje zapisa o dokumentu u blockchain, ali samo ako ovlašteni čvorovi blockchaina smiju zabilježiti novi zapis. TrustChain čvorovi (engl. *TrustChain nodes*) su zapravo serveri koje održava pojedina institucija koja sudjeluje u ovom projektu. Ti serveri prihvaćaju nove zahtjeve za dodavanje zapisa o dokumentu u blockchain, obrađuju ih i zapisuju u lanac, a blockchain se pohranjuje i dostupan je za „čitanje“. Komunikacija između strane koja je podnijela zahtjev za bilježenje zapisa u lanac i samih čvorova ostvaruje se putem posebnog TrustChain klijentskog softvera ili web sučelja. Strana koja je zainteresirana za potvrdu valjanosti dokumenta kojemu je istekao elektronički potpis kontaktirat će čvor, „pročitati“ blockchain tehnologiju, pronaći relevantan podatak i usporediti ga s dokumentom čiji elektronički potpis se želi potvrditi. Uspješan pronalazak bloka u tom lancu blokova moguć je uz primjenu sustava indeksiranja koji se oslanja na metapodatke dokumenata čiji zapisi su pohranjeni u blockchainu (slika 29). Taj sustav može biti dio TrustChain čvorova, a i ne mora. TrustChain ne može produžiti vrijeme trajanja certifikata, ali svakako može biti jamstvo da nije došlo do izmjena dokumenta i njemu pridruženog elektroničkog potpisa od trenutka kada je informacija o tom dokumentu zabilježena u lancu. S obzirom da elektronički potpis sadrži podatke o korisniku/potpisniku, moguće je kasnije potvrditi identitet osobe koja je sastavila i potpisala dokument.

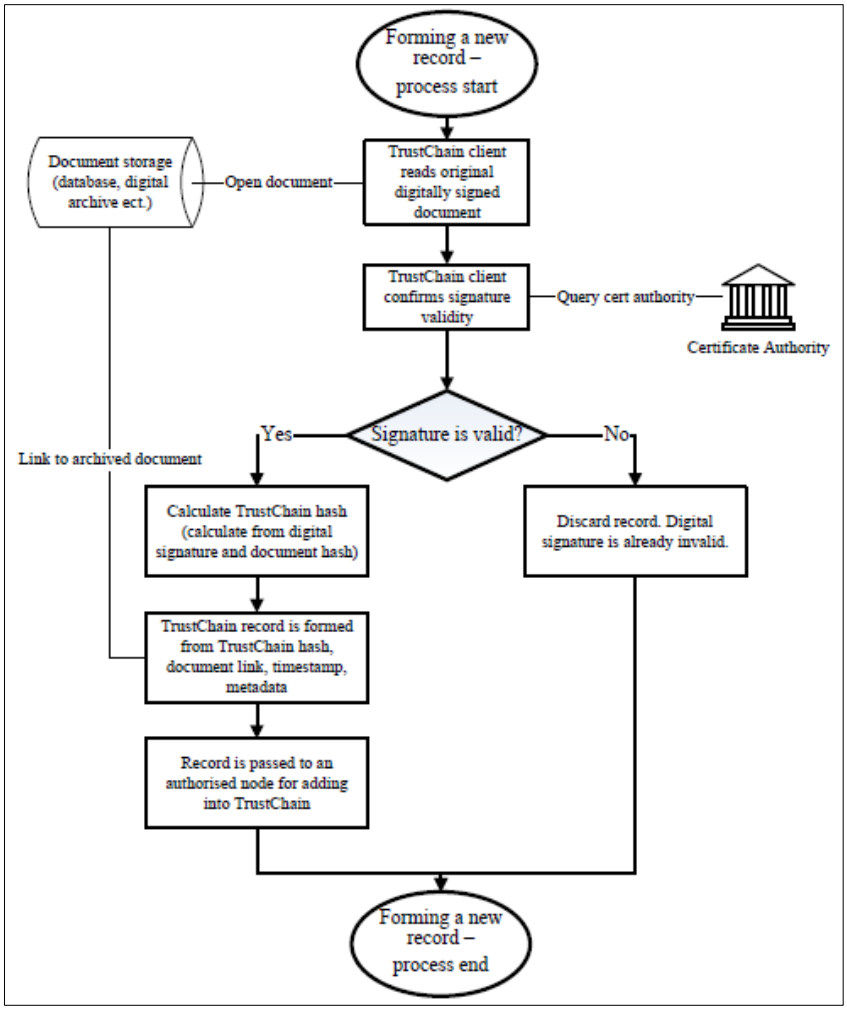


Slika 29. Osnovni koncept TrustChain modela[104]

