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](#_Toc80719535)

[2 Digitalni potpisi 2](#_Toc80719536)

[2.1 Asimetrična kriptografija 2](#_Toc80719537)

[2.1.1 RSA potpisivanje 3](#_Toc80719538)

[2.2 PKI 5](#_Toc80719539)

[2.3 X.509 6](#_Toc80719540)

[2.3.1 Opoziv certifikata 7](#_Toc80719541)

[3 eIDAS uredba 9](#_Toc80719542)

[3.1 Kvalificirani elektronski potpisi 11](#_Toc80719543)

[4 AdES digitalni potpisi 13](#_Toc80719544)

[4.1 AdES razine 14](#_Toc80719545)

[4.2 XAdES 15](#_Toc80719546)

[4.2.1 Pohrana potpisa 17](#_Toc80719547)

[4.3 PAdES 18](#_Toc80719548)

[4.3.1 Sintaksa 20](#_Toc80719549)

[4.4 CAdES 21](#_Toc80719550)

[4.4.1 Sintaksa 22](#_Toc80719551)

[4.5 Kriptografski algoritmi 24](#_Toc80719552)

[4.5.1 Prihvaćeni algoritmi 24](#_Toc80719553)

[5 DSS 27](#_Toc80719554)

[5.1 Apstrakcija podataka 28](#_Toc80719555)

[5.2 Potpisivanje 28](#_Toc80719556)

[5.3 Provjera valjanosti potpisa 33](#_Toc80719557)

[5.3.1 Politika valjanosti 37](#_Toc80719558)

[5.4 Upravljanje povjerenjem 37](#_Toc80719559)

[5.5 Izvori informacija o opozivu 38](#_Toc80719560)

[6 Arhitektura sustava 40](#_Toc80719561)

[6.1 Web aplikacija 40](#_Toc80719562)

[6.2 Servis za potpisivanje 44](#_Toc80719563)

[6.3 Servis za upravljanje digitalnim potpisima 44](#_Toc80719564)

[6.4 CRL poslužitelj 45](#_Toc80719565)

[6.5 OCSP poslužitelj 45](#_Toc80719566)

[6.6 Baza podataka 45](#_Toc80719567)

[7 Implementacija sustava 47](#_Toc80719568)

[8 Zaključak 48](#_Toc80719569)

[Literatura 49](#_Toc80719570)

[Popis oznaka i kratica 51](#_Toc80719571)

[Sažetak 52](#_Toc80719572)

[Summary 53](#_Toc80719573)

[Prilozi 54](#_Toc80719574)

[Kazalo slika 54](#_Toc80719575)

# 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 zahtijevaju 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 [10].

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.[11] 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.[12]

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 digitalni potpisi

Napredni elektronski potpis (engl. *Advanced electronic signature*) je elektronski potpis koji odgovara zahtjevima postavljenim EU uredbom eIDAS. Napredni elektronski potpisi moraju ispuniti stroge uvjete definirane uredbom. AdES elektronski potpis mora[9]:

* jedinstveno i nedvosmisleno biti povezan s entitetom koji ga je potpisao
* identificirati entitet koji ga je potpisao
* biti potpisan kroz sredstva koja su u potpunoj kontroli entiteta koji ga potpisuje, drugim riječima privatni ključ ne smije biti kompromitiran
* omogućiti provjeru integriteta popratnih podataka nakon potpisivanja te biti poništen u slučaju modifikacije

Ovakvi potpisi mogu se implementirati kroz AdES osnovne profile (engl. *AdES baseline profiles*) koje razvija ETSI:

* XAdES – XML AdES je skup proširenja na XML-DSig preporuku definiran standardom ETSI TS 103171 v.2.1.1
* CAdES – CMS AdES je skup proširenja sintaksi kriptografske poruke (engl. *Cryptographic message syntax*) definiran standardom ETSI TS 103173 v.2.2.1
* PAdES – PDF AdES je skup ograničenja i proširenja na PDF i ISO 32000-1 definiran standardom ETSI TS 103172 v.2.2.2
* ASiC – povezani spremnici potpisa (engl. *Associated Signature Containers*) definiraju korištenje struktura kojima se povezuje jedan ili više potpisanih objekata s naprednim elektronskim potpisom ili vremenskim žigom u jedan digitalni spremnik najčešće zip formata; definiran standardom ETSI TS 103174 v.2.2.1
* JAdES – JSON AdES je skup proširenja na JWS definiran standardom ETSI TS 119182-1

Brojne opcije, postavke i verzije ovih gore navedenih standarda otežavaju interoperabilnost zbog čega su novi, osnovni (engl. b*aseline*) profili objavljeni. Njihov je cilj ograničiti broj opcija i varijanti te time poboljšati interoperabilnost između sudionika.

Tablica 1 daje prikaz mogućnosti potpisivanja različitih vrsta podataka gore navedenim profilima.

Tablica 1 Vrste potpisa i formati podataka

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Profil potipsa** | | | **XML** | **JSON** | **PDF** | **Binarni podatak** | **Digest** | **Više datoteka** | **Više potpisa** | **Protupotpis** |
| XAdES | Enveloping | Base64 encoded | ✔ | ✔ | ✔ | ✔ | ❌ | ✔ | ❌ | ✔ |
| Embed XML | ✔ | ❌ | ❌ | ❌ | ❌ | samo XML | ❌ | ✔ |
| Manifest | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ❌ | ✔ |
| Canonicalization | ✔ | ❌ | ❌ | ❌ | ❌ | samo XML | ❌ | ✔ |
| Enveloped | enveloped transformation | ✔ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ✔ |
| based on XPath | ✔ | ❌ | ❌ | ❌ | ❌ | ❌ | ✔ | ✔ |
| based on Filter2 | ✔ | ❌ | ❌ | ❌ | ❌ | ❌ | ✔ | ✔ |
| Canonicalization | ✔ | ❌ | ❌ | ❌ | ❌ | samo XML | ✔ | ✔ |
| Detached | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ❌ | ✔ |
| Internally Detached | | ✔ | ❌ | ❌ | ❌ | ❌ | samo XML | ✔ | ✔ |
| CAdES | Enveloping | | ✔ | ✔ | ✔ | ✔ | ❌ | ❌ | ✔ | ✔ |
| Detached | | ✔ | ✔ | ✔ | ✔ | ✔ | ❌ | ✔ | ✔ |
| PAdES | Enveloped | | ❌ | ❌ | ✔ | ❌ | ❌ | ❌ | ✔ | ❌ |

## AdES razine

Dokumenti i drugi podatci mogu biti u uporabi dugi niz godina. U tom vremenskom periodu certifikati mogu isteći, CA može izgubiti akreditaciju, korišteni algoritmi postati ranjivi, itd.

