SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

DIPLOMSKI RAD

NASLOV DIPLOMSKOG RADA

Antonio Krističević

Split, srpanj 2021.

SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

Diplomski studij: **Računarstvo**

Smjer/Usmjerenje: /

Oznaka programa: 250

Akademska godina: 2020./2021.

Ime i prezime: Antonio Krističević

Broj indeksa: 507-2019

**ZADATAK DIPLOMSKOG RADA**

Naslov: **NASLOV RADA**

Zadatak: Prilikom prijave diplomskog rada mentor definira temu i radni naslov, a točan naslov rada utvrđuje se po završetku rada. Diplomski se rad, potpisan od strane mentora, predaje Odboru za diplomski rad u tri tiskana primjerka s tvrdim uvezom te na CD-u. Izradu diplomskog rada ocjenjuje mentor, a predsjednik Odbora za diplomski rad potvrđuje zadatak i konačni naslov rada. Ukoliko je predsjednik Odbora za diplomski rad ujedno i mentor, diplomski rad uz mentora potpisuje i jedan od članova Odbora. **Ovu stranicu piše mentor prije predaje rada nakon što je utvđen konačni naslov rada.**

Prijava rada: 05.10.2016. (početak semestra u kojem se prijavljuje rad)

Rok za predaju rada: 05.02.2017. (deset dana prije završetka semestra u kojem je rad prijavljen)

Rad predan:

Predsjednik

Odbora za diplomski rad: Mentor:

prof. dr. sc. Ime Prezime izv. prof. dr. sc. Ime Prezime

**IZJAVA**

Ovom izjavom potvrđujem da sam diplomski rad s naslovom (NASLOV DIPLOMSKOG RADA) pod mentorstvom (prof. dr. sc. IME I PREZIME NASTAVNIKA) pisao samostalno, primijenivši znanja i vještine stečene tijekom studiranja na Fakultetu elektrotehnike, strojarstva i brodogradnje, kao i metodologiju znanstveno-istraživačkog rada, te uz korištenje literature koja je navedena u radu. Spoznaje, stavove, zaključke, teorije i zakonitosti drugih autora koje sam izravno ili parafrazirajući naveo/la u diplomskom radu citirao/la sam i povezao/la s korištenim bibliografskim jedinicama.

Student

Antonio Krističević

**Sadržaj**

[1 Uvod 1](#_Toc80293116)

[2 Digitalni potpisi 2](#_Toc80293117)

[2.1 Asimetrična kriptografija 2](#_Toc80293118)

[2.1.1 RSA potpisivanje 3](#_Toc80293119)

[2.2 PKI 5](#_Toc80293120)

[2.3 X.509 6](#_Toc80293121)

[2.3.1 Opoziv certifikata 7](#_Toc80293122)

[3 eIDAS uredba 9](#_Toc80293123)

[3.1 Kvalificirani elektronski potpisi 11](#_Toc80293124)

[4 AdES razina digitalnih potpisa 13](#_Toc80293125)

[5 DSS 14](#_Toc80293126)

[6 Arhitektura sustava 15](#_Toc80293127)

[7 Implementacija sustava 16](#_Toc80293128)

[8 Zaključak 17](#_Toc80293129)

[Literatura 18](#_Toc80293130)

[Popis oznaka i kratica 19](#_Toc80293131)

[Sažetak 20](#_Toc80293132)

[Summary 21](#_Toc80293133)

[Prilozi 22](#_Toc80293134)

[Kazalo slika 22](#_Toc80293135)

# Uvod

Trend digitalizacije i modernizacije nezaobilazna je pojava 21. st. Veliki broj usluga razvija se u obliku web aplikacija koje se, u sve većem broju, izvršavaju u računalnim oblacima. Uz već poznate benefite ove tranzicije, javlja se niz problema koje je potrebno otkloniti kako bi postojeće usluge iz fizičkog svijeta bilo moguće zamijeniti digitalnima.

Jedna takva usluga, koja još nije u potpunosti digitalizirana, je razmjena dokumenata i ostalih datoteka uz očuvanje sigurnosnih značajki. Sustavi koji pružaju ovakve usluge moraju implementirati sigurnosne elemente primjenjive u fizičkom svijetu, poput potvrde vlasništva, a nerijetko ih i proširuju s konceptima koji nisu mogući izvan digitalnih sustava

U ovom diplomskom radu opisana je usluga elektroničkog potpisivanja datoteka u skladu s regulacijama Europske Unije.