Princip rada TrustChain modela

Proces bilježenja zapisa o dokumentu u TrustChain započinje tako što zainteresirana strana vrši selekciju onih dokumenata koji imaju pridružene elektroničke potpise, a potrebno ih je očuvati. Pritom elektronički potpis mora proći validaciju koju će provesti certifikacijska služba. Konkretan dokument se ne pohranjuje u TrustChain sustav zato što taj sustav pohranjuje jedino kontrolni hash elektroničkog potpisa. Softver koji priprema TrustChain zapis o dokumentu, izračunat će i hash koji se pohranjuje u sustav. Link na dokument, vremenski žig i drugi relevantni metapodaci koje je upisao korisnik, dodaju se hashu i formiran je TrustChain zapis. Nakon što je formiran, zapis se prosljeđuje TrustChain čvoru koji će pohraniti zapis u blockchain. Prvi dio procesa prikazan je na slici 30.

[104] Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long - term preservation of digital signature validity: TrustChain. INFuture2017 Conference Proceedings, str. 92. URL: https://www.researchgate.net/publication/321171227_A_Model_for_Longterm_Preservation_of_Digital_Signature_Validity_TrustChain



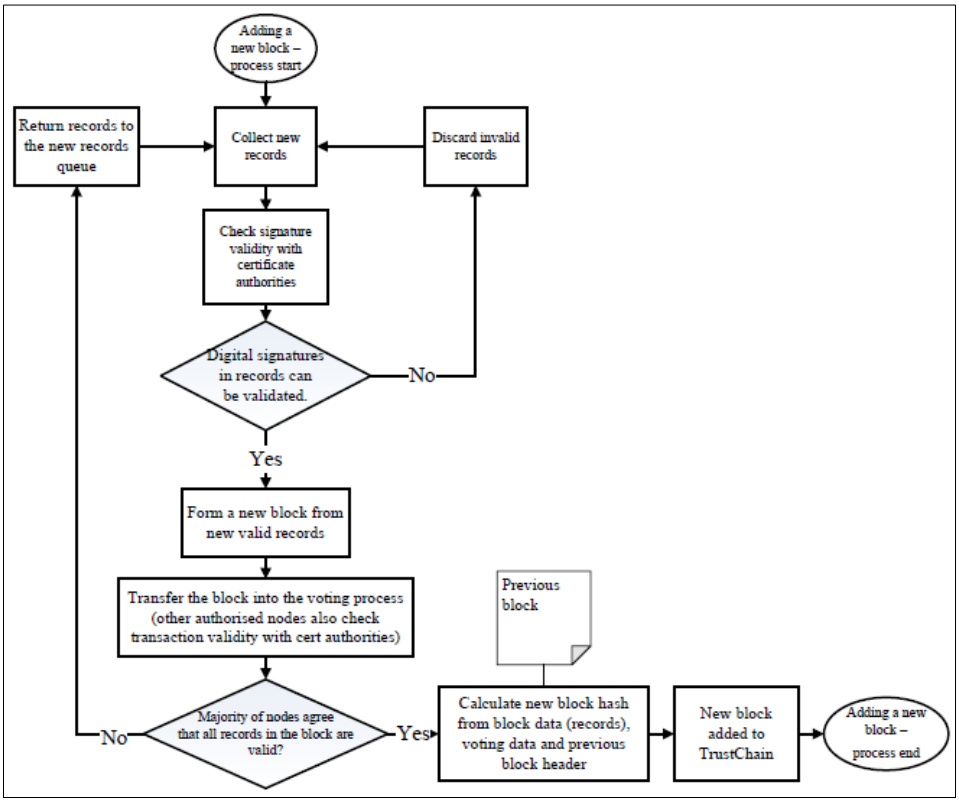
Slika 30. Dodavanje zapisa u TrustChain[105]