Novi ETSI standard definira četiri razine sukladnosti kojima se rješava problem valjanosti potpisa kroz vrijeme[12]:

* B – (engl. *Basic electronic signature*) – najniža i najjednostavnija izvedba koja sadrži podatke o potpisu, ključu i dodatnim svojstvima potpisa
* T – (engl. *Signature with a timestamp*) – vremenski žig povjerljivog izvora dodan prethodnoj razini u svrhu zaštite protiv odricanja od odgovornosti (engl. *repudiation*)
* LT – (engl. *Signature with Long Term data) –* certifikati i podatci o opozivu su ugrađeni u potpis čime se omogućuje provjera čak i ako originalni izvori nisu dostupni
* LTA – (engl. *Signature with Long Term Dana and Arhive timestamp)* – periodičkim dodavanjem vremenskog žiga sprječava se kompromitacija potpisa kao posljedica slabljenja sigurnosti korištenih algoritama

B razina sadrži nepromjenjive (engl. *immutable*) potpisane podatke. Jednom kada je potpis ove razine izrađen njegovi se podaci ne mogu mijenjati.

Razine T, LT i LTA dodaju nepotpisane podatke potpisu. To znači da se podaci ovih razina mogu dodati naknadno na bilo koji AdES potpis. Proširenje ovim razinama može učiniti potpis sigurnijim u dugom roku. Proširenja se rade inkrementalno, odnosno, kada se napravi proširenje na LT razinu, niža razina T je također dodana.

U praksi je moguće napraviti potpis direktno bilo kojom od ove četiri razine.[12]

## XAdES

XAdES je skup proširenja na XML-DSig preporuku koja implementiraju zahtjeve naprednih elektronskih potpisa. Organizacije W3C i ETSI rade na održavanju i ažuriranju.[13]

XAdES je čitljiv čovjeku i računalima što ga čini pogodnim za brojne uporabe, a zbog svojih svojstava njime je moguće potpisati čitav niz različitih vrsta podataka.

Slika 4.1 prikazuje pojednostavljeni dijagram XAdES potpisa koji ilustrira podatke koji se dodaju originalnoj XML-DSig preporuci.



Slika 4.1 XAdES dijagram

XAdES podaci se dodaju u ds:Object element XML-DSig strukture. Potpisana polja se nalaze pod elementom SignedProperties, dok se nepotpisana nalaze pod elementom UnsignedProperties.

Slika 4.2 prikazuje XML strukturu XAdES-Baseline-B.



Slika 4.2 XAdES-Baseline-B XML struktura

Obavezni podatci u polju SignedProperties su:

* jednoznačna referenca na certifikat autora potpisa - SigningCertificate
* jednoznačan način identifikacije politike potpisa pod kojom je potpis izrađen kako bi prilikom verifikacije bilo moguće ostvariti iste uvjete - SignaturePolicyIdentifier
* vrijeme potpisa (u ovom slučaju to nije nužno povjerljivi vremenski žig) - SigningTime

Potpis također može pokriti i ostala polja koja sadržavaju sljedeće informacije:

* format jednog ili više podatka koji su potpisani - DataObjectFormat
* vrsta opredjeljenja (engl. *commitment*) autora potpisa prilikom potpisivanja podataka u kontekstu odabrane politike potpisa; politika potpisa može imati višestruku pravnu interpretaciju - CommitmentTypeIndication
* tvrđena ili ovjerena uloga koju autor potpisa preuzima pri izradi potpisa - SignerRole
* navodno mjesto na kojem autor potpisa tvrdi da je izradio potpis - SignatureProductionPlace

Autor potpisa ili entitet koji obavlja provjeru može izraditi XAdES-Baseline-T dodavanjem djeteta elementu UnsignedProperties. Povjerljivi vremenski žig SignatureTimeStamp dokazuje da je elektronski potpis postojao prije naznačenog vremena.

Ostale razine na sličan način dodaju potrebne podatke kao djecu nepotpisanog XML elementa UnsignedProperties. To mogu biti lanci certifikata, liste opoziva, OCSP odgovori i sl.

### Pohrana potpisa

Potpis mora biti povezan s podatkom na koji se odnosi. To je moguće napraviti stvaranjem novog podatka koji obuhvaća potpis i originalni podatak ili pohranom potpisa u vanjski resurs te naknadnim povezivanjem podatka s potpisom.

Za XML datoteke moguće je izraditi omotnicu koja sadržava izvornu XML strukturu i potpis dok za binarne podatke to nije trivijalno napraviti.

XAdES definira načine ugrađivanja potpisa kroz sljedeće načine rada:

* Omotan (engl. *Enveloped*) – potpis se odnosi na podatak koji ga omeđuje
* Obavijajući (engl. *Enveloping*) – podatak koji se potpisuje je pod element samog potpisa
* Odvojen (engl. *Detached*) – potpis se odnosi na podatak od kojeg je odvojen
* Interno odvojen (engl. *Internally-detached*) – primjenjiv samo za XML podatke, potpis i podatak koji je potpisan su unutar elementa roditelja

## PAdES

PAdES je skup ograničenja i proširenja na PDF i ISO 32000-1 koja implementiraju zahtjeve naprednih elektronskih potpisa. PDF i ISO 32000-1 definiraju okvir za digitalno potpisivanje dokumenata, a PAdES definira profile kojima ih čini usklađenim s AdES standardom.

Digitalni potpisi u okviru ISO 32000-1 podržavaju tri značajke: dodavanje digitalnog potpisa dokumentu, rezerviranje mjesta za potpis u budućnosti i provjeru valjanosti potpisa. Potpis i ostale informacije se nalaze u strukturi PDF-a zvanoj rječnik potpisa (engl. *signature dictionary*).[14]

Hash vrijednost se računa na temelju niza bajtova PDF datoteke uključujući i rječnik potpisa, ali isključujući potpis sam. Raspon u kojem se obavlja hash je definiran ByteRange poljem rječnika potpisa. Time se osigurava da su svi bajtovi datoteke pokriveni osim samog potpisa.

Slika 4.3 prikazuje primjer takvog potpisa za potpis između bajtova 840 i 960 pri čemu je raspon bajtova zadano kao niz uređenih parova (početak, pomak).



Slika 4.3 ISO32000-1 PDF potpis

Binarna vrijednost PDF potpisa postavljena je u Contents unos rječnika potpisa. Veličina Contents polja se računa na temelju procjene maksimalne veličine potrebne za pohranu potpisa i dodatnih podataka poput podataka o opozivu i vremenskih žigova. Vrijednost potpisa je inicijalno zapisana na disk kao niz 0x00 heksadecimalnih vrijednosti te je naknadno popunjena sa stvarnom vrijednošću.[15]

Slika 4.4 prikazuje detaljniji pogled na rječnik potpisa i njegov sadržaj.