U prvom poglavlju opisani su koncepti kriptografije temeljene na privatnom ključu na kojima se temelji čitava infrastruktura elektroničkih potpisa.

Iduće poglavlje sažima bitne značajke europske regulative koje je potrebno ispuniti prilikom implementacije elektroničkih potpisa.

Detaljniji pregled AdES razine digitalnih potpisa definiranih prethodno navedenom regulativom izložen je u trećem poglavlju.

U četvrtom poglavlju istražuje se DSS biblioteka čiji je cilj podržati interoperabilno i sigurno stvaranje i verifikaciju elektroničkih potpisa.

Zadnja dva poglavlja opisuju arhitekturu realiziranog sustava i implementacijske detalje bitne za razumijevanje sustava. Povrh toga, dan je pregled tehnologija i odluka prilikom dizajniranja sustava.

# Digitalni potpisi

Digitalni potpis je matematički postupak kojim se utvrđuje autentičnost i integritet digitalne poruke odnosno dokumenta. Često se naziva i digitalni otisak prsta (engl. f*ingerprint*) jer može jedinstveno predstavljati osobnu ili bilo koji drugi entitet. Ispravno izrađen digitalni potpis može služiti kao dokaz o podrijetlu, vremenu, identitetu i statusu digitalnog dokumenta.[1]

Nazivi digitalni potpis i elektronski potpis se često koriste proizvoljno i naizmjenično iako se konceptualno razlikuju. Elektronski potpis je bilo koji elektronski podatak koji je povezan s nekim drugim elektronskim podatkom s namjerom potpisivanja toga podatka. Elektronski potpis može biti zvuk, simbol, ilustracija i sl. Elektronske potpise odlikuje lakoća korištenja uz relativno nisku razinu sigurnosti. Nerijetko se koriste za potpisivanje ugovora putem web-a.[2]

Digitalni potpisi su podskup elektroničkih potpisa, odnosno specifična implementacija elektroničkih potpisa. Kategorije elektroničkih potpisa su brojne, a razlikuju se prema tehničkoj implementaciji, pravnoj prihvaćenosti, geografskom području, itd.

Mnoge industrije i geografske regije su uspostavile standarde za digitalne potpise. Ispravno praćenje i implementacija ovih standarda omogućava brojne organizacijske, sigurnosne i pravne benefite.

## Asimetrična kriptografija

Digitalni potpisi temelje se na asimetričnoj kriptografiji (kriptografija javnog ključa) iz čega proizlaze njihova sigurnosna svojstva. Neki od najčešće korištenih algoritama su RSA, DSA, ECDSA, EdDSA.

Privatni ključ definira transformaciju potpisa SA:

|  |  |  |
| --- | --- | --- |
|  |  | (1) |

Javni ključ definira transformaciju verifikacije VA:

|  |  |  |
| --- | --- | --- |
|  |  | (2) |

Verifikacija je uspješna ako i samo ako je ispunjeno[3]:

|  |  |  |
| --- | --- | --- |
|  |  | (3) |

Tehnologija digitalnih potpisa zasniva se na povjerenju da entitet koji je napravio potpis ima isključivi pristup pripadajućem privatnom ključu. U slučaju da je privatni ključ kompromitiran, moguće je stvaranje potpisa koje nije stvorio vlasnik ključa.

Princip potpisivanja bazira se na tzv. „Hash and Sign“ paradigmi u kojoj se potpisuje hash vrijednost podatka umjesto samog podatka. Slika 2.1 ilustrira ovaj postupak.



Slika 2.1 Dijagram potpisa i verifikacije podataka (izvor: <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq>, preuzeto 18.8.2021.)

### RSA potpisivanje

Prethodno spomenutu „Hash and Sign“ paradigmu moguće je implementirati koristeći RSA algoritam. Matematički opis digitalnog potpisa koristeći RSA algoritam je izložen u nastavku.

Neka je zadan ulazni podatak M. U prvom koraku računa se hash vrijednost podatka M koristeći jednu od kriptografskih funkcija (npr. SHA256):

|  |  |  |
| --- | --- | --- |
|  |  | (4) |

Na dobivenu hash vrijednost primjeni se PKCS #1 formatiranje:

|  |  |  |
| --- | --- | --- |
|  |  | (5) |

Formatirana vrijednost se enkriptira koristeći prethodno generirani privatni ključ (e, n):

|  |  |  |
| --- | --- | --- |
|  |  | (6) |

Dobivena vrijednost je potpis ulaznog podatka M.