TrustChain čvor će provjeriti valjanost potpisa i kreirati novi zapis dokumenta koji će biti pridružen ostalim zapisima koji će kasnije tvoriti novi TrustChain blok. Potvrda valjanosti potpisa je upravo to što će čvor prihvatiti novi blok. Ovaj proces ovisi o formatu zapisa i pridruženom elektroničkom potpisu. O instituciji i njezinim zahtjevima također ovisi i koje vrste dokumenata i elektronički potpisi mogu biti provjereni. Ovaj korak generalno podrazumijeva provjeru je li možda došlo do izmjena u sadržaju dokumenta nakon što je potpisan te slanje certifikata certifikacijskoj službi na validaciju. Predloženo rješenje ne ovisi o dokumentu niti pohranjuje dokument ili potpis, jedino dolazi u interakciju s njima u procesu

[105] Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long - term preservation of digital signature validity: TrustChain, n. dj., str. 93.

provjere valjanosti. Stoga je ovaj dio sustava neovisan i očekuje se da će prihvaćati i buduće formate elektroničkog potpisa.

Proces dodavanja zapisa u blok i zapisivanje tog bloka u blockchain je radnja koju obavljaju TrustChain čvorovi (slika 31). Čvor prikuplja nove zapise koji su u redu čekanja i pokušava provesti validaciju svih elektroničkih potpisa. Ako potpis nije valjan, zapis se također smatra nevaljanim i čvor nastavlja prikupljati nove zapise za validaciju. Nakon što je prikupljena određena količina zapisa s valjanim elektroničkim potpisom, dodaju se u blok, ali ovaj blok se još uvijek ne dodaje u blockchain. Prije toga, potreban je određeni broj drugih čvorova koji će potvrditi valjanost svih zapisa. Zahtijevani broj ovisi o ukupnom broju TrustChain čvorova i zahtijevanoj razini pouzdanosti (što više čvorova provjeri isti zapis, to će odgovor o tom zapisu biti pouzdaniji). Ako je odgovor većine čvorova da je blok valjan, blok se dodaje u blockchain (nakon što je izračunat hash sadržaja tog bloka i hash prethodnih blokova). Inače će blok biti odbačen, a zapisi koji su tvorili taj blok će biti vraćeni u red čekanja, tj. skupinu novih zapisa.