Slika 4.4 Rječnik potpisa

### Sintaksa

PAdES profili proširuju ISO 32000-1 standard s alternativnim kodiranjem potpisa dodavajući potpisane i nepotpisane atribute ekvivalentne CAdES formatu potpisa.

DER kodirani SignedData objekt mora biti dodan u Contents unos rječnika potpisa. Može postojati samo jedan autor potpisa, odnosno, može postojati samo jedan objekt tipa SignerInfo unutar SignerInfos elementa u bilo kojem PDF potpisu.

Zahtjevi za rukovanjem PDF potpisima navedeni u ISO 32000-1 standardu se primjenjuju osim ako nisu nadjačani u ETSI 319 142-1 standardu.

Neki atributi imaju isto ili slično značenje kao ključevi rječnika potpisa opisanim u ISO standardu. Takvi atributi i ključevi se interpretiraju prema tablici koju definira ETSI standard.

Za potrebe produljenja životnog vijeka PDF potpisa, ETSI definira dodatna proširenja na ISO standard. Za potpunu provjeru digitalnog potpisa potrebni su podatci poput lanca certifikata, liste opoziva, OCSP odgovori, itd.

Sigurno spremište dokumenata (engl. *Document security store*) je proširenje koje definira pohranu svih podataka potrebnih za provjeru potpisa. Opcionalno se dodaje i polje podataka povezanih s provjerom valjanosti (engl. *Validation related information*) koje povezuje podatke s konkretnim potpisom.

Životni vijek valjanosti potpisa produljuje se na način da se dodaju dodatne informacije u DSS prilikom dodavanja vremenskih žigova. Svako inkrementalno ažuriranje DSS-a zahtjeva očuvanje vrijednosti prethodnog DSS-a.

## CAdES

CAdES je skup proširenja sintaksi kriptografske poruke (engl. *Cryptographic message syntax*) koja implementiraju zahtjeve naprednih elektronskih potpisa.

CMS je IETF standard definiran kroz RFC5652 koji opisuje sintaksu za zaštitu podataka. Podržava digitalne potpise i enkripciju. Sintaksa podržava višestruku enkapsulaciju što u omogućava višestruko potpisivanje podataka.

Također omogućeno je potpisivanje proizvoljnih atributa, poput vremena potpisa i protu potpisa, uz sam podatak koji se potpisuje.

CMS vrijednosti su definirane koristeći ASN.1 standard uz BER kodiranje pri čemu su vrijednosti obično niz okteta.

CMS standard je dovoljno generalan da može podržavati brojne vrste sadržaja. ContentInfo enkapsulira jednu identificiranu vrstu sadržaja, a identificirani tip može osigurati daljnju enkapculaciju.

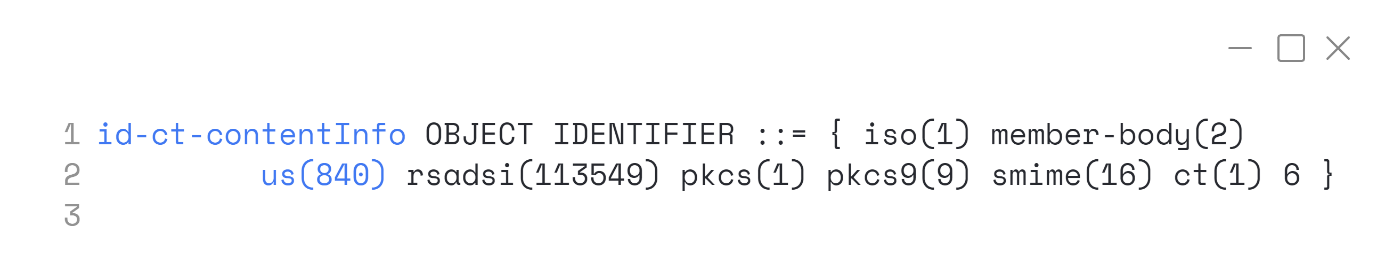
Svaka vrsta sadržaja omogućava obradu u jednom prolasku (engl. *single pass processing*) koristeći BER kodiranje proizvoljne duljine. Operacija jednog prolaska daje dobre rezultate kod velikih podataka i u slučajevima kada nasumičan pristup podacima nije moguć (npr. podatak dolazi kroz cjevovod iz drugog procesa).

Ova operacija nije trivijalna kada je potrebno napraviti DER kodiranje jer duljine različitih komponenti nisu unaprijed poznate. Potpisani atributi unutar signed-data sadržaja i ovjereni atributi unutar authenticated-data sadržaja moraju biti preneseni u DER formatu kako bi primatelji mogli provjeriti sadržaj koji sadrži jedan ili više nepoznatih atributa.

Potpisani i ovjereni atributi su jedine vrste podataka u CMS-u koje zahtijevaju DER kodiranje.[16]

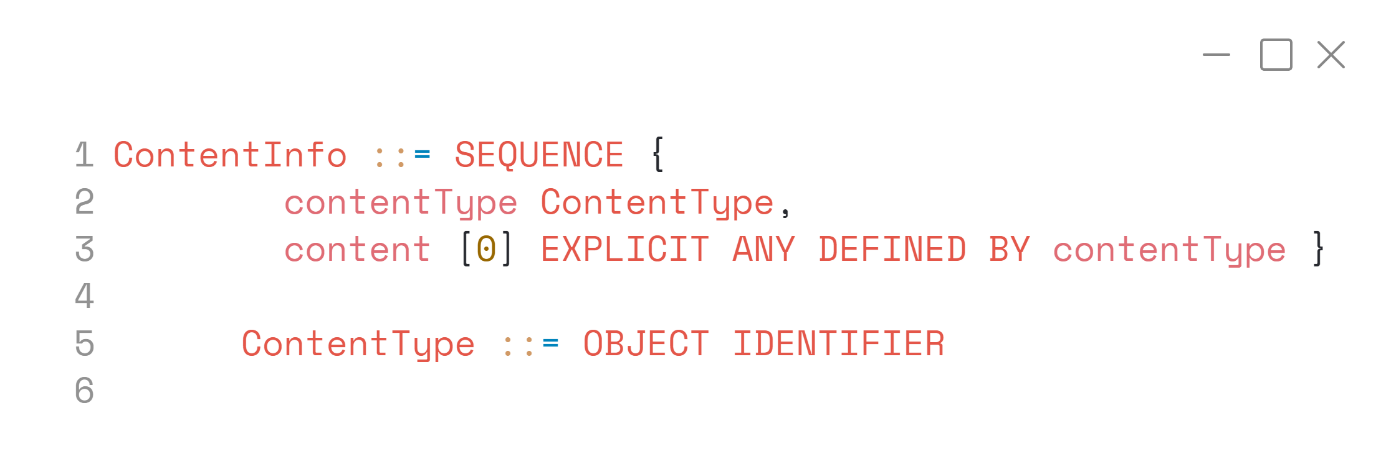
### Sintaksa

Slika 4.5 prikazuje identifikator objekta koji identificira vrstu sadržaja:



Slika 4.5 Identifikator vrste sadržaja

CMS povezuje identifikator vrste sadržaja sa sadržajem. Sintaksa mora sadržavati ASN.1 tip ContentInfo. Slika 4.5 prikazuje definiciju tipa.