Provjeru potpisa moguće je napraviti ako su poznati ulazni podatak M i potpis . U prvom koraku potrebno je dohvatiti autentični javni ključ (d, e) te izračunati:

|  |  |  |
| --- | --- | --- |
|  |  | (7) |

se obradi PKCS #1 formatiranjem. U ovom koraku moguće je odbaciti dobiveni rezultat u slučaju da nije dobro formatiran.

Izračuna se hash vrijednost ulaznog podatka:

|  |  |  |
| --- | --- | --- |
|  |  | (8) |

Digitalni potpis može biti prihvaćen ako i samo ako vrijedi:

|  |  |  |
| --- | --- | --- |
|  |  | (9) |

U suprotnom, potpis treba biti odbačen jer javni ključ ne odgovara privatnom ključu kojim je izračunat potpis ili ulazni podatak ne odgovara originalnom ulaznom podatku.

## PKI

Sustav digitalnog potpisivanja mora omogućiti provjeru vlasništva javnog ključa. Drugim riječima, potrebno je odgovoriti na pitanje kako znati da korišteni javni ključ entiteta pripada upravo tom entitetu.

Infrastruktura javnog ključa (PKI) omogućava tu funkcionalnost pri čemu asocijaciju između javnog ključa i entiteta potvrđuje operater PKI-a tj. certifikacijsko tijelo (engl. *Certificate authority*).

PKI se sastoji od politika, standarda, ljudi i sustava koji podržavaju distribuciju javnih ključeva i provjeru identiteta pojedinaca ili subjekata s digitalnim certifikatima i tijelom za izdavanje certifikata.[4]

PKI se sastoji od[5]:

* CA – pohranjuje, izdaje i potpisuje digitalne certifikate
* RA – provjerava identitet subjekata koji zahtjevaju pohranu pohranu vlastitog digitalnog certifikata od CA
* Centralni direktorija – sigurna lokacija u kojoj su certifikati (zajedno s javnim ključevima) pohranjeni
* Sustav upravljanja certifikatima

Postoje sigurnosna ograničenja vezana uz PKI. Glavna slabost javnog PKI je što bilo koji CA može potpisati certifikat za bilo koji entitet. CA postoje u brojnim državama, među kojima su i one s autoritarnim i potencijalno neprijateljskim režimima. Nepovjerljivi CA mogu izdati certifikate s namjerom špijunaže, krivotvorenja poruka ili dokaza te brojnih drugih prevara. Zbog toga povjerenje u javne CA i certifikate koje su izdali mora biti ograničeno.[6]

Neke organizacije stvaraju vlastite PKI. To znači da imaju kontrolu nad CA. Kada organizacija daje povjerenje isključivo internom CA za neku svrhu, šansa za prijevarno izdavanje certifikata može biti smanjena u odnosu na javni CA pod uvjetom da je interni PKI implementiran ispravno.

## X.509

X.509 je standard koji definira format digitalnih certifikata. Bez obzira na primjenu, svaki X.509 certifikat sadrži javni ključ, digitalni potpis, informacije o subjektu vezanog uz taj certifikat i tijelu koje ga je izdalo. Pored tih informacija, može sadržavati i informacije o verziji, periodu u kojem je valjan, a verzija 3 definira skup proširenja koji definiraju dodatne informacije o certifikatu.[7]

Slika 2.1 prikazuje digitalni certifikat web stranice FESB-a dohvaćen preglednikom Google Chrome.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 2.2 Digitalni certifikat web stranice FESB-a

Zbog administrativnih i sigurnosnih razloga, X.509 certifikate se obično povezuju u lance. Slika 2.3 prikazuje takav lanac certifikata na primjeru FESB-ovog certifikata.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 2.3 Lanac certifikata

Web poslužitelji obično šalju svoj krajnji certifikat i posredne certifikate koji su potrebni za provjeru lanca. Certifikat na vrhu lanca i njegov pripadajući javni ključ (Sectigo (AAA) u ovom slučaju) su obično pohranjeni u operacijski sustav ili preglednik korisnika čime se uspostavlja lanac povjerenja.

### Opoziv certifikata

X.509 certifikate moguće je opozvati prije formalnog isteka njihovog trajanja. RFC 5280 definira liste opoziva certifikata (engl. *Certificate Revocation List*). CRL je potpisana lista opozvanih certifikata s vremenskim žigom koju CA obično obnavlja u regularnim intervalima. Klijentski softver može postavljati upite na ovu listu kako bi utvrdio valjanost digitalnog certifikata.