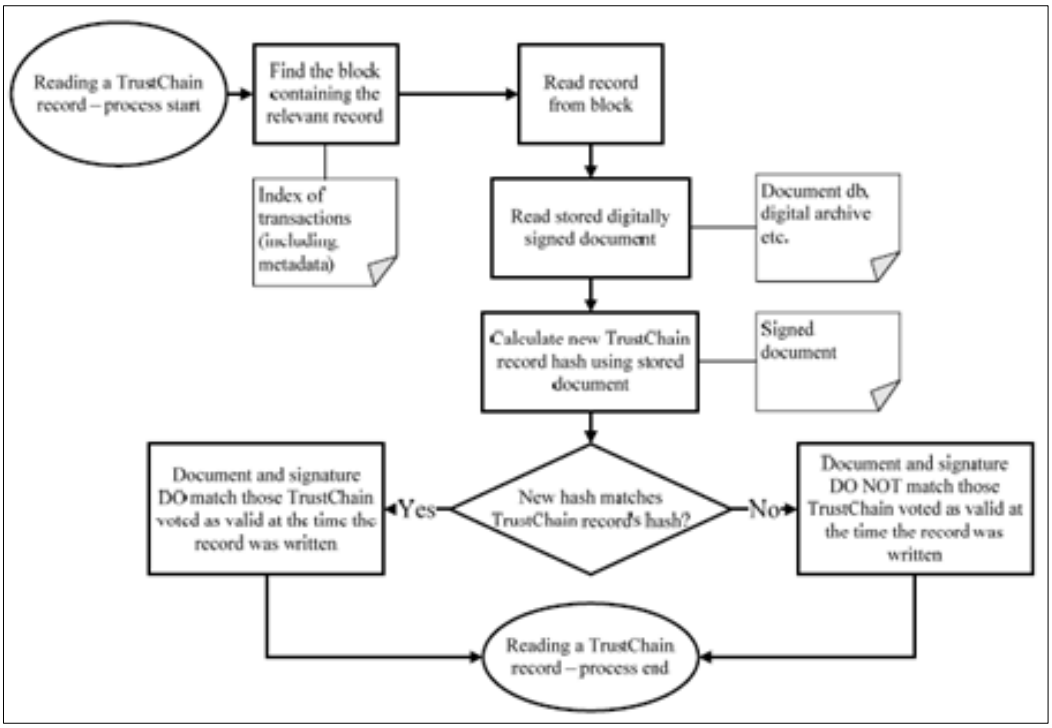


Slika 31. Dodavanje novog bloka u TrustChain[106]

[106] Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long - term preservation of digital signature validity: TrustChain, n. dj., str. 95.

Proces potvrde valjanosti (slika 32) elektroničkih potpisa počinje pronalaskom relevantnih zapisa u TrustChain blockchainu. U ovome dijelu procesa TrustChain se oslanja na zabilježene metapodatke o pojedinim dokumentima. S obzirom da je blockchain zapisan u tekstualnom obliku, moguće ga je preuzeti i pretražiti bez potrebe za specijaliziranim alatima.

Nakon što je pronađen relevantan zapis, potrebno je ponovno izračunati hash izvornog dokumenta i usporediti ga s onim hashom koji je zabilježen u TrustChainu. Ako se hash vrijednosti podudaraju, može se potvrditi da nije došlo do izmjena dokumenta i pridruženog mu elektroničkog potpisa od datuma koji je zabilježen u blockchainu putem vremenskog žiga.



Slika 32. Čitanje zapisa iz TrustChaina[107]

Format TrustChain zapisa i blockchaina

Nakon što je opisan proces validacije elektroničkog potpisa, potrebno je opisati podatkovnu strukturu TrustChaina – blockchain. Trenutno je blockchain dizajniran kao tekstualna datoteka čiji je sadržaj u JSON formatu. Kao i svaki blockchain, i rješenje predloženo ovdje sastoji se od više blokova koji tvore nepromjenjiv lanac koji uključuje hash vrijednost izračunatu za sadašnji i prethodni blok. Svaki blok se može „razbiti“ na nekoliko dijelova –

[107] Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long - term preservation of digital signature validity: TrustChain, n. dj., str. 96.

header, *records* i *votes*. Records sekcija sadrži informacije o pojedinom digitalno potpisanom dokumentu i hash tog dokumenta. Hash algoritam koji se primjenjuje u ovom modelu je SHA256, ali se s vremenom može promijeniti. Hash, link na dokument i relevantni metapodaci predstavljaju najvažnije komponente TrustChain zapisa.

Polje *version* odnosi se na verziju podatkovnog modela koji je korišten prilikom izrade zapisa. *Metadata* pododjeljak oslanja se na ISAD(G) skup elemenata i mora sadržavati sve informacije potrebne za indeksiranje i kasniji pronalazak zapisa o dokumentu u blockchainu. Međutim, nije obavezno uključiti ona polja koja će ostati prazna.

Nakon *records* sekcije slijedi *votes* sekcija. Ova sekcija se također sastoji od više pododjeljaka. Cijela sekcija se formira u trenutku kreiranja bloka i to pomoću izvornog čvora, ali čvorovi koji su zapravo zaduženi za glasanje (engl. *voting nodes*) upisuju svoj glas u polje „*is_block_valid*“.

Sustav glasanja temelji se na pojednostavljenoj verziji sustava korištenog u *BigChainDB* sustavu. Nakon što je izvorni čvor primio odgovor od čvorova „glasača“, potvrđuje glasove kao valjane tako što provjerava potpise čvorova „glasača“. Nakon što je sekcija popunjena glasovima koji potvrđuju valjanost bloka, izračunat je konačni hash i blok se zapisuje u blockchain. Za izračun konačnog hasha koristi se trenutni i prethodni blok.