Slika 4.6 Definicija ContentInfo tipa

ContentType označava vrstu sadržaja. To je identifikator objekta u obliku jedinstvenog niza koji dodjeljuje tijelo koje definira taj tip.

Slika 4.5 ilustrira osnovni tip-vrijednost format koji se koristi u CMS-u.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 4.7 Osnovni CMS tip-vrijednost format

Standard definira 6 vrsta podataka:

* Data – koristi se za proizvoljni niz okteta (npr. tekst) i u pravilu je sadržan u ostalim tipovima
* Signed-Data – koristi se za digitalno potpisivanje sadržaja
* Enveloped-Data – sadrži enkriptirani sadržaj zajedno s jednim dekripcijskim ključem po primatelju
* Digested-Data – sadrži podatke i hash vrijednost sadržaja
* Encrypted-Data – sadrži samo enkriptirane podatke
* Authenticated-Data – sadrži podatak, MAC i enkriptirane autentikacijske ključeve za jednog ili više primatelja

Slika 4.6 ilustrira format za digitalno potpisivanje koji se koristi u CMS-u.

Slika na kojoj se prikazuje stol

Opis je automatski generiran

Slika 4.8 CMS Signed-Data tip formata

## Kriptografski algoritmi

Odabir kriptografskih algoritama koji se primjenjuju kroz digitalne potpise bitan je parametar usluga koje implementiraju digitalne potpise. Jedan od bitnih faktora prilikom odabira algoritama je interoperabilnost. ETSI standard delegira procjenu sigurnosti kriptografskih algoritama SOG-IS Crypto WG grupi kako bi se izbjegli konflikti prilikom evaluacije sigurnosti pojedinih usluga i proizvoda.[17]

Druga standardizacijska tijela i agencije zemalja članica objavljuju slične dokumente s djelomično preklapajućim opsegom preporuka. Takvi dokumenti mogu se iskoristiti kao dodatni materijali prilikom projektiranja implementacije usluga i proizvoda.

SOG-IS evaluacijski okvir razlikuje dvije vrste mehanizama:

* naslijeđene (engl. *legacy*) – algoritmi i parametri koji su široko korišteni, ali ne predstavljaju moderno, „state of the art“, kriptografsko rješenje
* predložene (engl. *recommended*) – „state of the art“ kriptografski algoritmi i parametri

U generalnom slučaju, digitalni potpisi trebali bi biti izrađeni predloženim algoritmima i parametrima osim kada postoji zahtjev za interoperabilnost s postojećim sustavima.

SOG-IS grupa provodi reviziju svake dvije godine ili neposredno nakon otkrivanja ranjivosti.

### Prihvaćeni algoritmi

Tablica 2 prikazuje skup hash funkcija koje prihvaća SOG-IS grupa pri čemu se SHA-224 ne smatra preporučenom funkcijom.[18]

Tablica 2 SOG-IS prihvaćene hash funkcije

|  |  |
| --- | --- |
| **Hash funkcija** | **Reference** |
| SHA-224 | FIPS publikacija 180-4 |
| SHA-256 | FIPS publikacija 180-4 |
| SHA-384 | FIPS publikacija 180-4 |
| SHA-512 | FIPS publikacija 180-4 |
| SHA-512/256 | FIPS publikacija 180-4 |
| SHA3-256 | FIPS publikacija 202 |
| SHA3-384 | FIPS publikacija 202 |
| SHA3-512 | FIPS publikacija 202 |

SHA-1 nije prihvaćena funkcija ali HMAC-SHA-1 je prihvaćen i ne smatra se preporučenom funkcijom.

Tablica 3 prikazuje skup algoritama za potpisivanje (engl. *signature algorithms*) koje prihvaća SOG-IS grupa. EC-GDSA je preporučen, ali nije naveden zbog loše interoperabilnosti.[17]

Tablica 3 SOG-IS prihvaćeni algoritmi za potpisivanje

|  |  |
| --- | --- |
| **Algoritam** | **Reference** |
| RSA-PKCS#1v1\_5 | IETF RFC 3447 |
| RSA-PSS | IETF RFC 3447 |
| DSA (FF-DLOG DSA) | FIPS Publication 186-4, ISO/IEC 14888-3 |
| EC-DSA (EC-DLOG EC-DSA) | FIPS Publication 186-4 |
| EC-SDSA-opt (EC-DLOG EC-Schnorr) | ISO/IEC 14888-3 |

Tablica 4 prikazuje skup kombinacija algoritama za potpisivanje i hash funkcija (engl. *signature suite*) koje prihvaća SOG-IS grupa. Kombinacije zasnovane na eliptičkim krivuljama su odabrane na način da duljina izlaza hash funkcije odgovara veličini ključa odgovarajuće eliptičke krivulje.

Tablica 4 SOG-IS prihvaćene kombinacije algoritama za potpisivanje i hash funkcija

|  |  |  |  |
| --- | --- | --- | --- |
| **Naziv** | **Hash funkcija** | **Algoritam za potpisivanje** | **Vrsta** |
| sha224-with-rsa | SHA-224 | RSA-PKCSv1\_5 | Nasljeđen |
| sha256-with-rsa | SHA-256 | RSA-PKCSv1\_5 | Nasljeđen |
| sha512-with-rsa | SHA-512 | RSA-PKCSv1\_5 | Nasljeđen |
| rsa-pss with mgf1SHA-256Identifier | SHA-256 | RSA-PSS | Preporučen |
| rsa-pss with mgf1SHA-512Identifier | SHA-512 | RSA-PSS | Preporučen |
| rsa-pss with mgf1SHA3-Identifier | SHA3-256, SHA3- 384 ili SHA3-512 | RSA-PSS | Preporučen |
| sha224-with-ecdsa | SHA-224 | EC-DSA | Preporučen |
| sha2-with-ecdsa | SHA-256, SHA-384 ili SHA-512 | EC-DSA | Nasljeđen |
| sha2-with-ecsdsa | SHA-256, SHA-384 ili SHA-512 | EC-SDSA-opt | Preporučen |
| sha3-with-ecdsa | SHA3-256, SHA3- 384 ili SHA3-512 | EC-DSA | Preporučen |
| sha3-with-ecsdsa | SHA3-256, SHA3- 384 ili SHA3-512 | EC-SDSA-opt | Preporučen |

SOG-IS također definira vremensku preporuku funkcija kroz vrijeme za olakšano planiranje i projektiranje. Grupa radi procjene na temelju trenutnih trendova računalne snage potrebne za probijanje algoritma.