U praksi su se CRL pokazale nepraktične zbog nemogućnosti skaliranja. RFC 2560 definira OCSP koji daje mogućnost provjere certifikata bez pretraživanja liste opoziva. CA obično održava jednostavni HTTP poslužitelj koji odgovaraju na OCSP zahtjeve. Klijentski softver šalje HTTP zahtjev OCSP poslužitelju koji vraća potpisani odgovor o valjanosti certifikata.

RFC 6066 definira proširenje OCSP-a pod nazivom „OCSP Stapling“ koje rješava potencijalne probleme s performansama i sigurnosti OCSP-a.

Kod ove tehnike web poslužitelji u ime klijenata dohvaćaju OCSP odgovore za vlastiti certifikat te ga obično pohrane u privremenu memoriju i do 7 dana. Poslužitelj tada može poslati OCSP odgovor prilikom uspostave TLS veze (engl. *TLS handshake)* čime se smanjuje broj HTTP zahtjeva koje klijent mora poslati.[8]

# eIDAS uredba

Uredba (EU) br. 910/2014 Europskog parlamenta i vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu iznesena je 23. srpnja 2014. godine [2.1].

eIDAS igra ključnu ulogu u omogućavanju sigurnih prekograničnih transakcija. To je svojevrsna prekretnica u stvaranju predvidivog regulatornog okvira na području EU. Cilj je pomoći tvrtkama, privatnim osobama i javnim ustanovama u izvršavanju elektronskih radnji na jednostavan i siguran način.

S ovom uredbom, EU je postavila temelje i pravni okvir za sve sudionike kako bi na siguran način i uz manje prepreka pristupali elektroničkim uslugama. U tom smislu, eIDAS omogućuje usluge poput prijave poreza, upisa na sveučilišta diljem Europe, uspostavljanja tvrtke u zemljama članicama, itd.

Uredba je postala potpuno primjenjiva gotovo dvije godine nakon uvođenja, a od 29. rujna 2018. sve organizacije koje pružaju digitalne usluge unutar zemlje članice EU moraju priznati elektronsku identifikaciju definiranu ovom uredbom.[2.2] Slika 3.1 prikazuje značajne događaje u razvoju eIDAS uredbe.



Slika 3.1 Vremenska traka razvoja eIDAS uredbe (izvor: https://www.eid.as/, preuzeto 17.8.2021.)

Iste godine kada je priznavanje elektronske identifikacije postalo obavezno na razini EU, vodeći Europski stručnjaci, organizacije i udruženja u području elektronske identifikacije su pokrenuli neprofitnu inicijativu go.eIDAS.

Cilj organizacije je podizanje svijesti kroz stvaranje lokaliziranog informativnog materijala, implementaciju i održavanje softvera te brojne druge aktivnosti kojima se promoviraju benefiti uredbe.

Slika 3.2 ilustrira ideju uredbe o jedinstvenom EU tržištu i olakšanom prekograničnom pristupu javnim uslugama.



Slika 3.2 Jedinstveno elektroničko EU tržište (izvor: <https://en.wikipedia.org/wiki/EIDAS#/media/File:E-SENS_architecture.jpg>, preuzeto 17.8.2021.)

eIDAS definira okvir za sljedeće aspekte elektronskih transakcije:

* Napredni elektronski potpisi (engl. *Advanced electronic signature)*
* Kvalificirani elektronski potpisi (engl. *Qualified electronic signature)*
* Kvalificirani digitalni certifikati (engl. *Qualified digital certificate)*
* Kvalificirani autentifikacijski certifikati za web stranice (engl. *Qualified website authentication certificate)*
* Usluge povjerenja (engl. *Trust service*) koje uključuju stvaranje i verifikaciju elektronskih pečata i potpisa, vremenskih oznaka (engl. *Timestamps)* i certifikata)

U narednom poglavlju detaljnije će biti obrađeni napredni elektronski potpisi koji su temelj implementiranog sustava za digitalno potpisivanje dokumenata.

U sklopu izrade sustava za digitalno potpisivanje dokumenata bitno je uzeti u obzir ovu regulativu jer su njome definirani brojni pravni učinci koje je moguće ostvariti uz poštivanje implementacijskih smjernica.

Prema čl. 46 ove uredbe, elektronički dokumenti se mogu koristiti kao dokaz u sudskim postupcima te im se ne smije uskratiti pravni učinak isključivo zato jer su u elektroničkom obliku.