Predloženi model za dugotrajno očuvanje digitalno potpisanih dokumenata nije isključivo arhivski sustav ili sustav za digitalno očuvanje dokumenata, nego se radi o sustavu koji se primjenjuje u kombinaciji s takvim sustavima kako bi se sigurno pohranila informacija o valjanosti elektroničkog potpisa. Primjenom ovog modela, nije više potrebno puno povjerenje u certifikacijsku službu. Sustav se oslanja na grupu institucija od povjerenja koje su zainteresirane za implementiranje ovakvog sustava. Jedna od mana sustava je ta što trenutno rješava samo problem dokumenata koji imaju valjane elektroničke potpise, te ne nudi rješenje rješenje za dokumente čiji certifikat je istekao. Riječ je o prototipu modela koji je samo jedno od mogućih rješenja za dugotrajno očuvanje valjanosti digitalno potpisanih zapisa.

9. Zaključak

Dugotrajno očuvanje digitalnih zapisa je proces koji arhivistima predstavlja izazov. Posebno su izazov oni digitalni zapisi koji su i digitalno potpisani tj. imaju pridružene elektroničke potpise/certifikate/pečate/vremenske žigove. Takvi zapisi predstavljaju izazov jer moraju prilikom očuvanja zadržati određene karakteristike. Stoga se kroz ovaj rad analizirala problematika očuvanja takvih zapisa. Zapravo je srž problema u očuvanju valjanosti elektroničkih potpisa i mogućnosti provjere valjanosti dugo nakon nastanka elektroničkog potpisa. Na početku rada su ukratko pojašnjeni koncepti dugotrajnog očuvanja, digitalnog zapisa, digitalno potpisanog zapisa i elektroničkog potpisa. Dio rada bavi se i kriptografijom kao okruženjem u kojem je elektronički potpis nastao i kao infrastrukturom koju je iskoristio. Nakon toga slijedi dio koji se bavi upravljanjem elektronički potpisom, a tu su obuhvaćeni PKI infrastruktura i elektronički certifikat. U sklopu istraživanja provedena je analiza Fininog okruženja. Razlog odabira Fine je taj što Fina predstavlja prvog davatelja usluge certificiranja u Republici Hrvatskoj, a svoju uslugu temelji na PKI infrastrukturi. Također je detaljnije pojašnjen napredni elektronički potpis, a predstavljeni su i postojeći pristupi u dugotrajnom očuvanju digitalno potpisanih zapisa. Osim postojećih pristupa izdvojene su i najznačajnije norme i uredbe na koje se treba osloniti prilikom rješavanja ove problematike. Analizirana je i blockchain tehnologija kao novi pristup u dugotrajnom očuvanju digitalno potpisanih zapisa. Može se zaključiti kako problematika dugotrajnog očuvanja digitalno potpisanih zapisa obuhvaća niz faktora na koje je potrebno obraditi pozornost. U cijelom procesu digitalno potpisani zapis bi trebao zadržati određena svojstva, a valjanost potpisa bi se trebala moći provjeriti i dugo nakon nastanka potpisa. Infrastruktura koja se većinom primjenjuje u certifikacijskim službama je PKI, koja se pokazala kao rješenje koje ima prednosti, ali i određene rizike. Upravo te rizike može se riješiti primjenom blockchain tehnologije. Prednosti blockchaina u kontekstu dugotrajnog očuvanja predstavljaju potvrda integriteta zapisa, potvrda da je zapis postojao ili je nastao u određenom trenutku (ali prije nego što je zapisan u blockchain), potpora neporecivosti, unapređenje mogućnosti validacije tijekom dugotrajnog očuvanja, te onemogućavanje manipuliranja procesima.

Literatura

1. Anić, Vladimir; Rončević Brozović, Dunja; Goldstein, Ivo; Goldstein, Slavko; Jojić, Ljiljana; Matasović, Ranko; Pranjković, Ivo . Hrvatski enciklopedijski rječnik. Zagreb: EPH d.o.o. i Novi Liber d.o.o., 2004.