Trenutna revizija ne predviđa mehanizme otporne na probijanje kvantnim računalima. Razvijanje sustava čija je svrha zaštita informacija u dugom roku treba uzeti u obzir napredak tehnologije kvantnih računala i implementirati nove mehanizme koji pružaju prikladnu zaštitu.

# DSS

Servis digitalnih potpisa (engl. *Digital signature services*) je otvorena softverska biblioteka za stvaranje i provjeru elektronskih potpisa. DSS podržava stvaranje i provjeru interoperabilnih i sigurnih elektronskih potpisa definiranih eIDAS uredbom.[19]

DSS je Java biblioteka izdana pod LGPL 2.1 licencom koju razvija i aktivno održava Luksemburška tvrtka Nowina Solutions. Biblioteka mogu koristiti fizičke i pravne osobe u svrhu izrade rješenja za digitalno potpisivanje.

Korištenje DSS razvojnog okvira osigurava usklađenost izrađenih potpisa s EU uredbom i olakšava razvoj rješenja bez obzira na ciljanu platformu.

Glavne značajke razvojnog okvira su stvaranje, proširenje i provjera digitalnih potpisa uz brojne podržane koncepte i značajke:

* upravljanje podatcima o opozivu
* izgradanja lanca certifikata
* upravljanje vremenskim žigovima
* REST i SOAP web usluge
* izvješća o provjeri potpisa
* upravljanje povjerenjem

DSS također podržava provjeru valjanosti kvalificiranih i naprednih elektronskih potpisa. Biblioteka implementira algoritam koji određuje odgovor na sljedeća pitanja[20]:

* je li certifikat kvalificiran
* koji je tip certifikata
* je li odgovarajući privatni ključ zaštićen QSCD-om

Odgovor na ova tri pitanja određuje može li potpis biti kvalificiran pod eIDAS uredbom.

DSS projekt se sastoji od više modula koji se mogu referencirati u vlastitom rješenju koristeći Maven. Verzija 5.8 ima sljedeće minimalne zahtjeve za uspješno pokretanje u vlastitom okruženju:

* Java 9 i više
* Maven 3.6 i više

## Apstrakcija podataka

Ulazni podatci, odnosno dokumenti, u DSS razvojnom okviru apstrahirani su tipom DSSDocument bez obzira na njihov tip. DSS predviđa tri implementacije:

* InMemoryDocument – u potpunosti učitava podatak u memoriju na temelju niza bajtova ili ulaznog toka (engl. *input stream*)
* FileDocument – odnosi se na postojeću datoteku u sustavu datoteka
* DigestDocument – sadrži unaprijed izračunatu hash vrijednost podatka; klijent ne mora poslati čitavi podatak, ali je moguće izraditi potpis jedino u Detached načinu rada

Slika 5.1 prikazuje stvaranje PDF dokumenta u memoriji na temelju bajtova ulaznog podatka i imena datoteke.



Slika 5.1 Stvaranje DSS dokumenta u memoriji

Stvoreni objekt predstavlja originalni podatak u DSS razvojnom okviru te se dalje koristi za operacije potpisivanja i validacije.

Razvojni okvir implementira modul DSSUtil koji sadrži pomoćne funkcije često korištene u implementaciji rješenja. Modul definira funkciju toByteArray kojom se objekt tipa DSSDocument na jednostavan način pretvara u niz bajtova koji je moguće koristiti van konteksta DSS-a.

## Potpisivanje

DSS razvojni okvir podržava izradu potpisa za XAdES, CAdES, PAdES, JAdES i ASIC formate u osnovnim profilima. Od verzije 4 nije moguće izraditi potpis jednim od naslijeđenih (engl. *legacy*), standardnih profila, ali je moguće provjeriti valjanost takvih potpisa.[12]

Tablica 5 definira podržane profile u DSS-u te ekvivalenciju osnovnih (engl. *baseline*) profila sa standardnim profilima.

Tablica 5 Podržani profili u DSS-u

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **XAdES** | | **CAdES** | | **PAdES** | | **JAdES** |
| **STANDARD** | **BASELINE** | **STANDARD** | **BASELINE** | **STANDARD** | **BASELINE** | **BASELINE** |
| XAdES-BES | XAdES-B | CAdES-BES | CAdES-B | PAdES-BES | PAdES-B | JAdES-B |
| XAdES-EPES | CAdES-EPES | PAdES-EPES |
| XAdES-T | XAdES-T | CAdES-T | CAdES-T | PAdES-T | PAdES-T | JAdES-T |
| XAdES-XL | XAdES-LT | CAdES-XL | CAdES-LT | PAdES-XL | PAdES-LT | JAdES-LT |
| XAdES-A | XAdES-LTA | CAdES-A | CAdES-LTA | PAdES-LTV | PAdES-LTA | JAdES-LTA |

Potpisivanje dokumenta se provodi kroz tri nedjeljiva koraka:

1. izračunaj sažetak (engl. *digest*) koji će biti potpisan
2. potpiši sažetak
3. potpiši dokument (dodaj potpisani sažetak dokumentu)

DSS okvir u potpunosti upravlja ovim koracima, a klijentski kod upravlja postavkama i ulaznim podatcima operacije.

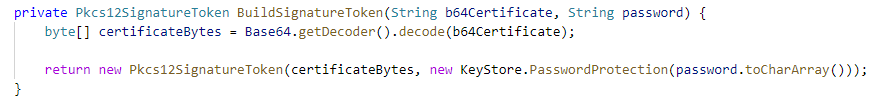
Klijentski kod mora navesti vrstu pohrane ključa (engl. *key store*) koji se koristi za potpisivanje dokumenata. DSS okvir predviđa četiri implementacije:

* Pkcs11SignatureToken – omogućava komunikaciju s pametnim karticama kroz PKCS#11 sučelje
* Pkcs12SignatureToken – omogućava potpisivanje s PKCS#12
* MSCAPISignatureToken – omogućava potpisivanje s MS CAPI (Microsoftovo sučelje za komunikaciju s pametnim karticama)
* JKSSignatureToken – omogućava potpisivanje s Java Key Store datotekama (.jks)

DSS razvojni okvir koristi sučelje SignatureTokenConnection za upravljanje implementacijom procesa potpisivanja kako bi potpisivanje bilo neovisno o sredstvu kojim se potpisuje. Također implementira apstraktnu klasu AsyncSignatureTokenConnection koja omogućava računanje hash vrijednosti i potpisivanja u različitim nitima ili na različitom sklopovlju.

Kroz ovakav dizajn, biblioteka omogućava proširenje funkcionalnosti proizvođačima čitača kartica i razvojnim timovima koji implementiraju vlastita rješenja na temelju ove biblioteke.