## Kvalificirani elektronski potpisi

Kvalificirani elektronski potpis je napredni elektronski potpis izrađen uz pomoć uređaja za izradu kvalificiranih elektronskih potpisa (engl. *Qualified signature creation device)* koristeći kvalificirani digitalnih certifikat.

Kvalificirani digitalni certifikat mora biti izdan od strane kvalificiranog izdavatelja usluga povjerenja (engl. *Trust service provider*). Time se osigurava autentičnost elektronskog potpisa te on može služiti kao dokaz identiteta. U Republici Hrvatskoj postoje tri aktivna TSP-a: AKD d.o.o., FINA i Zagrebačka banka d.d.[3.3]

QES omogućava provjeru autorstva u elektronskoj razmjeni podataka u dugom roku te je prema čl. 25 uredbe ekvivalentan rukom napisanom potpisu.

QSCD je podvrsta uređaja za izradu sigurnih potpisa (engl. *Secure signature creation* device) koji ispunjavaju uvjete navedene u eIDAS uredbi. Potpunu listu uvjeta koje ovi uređaji moraju ispuniti moguće je pronaći u prilogu 2 uredbe.

U sklopu ovoga rada neće se dalje razmatrati ova vrsta potpisa zbog nemogućnosti nabave kvalificiranog certifikata i QSCD-a u svrhu testiranja i prezentacije.

# AdES razina digitalnih potpisa

# DSS

# Arhitektura sustava

# Implementacija sustava

# Zaključak

# Literatura

[1] Paul, E.: „What are digital signatures: how it works, benefits, objectives, concept“, s Interneta, <https://www.emptrust.com/blog/benefits-of-using-digital-signatures>, 18.8.2021.

[2] Mark, T.: „Difference between digital signature and electronic signature“, s Interneta, <http://www.differencebetween.net/technology/difference-between-digital-signature-and-electronic-signature/>, 18.8.2021.

[3] Čagalj, M.: „Asymmetric key cryptography“, ak.god. 2020./2021.

[4] CISA: Security Tip (ST04-018), Understanding Digital Signatures, 24.8.2020

[5] Vacca, Jhn R..: „Public Key Infrastructure: Building Trusted Applications and Web Services“, 2004

[6] SSH.com: „What is PKI (Public Key Infrastructure)?“, s Interneta, <https://www.ssh.com/academy/pki>, 19.8.2021.

[7] Cooper, et al.: RFC5280 Internet X.509 Public Key Infrastructure Certificate

[8] Naziridis, N.: „Page Load Optimization: OCSP Stapling“, s Interneta, <https://www.ssl.com/article/page-load-optimization-ocsp-stapling/>, 8.2.2019.

and Certificate Revocation List (CRL) Profile, Svibanj 2008

[2.1] Službeni list Europske unije, L 257/73, 28.8.2014.

[2.2] go.eIDAS: „About“, s Interneta, <https://go.eid.as/#about>, 17.8.2021.

[2.3] European commission: „Trusted List Croatia“, s Interneta, <https://webgate.ec.europa.eu/tl-browser/#/tl/HR>, 17.8.2021.

# Popis oznaka i kratica

RSA - Rivest–Shamir–Adleman

DSA – Digital Signature Algorithm

ECDSA – Elliptic Curve Digital Signature Algorithm

EdDSA – Edwards-curve Digital Signature Algorithm

PKI – Public key infrastructure

CA – Certificate Authority

RA – Registration Authority

CRL – Certificate Revocation List

OCSP – Online Certificate Status Protocol

TSP – Trusted source provider

QES – Qualified electronic signature

QSCD – Qualified signature creation device

# Sažetak

# Summary

# Prilozi

## Kazalo slika

[Slika 2.1 Dijagram potpisa i verifikacije podataka (izvor: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq, preuzeto 18.8.2021.) 3](#_Toc80293094)

[Slika 2.2 Digitalni certifikat web stranice FESB-a 6](#_Toc80293095)

[Slika 2.3 Lanac certifikata 7](#_Toc80293096)

[Slika 3.1 Vremenska traka razvoja eIDAS uredbe (izvor: https://www.eid.as/, preuzeto 17.8.2021.) 9](#_Toc80293097)

[Slika 3.2 Jedinstveno elektroničko EU tržište (izvor: https://en.wikipedia.org/wiki/EIDAS#/media/File:E-SENS\_architecture.jpg, preuzeto 17.8.2021.) 10](#_Toc80293098)