2. Boudrez, Filip. Digital signatures and electronic records//Archival Science 7, 2(2007). URL: http://www.edavid.be/docs/digitalsignatures.pdf

3. Borghoff, Uwe: Rodig, Peter; Scheffczyk, Jan; Schmitz, Lothar. Long-Term preservation of Digital

4. Bralić, V., Kuleš, M., & Stančić, H. (2017). A model for long - term preservation of digital signature validity: TrustChain. INFuture2017 Conference Proceedings. URL: https://www.researchgate.net/publication/321171227_A_Model_for_Longterm_Preservation_of_Digital_Signature_Validity_TrustChain

5. CARnet CERT. Algoritmi za izračunavanje sažetaka. 2006. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-166.pdf

6. CARNet CERT. Digitalni potpis. 2007. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf

7. CARNet - CERT. Metode povlačenja digitalnih certifikata. 2005. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-03-115.pdf

8. CARNet CERT. Napadi na RSA. 2003. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-04-19.pdf

9. CARNet CERT. Nedostaci PKI infrastrukture. 2009. URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-02-255.pdf

10. CCSDS. Reference model for an open archival information system (OAIS), 2012. URL: https://public.ccsds.org/pubs/650x0m2.pdf

11. Documents: Principles and Practices. USA: International Computer Science Institute, 2012.

12. Duđela, Andrej; Maretić, Marcel. Kriptografija. Zagreb: Element, 2007

13. ETSI. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). URL: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf

14. ETSI. Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

15. ETSI. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES. URL:https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf

16. ETSI. ML Advanced Electronic Signatures (XAdES). URL: https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf

17. etutorials. org. Asymmetric Encryption Explained. URL: http://etutorials.org/Programming/Programming+.net+security/Part+III+.NET+Cryptography/Chapter+15.+Asymmetric+Encryption/15.1+Asymmetric+Encryption+Explained/

18. Fina. Certifikati za poslovne subjekte. URL: http://www.fina.hr/Default.aspx?art=10752

19. Fina. Digitalni cerifikati. URL: https://www.fina.hr/Default.aspx?art=10751

20. Fina. Elektroničko poslovanje. URL: http://www.fina.hr/Default.aspx?sec=940

21. Fina. e-Potpis. URL: http://www.fina.hr/Default.aspx?sec=960

22. Fina. Fina PKI sustav. URL: http://www.fina.hr/Default.aspx?sec=1799

23. Fina. Opoziv, suspenzija, reaktivacija i oporavak certifikata. URL: https://www.fina.hr/Default.aspx?art=10740

24. Fina. Poslovni subjekti/građani. URL: http://www.fina.hr/Default.aspx?sec=1714

25. Fina. RFC Editor. URL: https://www.rfc-editor.org/info/rfc6960

26. Fina. Web e-Potpis. URL: https://www.fina.hr/Default.aspx?sec=960

27. Herceg, Boris; Brzica, Hrvoje; Stančić, Hrvoje. Digitally Signed Records – Friend or Foe?, u: Anderson, Karen; Duranti, Luciana; Jaworski, Rafał; Stančić, Hrvoje; Seljan, Sanja; Mateljan, Vladimir (ur.), e-Institutions - Openness, Accessibility, and Preservation. Zagreb: Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, Croatia, 2015.

28. Heslop, Helen; Davis, Simon; Wilson, Andrew. An Approach to to the Preservation of Digital Records, National Archives of Australia, 2002. URL: http://www.imaginar.org/taller/dppd/DPPD/40%20pp%20Approach.pdf

29. Houghton, Bernadette. Preservation Challenges in the Digital Age, D-Lib Magazine, 22(7/8), srpanj/kolovoz 2016. URL: http://www.dlib.org/dlib/july16/houghton/07houghton.html

30. IBM Terminology, s.v. record. URL: https://www01.ibm.com/software/globalization/terminology/r.html

31. IETF. Cryptographic Message Syntax (CMS). URL: https://tools.ietf.org/html/rfc5652

32. Information security. URL: https://security.stackexchange.com/questions/20134/in-pgp-why-not-just-encrypt-message-with-recipients-public-key-why-the-meta-e

33. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. URL: https://tools.ietf.org/html/rfc5280

34. InterPARES Trust – Research Studies URL: https://interparestrust.org/trust/about_research/studies

35. ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles. URL: https://www.iso.org/standard/62542.html