Slika 5.1 prikazuje funkciju kojom se stvara PKCS12 objekt na temelju Base64 kodirane PKCS#12 datoteke i lozinke.



Slika 5.2 Stvaranje PKCS12 objekta za potpisivanje

Ovako pripremljen objekt koji sadrži certifikat može se iskoristiti za potpisivanje podataka. Slika 5.2 prikazuje funkciju za potpisivanje PDF dokumenta.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 5.3 Potpisivanje PDF dokumenta

U prvom koraku se kreira PKCS12 objekt za potpisivanje na temelju certifikata. Iz tog objekta se izvede privatni ključ koji će biti korišten za potpisivanje.

Dohvaćaju se parametri koji će biti korišteni za potpisivanje. Parametri uključuju razinu potpisa, hash algoritam, podatke o certifikatu kojim se potpisuje i čitavom lancu certifikata. Dodavanje lanca certifikata pojednostavljuje provjeru valjanosti potpisa.

Metoda getDataToSign dohvaća podatke iz dokumenta koje je potrebno potpisati na temelju proslijeđenih parametara. Ti podaci odgovaraju SignedInfo XMLDSig elementu u slučaju XAdES-a i rasponu bajtova zadanom u rječniku potpisa u slučaju PAdES-a.

Dohvaćeni podaci za potpisivanje koriste se kao ulaz metodi sign objekta spremišta ključeva PKCS12SignatureToken. Prvi parametar je niz bajtova koje treba potpisati, drugi parametar je hash algoritam, a treći je privatni ključ kojim se obavlja potpisivanje.

Potrebno je eksplicitno navesti privatni ključ jer jedno spremište ključeva (engl. *KeyStore*) može sadržavati više certifikata odnosno privatnih ključeva.

U posljednjem koraku se potpis integrira s dokumentom koji se potpisuje ovisno o načinu rada algoritma. PAdES podržava samo Enveloped način rada, dok je za XAdES i CAdES moguće postaviti više različitih načina rada prilikom postavljanja parametara.

Pozivom metodi signDocument obavlja se ova integracija. Uz originalni podatak i vrijednost potpisa, prosljeđuju joj se i parametri koji određuju način ugradnje potpisa u podatak. Metoda vraća objekt tipa DSSDocument koji je moguće dalje u implementaciji logike sustava.

Razdvajanje procesa potpisivanja u tri koraka omogućava razdvajanje odgovornosti prilikom implementacije sustava. Preporučena praksa je razdvojiti operacije potpisivanja i ostatak logike sustava u zasebne jedinice sustava.

Slika 5.4 prikazuje primjer jednostavnog XAdES potpisa B razine osnovnog profila.



Slika 5.4 Primjer XAdES-Baseline-B potpisa

Princip potpisivanja podataka svim podržanim standardima i profilima u DSS razvojnom okviru implementiran je kroz iste korake i isto klijentsko sučelje koji su opisani u ovom poglavlju.

## Provjera valjanosti potpisa

Proces provjere valjanosti potpisa temelji se na ETSI standardima pri čemu rezultat provjere mora biti TOTAL-FAILED, TOTAL-PASSED, ili INDETERMINATE.

TOTAL-PASSED rezultat označava da je potpis u potpunosti prošao provjeru valjanosti i da je sukladan definiranoj politici provjere potpisa.

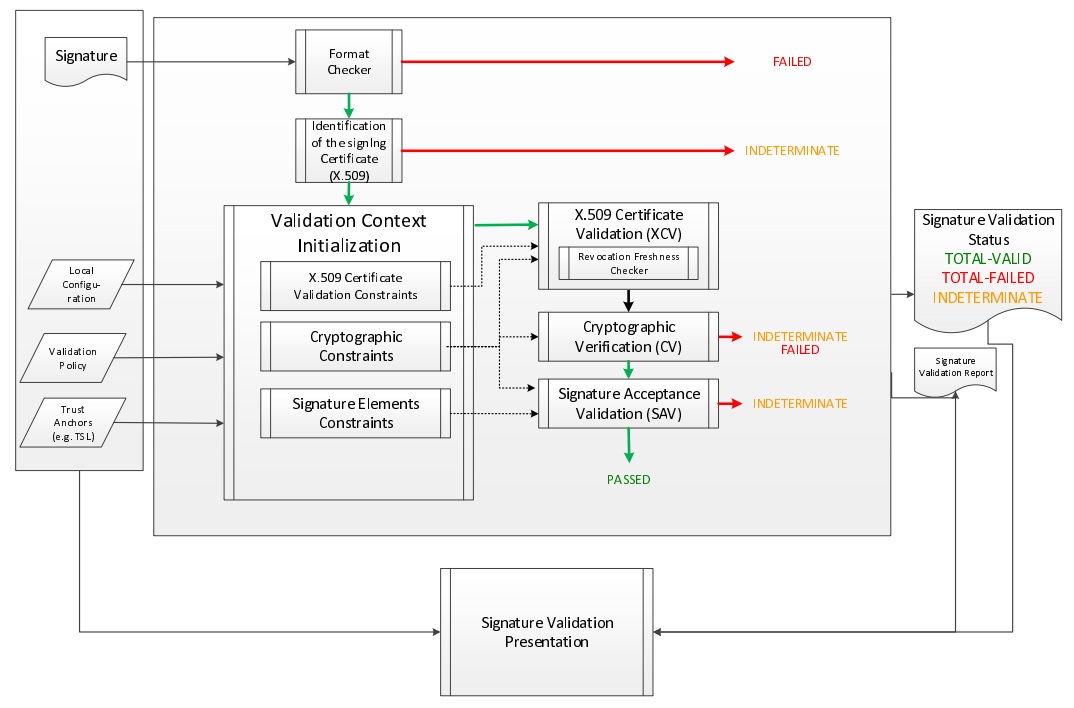
TOTAL-FAILED rezultat označava da je format potpisa neispravan ili da sama vrijednost potpisa nije valjana.

INDETERMINATE rezultat označava da format i vrijednost potpisa nisu neispravni, ali nema dovoljno informacija na temelju koji se može provjeriti ispravnost potpisa.

Za svaku stavku koja se provjerava razvojni okvir daje informacije na temelju kojih je određeni status dodijeljen.

Provjera valjanosti potpisa u razvojnom okviru temeljena je na ETSI EN 319 102-1 standardu pri čemu je politika valjanosti glavni pokretač procesa. Proces validacije provjerava postojanje određenih podataka i njihovu valjanost te provjerava vremenske ovisnosti među tim podatcima.

Slika 5.5 predstavlja pojednostavljeni dijagram procesa provjere valjanosti potpisa. Veze i elementi dijagrama definiraju logički skup provjera korištenih u procesu.



Slika 5.5 Pojednostavljeni process provjere valjanosti potpisa u DSS-u (izvor: https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#\_validation\_process, preuzeto 22.8.2021.)

Rezultat ovog procesa su četiri izvješća različitih razina detalja:

* jednostavni izvještaj
* detaljni izvještaj
* dijagnostički izvještaj
* ETSI validacijski izvještaj

Provjera valjanosti potpisa u razvojnom okviru izvršava se kroz iste korake i klijentska sučelja bez obzira na vrstu potpisa.

Slika 5.6 prikazuje funkciju za provjeru valjanosti potpisa proizvoljne binarne datoteke s odvojenim (engl. *detached*) potpisom.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 5.6 Provjera valjanosti potpisa binarne datoteke

U prvom koraku se stvara SignedDocumentValidator objekt koji upravlja provjerom pozivom statičkoj funkciji fromDocument.

Objekt validator koristi certificateVerifier objekt za provjeru statusa korištenih certifikata. Klasa CertificateVerifier definira izvore povjerenja koji se koriste tijekom validacije. Slika 5.7 prikazuje postupak stvaranja objekta tipa CertificateVerifier.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 5.7 Stvaranje CertificateVerifier objekta

Pozivom metode validateDocument obavlja se provjera valjanosti na temelju argumenta validacijske politike. Metoda vraća objekt tipa Reports koji sadrži različite poglede na rezultat provjere valjanosti.

Slika 5.8 prikazuje primjer jednostavnog izvještaja provjere valjanosti.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 5.8 Primjer jednostavnog izvještaja

### Politika valjanosti

DSS razvojni okvir omogućava definiranje politike valjanosti potpisa kroz kod i kroz konfiguracijsku XML datoteku. Proces provjere valjanosti potpisa se tada temelji na postavkama navedenima kroz politiku.

Svako ograničenje ima dodijeljenu FAIL, WARN ili INFORM razinu koja definira ponašanje procesa provjere u slučaju da potpis krši zadano ograničenje.

Neka od ograničenja koja je moguće definirati politikom su ponašanje vezano uz certifikate, vremenske žigove, korištene algoritme i parametre algoritama, itd.

## Upravljanje povjerenjem

DSS razvojni okvir omogućava upravljanje povjerenjem kroz tzv. sidra povjerenja (engl. *trust anchor*). Kroz njih se definira povjerenje prema entitetima odnosno potpisima koje ti entiteti generiraju.

Od verzije 5.6. razvojnog okvira omogućeno je postavljanje jednog ili više izvora pouzdanih certifikata. Izvori se mogu postaviti iz spremišta povjerenja (engl. *trust store*), pouzdane liste (engl. *trusted list*), i liste pouzdanih listi (engl. *list of trusted lists*).

U slučaju izrade vlastite PKI, moguće je dodati CA certifikat u popis pouzdanih certifikata. Na taj način moguće je stvoriti naprednih elektronski potpis koji je valjan u okviru ETSI standarda uz povjerenje prema privatnom CA.

Slika 5.9 prikazuje funkciju kojom se dodaje izvor pouzdanih certifikata za privatni CA certifikat i certifikat usluge pružanja vremenskog žiga.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 5.9 Dodavanje privatnog CA u pouzdane izvore

## Izvori informacija o opozivu

Svaki certifikat treba biti provjeren koristeći CRL ili OCSP prilikom provjere valjanosti potpisa. Informacija o opozivu može doći iz više različitih izvora. DSS razvojni okvir implementira CRLSource i OCSPSource sučelja koja pružaju generički način pristupanju CRL i OCSP izvorima.

U praksi je moguće implementirati predmemoriju (engl. *cache*) kako bi se ovaj postupak dodatno ubrzao.

Razvojni okvir prvo pokušava dohvatiti odgovor od OCSP poslužitelja, a ako to nije moguće šalje upit CRL poslužitelju.

Izvori ovih informacija mogu biti mrežni ili mogu biti lokalno dostupni. Razvojni okvir pruža implementaciju za svaki od ovih scenarija. Za mrežne izvore upit se šalje poslužiteljima koji su navedeni u certifikatu:

* CRL – naveden u polju CRL distribucijska mjesta (engl. *CRL distribution points)*
* OCSP - naveden u polju pristupa informacijama nadležnog tijela (engl. *Authority Information Access)* AIA

Slika 5.10 prikazuje dvije funkcije za stvaranje CRL i OCSP izvora informacija u sklopu DSS razvojnog okvira koje se mogu pridružiti CertificateVerifier objektu.

Slika na kojoj se prikazuje tekst

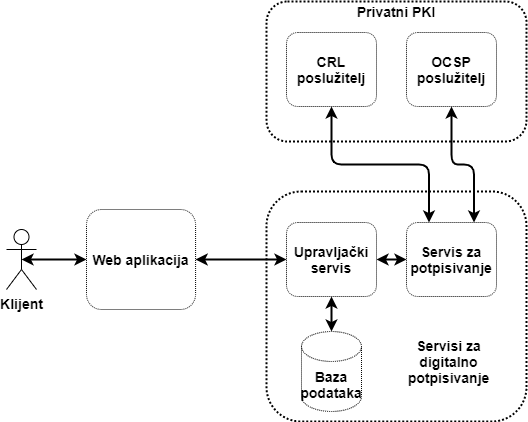
Opis je automatski generiran

Slika 5.10 Stvaranje objekata za dohvaćanje informacija o opozivu

Razvojni okvir daje točke proširenja za RevocationSource<T> objekte, a zadane postavke omogućavaju dohvaćanje rezultata od svih standardnih CRL i OCSP poslužitelja.