36. ISO 16363:2012 Space data and information transfer systems – Audit and certification of trustworthy digital repositories. URL: https://www.iso.org/standard/56510.html

37. ISO 14721:2012 Space data and information transfer systems – Open archival information system (OAIS) – Reference model. URL: https://www.iso.org/standard/57284.html

38. ISO/TC 307 Blockchain and Distributed Ledger Technologies URL: https://www.iso.org/committee/6266604.html

39. Keith, Martin. Everyday Cryptography: Fundamental Principles and Applications. New York:Oxford University Press, 2012. URL: https://bayanbox.ir/view/2880755982131658715/Oxford-Everyday-Cryptography-Fundamental-Principles-and-Applications-2014.pdf

40. Kessler, Gary C. An overview of criptography. 2018. URL: https://www.garykessler.net/library/crypto.html#why3

41. Kwidama, Sevickson; Hassanmahomed, Taarik. Criptographyc Key Management. Academiyear 2008-2009. URL: https://www.os3.nl/_media/2008-2009/courses/lia/ckm_thassanmahomed_skwidama.pdf

42. Menzes, J. Alfred; Oorschot, Paul C.;Vanstone, Scott A. Handbook of applied cryptography.USA: CRC Press, 1996. URL: http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf

43. Multilingual Archival Terminology. Emulacija. URL: http://www.ciscra.org/mat/mat/term/4549

44. Multilingual Archival Terminology. Migracija. URL: http://www.ciscra.org/mat/mat/term/4622/6029

45. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 11 21, 2015. URL: https://bitcoin.org/bitcoin.pdf

46. National Security Agency; Queensland University of Technology. X.509v3 Certificates for Secure Shell Authentication. 2011. URL: https://tools.ietf.org/html/rfc6187

47. NIST. Digital Signature Standard (DSS). URL: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

48. NIST. Reccomendation for Key Management: Part 1: General.2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

49. Radić, Drago. " Informatička abeceda ". Kriptiranje – zaštita poruka u komunikaciji. URL: https://informatika.buzdo.com/pojmovi/gpg-1.htm

50. RFC 1312. The MD5 Message-Digest Algorithm URL: https://www.ietf.org/rfc/rfc1321.txt

51. Stančić, Hrvoje. Arhiviranje digitalnih dokumenata, 4. seminar Arhivi, knjižnice i muzeji. Mogućnosti suradnje u okruženju globalne informacijske infrastrukture. Zagreb, 2001.

52. Stančić, Hrvoje.Digitalizacija građe, 2. i 3. seminar Arhivi, knjižnice, muzeji. Mogućnosti suradnje u okruženju globalne informacijske infrastrukture, Zagreb, 2000.

53. Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report, 2018. URL: https://interparestrust.org/assets/public/dissemination/TRUSTERPreservationModel(EU31)-Finalreportv_1_3.pdf

54. Stančić et. al., Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model) (EU31). Final report.

55. The AdES family of standards: CAdES, XAdES, and PAdES. Implementation guidance for using electronic signatures in the European Union, White paper, Adobe Systems, 2009. URL: http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf

56. Trusted List Croatia. Trust service providers. URL: https://webgate.ec.europa.eu/tl-browser/#/tl/HR

57. TRUSTER Preservation Model (31) - Model for Preservation Of Trustworthiness of Digitally Signed, Timestamped and /or Seald Digital Records. URL: https://interparestrust.org/trust/about_research/studies

58. Uredba eIDAS, 2014. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014R0910&from=HR

59. Volarević, Ira; Stančić, Hrvoje, Norme za elektroničke vremenske žigove i mogućnosti njihove primjene u arhivskoj struci, u: Babić, Silvija (ur.), Arhivi i domovinski rat, Zagreb: Hrvatsko arhivističko društvo, 2016., str. 425-435.

60. X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 2016. URL: http://www.itu.int/rec/T-REC-X.509-201610-I/en

Popis slika

Slika 1. Model izvedbe: izvor i proces komponente 8
Slika 2. Model izvedbe: digitalni zapis 8
Slika 3. Shema klasične kriptografije 13
Slika 4. Simetrična kriptografija, asimetrična kriptografija, hash funkcija 17
Slika 5. Proces šifriranja i dešifriranja tajnim ključem 18
Slika 6. Proces šifriranja i dešifriranja primjenom dva različita ključa 20
Slika 7. Oba pošiljatelja koriste isti ključ za šifriranje, a šifrat može dešifrirati samo primatelj 21
Slika 8. Svojstva sigurnosti 24
Slika 9. Opći model iterativne hash funkcije – jednostavni i detaljni prikaz 26
Slika 10. Pojednostavljena klasifikacija kriptografskih hash funkcija 27
Slika 11. Princip rada PGP sustava – šifriranje i dešifriranje 30
Slika 12. Faze i stanja u procesu upravljanja ključevima 36
Slika 13. Generiranje elektroničkog potpisa 39
Slika 14. Verifikacija i validacija elektroničkog potpisa 40
Slika 15. Komponente PKI infrastrukture 43
Slika 16. Izdavanje certifikata 46
Slika 17. Prikaz strukture digitalnog certifikata 47
Slika 18. Prikaz strukture CRL liste 48
Slika 19. Sadržaj OCSP zahtjeva 50
Slika 20. Struktura OCSP odgovora 51
Slika 21. Sučelje web stranice Fine – Digitalni certifikati 54
Slika 22. Sučelje web stranice Fine – Digitalni certifikati 55
Slika 23. FINA RDC 2015 okolina 58
Slika 24. Usporedba PAdES, CAdES i XAdES formata 68
Slika 25. Merkleovo stablo 80
Slika 26. Povezivanje hash vrijednosti 81
Slika 27. Nastanak blockchain tehnologije 81
Slika 28. Provjera hash vrijednosti u blockchainu 82
Slika 29. Osnovni koncept TrustChain modela 84
Slika 30. Dodavanje zapisa u TrustChain 85
Slika 31. Dodavanje novog bloka u TrustChain 86
Slika 32. Čitanje zapisa iz TrustChaina 87

Popis tablica

Tablica 1. Simetrični i asimetrični algoritmi 31
Tablica 2. Vrste digitalnih certifikata u novoj dvorazinskoj okolini 57
Tablica 3. Certifikati prema namjeni 59

Sažetak

Arhivistima su osobito izazov oni digitalni zapisi koji su i digitalno potpisani tj. imaju pridružene elektroničke potpise. Takvi zapisi predstavljaju izazov jer moraju prilikom očuvanja zadržati određene karakteristike. Zapravo je srž problema u očuvanju valjanosti elektroničkih potpisa i mogućnosti provjere valjanosti dugo nakon nastanka elektroničkog potpisa. Stoga se kroz ovaj rad analizira problematika očuvanja takvih zapisa. Kroz ovaj interdisciplinarni rad pojašnjeni su koncepti dugotrajnog očuvanja, digitalnog zapisa i digitalno potpisanog zapisa. Dio rada bavi se i kriptografijom kao okruženjem u kojem je nastao elektronički potpis. Također je provedeno i istraživanje tj. analiza usluge certificiranja koju pruža Fina. Izdvojene su i norme i uredbe na koje se potrebno osloniti u ovoj problematici, analizirani su postojeći pristupi dugotrajnom očuvanju ovakvih zapisa gdje je izdvojena i blockchain tehnologija kao novi pristup.

Ključne riječi: Fina, elektronički potpis, digitalni zapis, dugotrajno očuvanje, kriptografija

Technologies for long-term preservation of digitally signed archival records

Summary

Archivists are especially challenged by digital records that are digitally signed. Such records represent a challenge because they have to retain certain characteristics when preserving them. It is, in fact, the core of the problem in preserving the validity of electronic signatures and validation opportunities long after the electronic signature has been created. Therefore, this thesis will analyze the issues of preserving such records. The concepts of long-term preservation, digital records and digitally signed records have been clarified. Part of this thesis also deals with cryptography as the environment in which an electronic signature emerged. Research has also been carried out in which the certification service provided by Fina is analyzed. The standards and regulations to which this issue has to be addressed are outlined. Existing approaches have been analyzed for the long-term preservation of this kind of records, where blockchain technology has been represented as a new approach.

Key words: Fina, electronic signature, digital record, long-term preservation, cryptography