# Arhitektura sustava

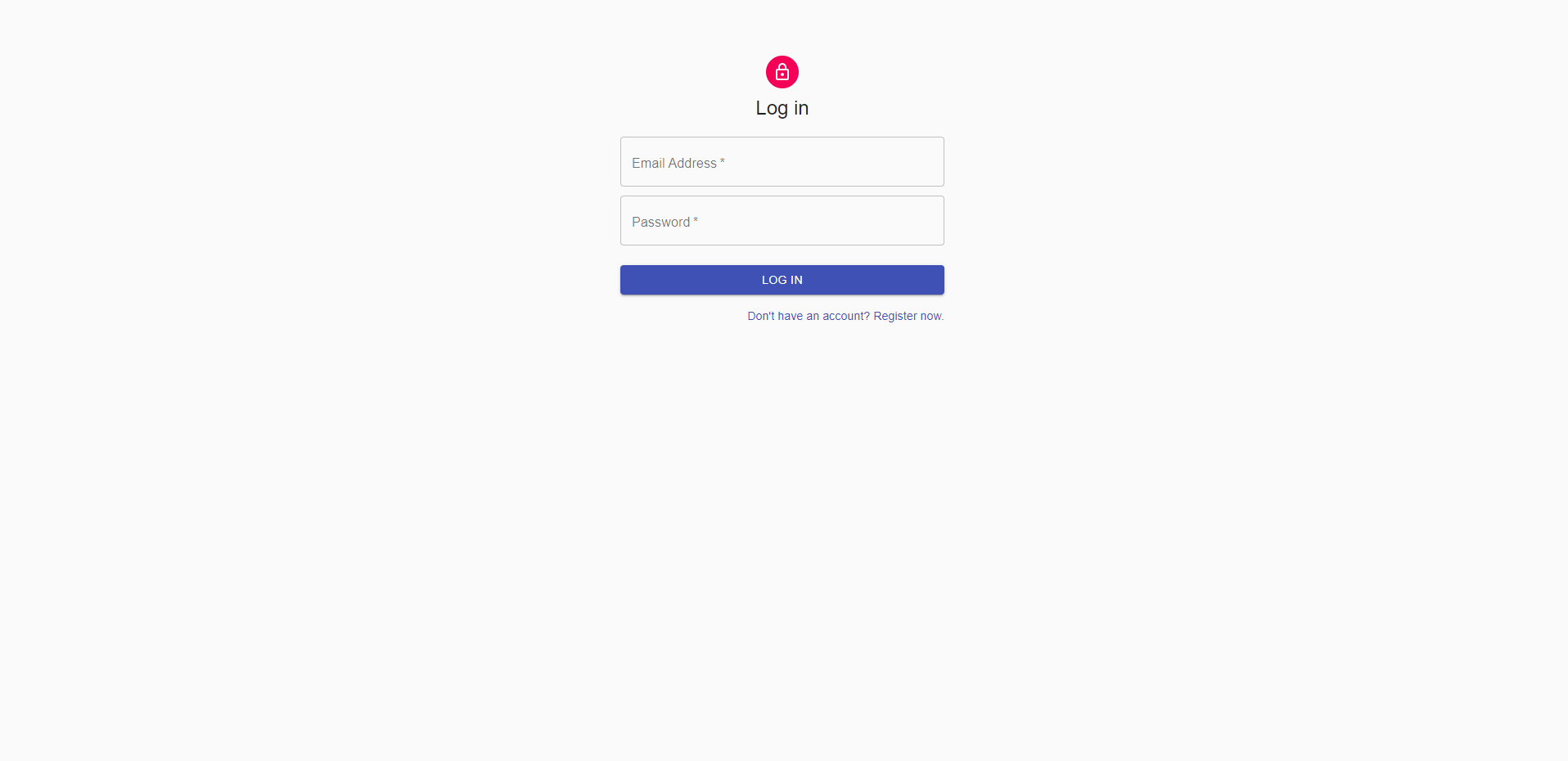
Implementirani sustav za digitalno potpisivanje sastoji se od klijentske web aplikacije, skupa servisa zajedno s bazom podataka i potporne PKI. Slika 6.1 prikazuje arhitekturu implementiranog sustava.



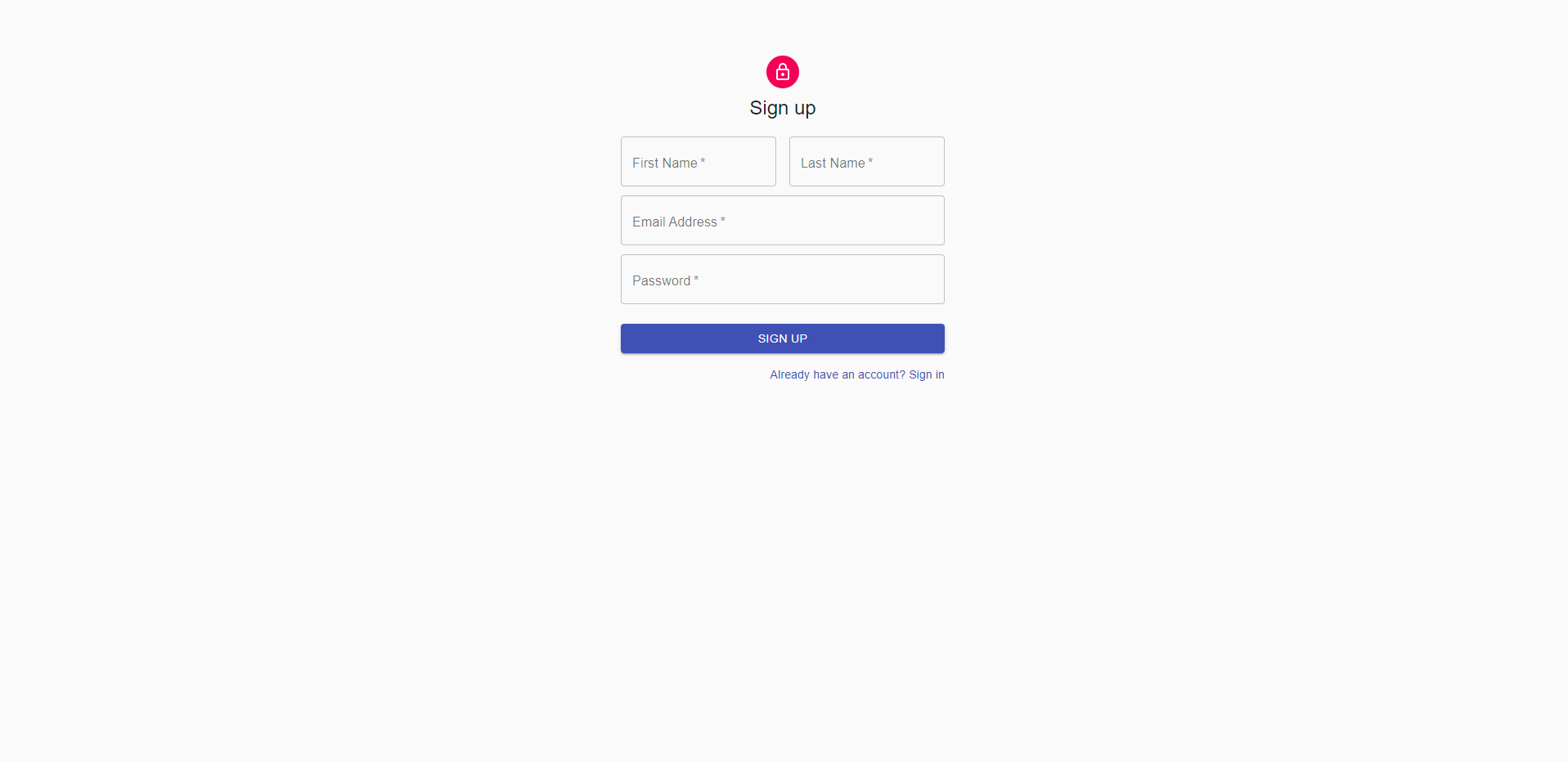
Slika 6.1 Arhitektura sustava

## Web aplikacija

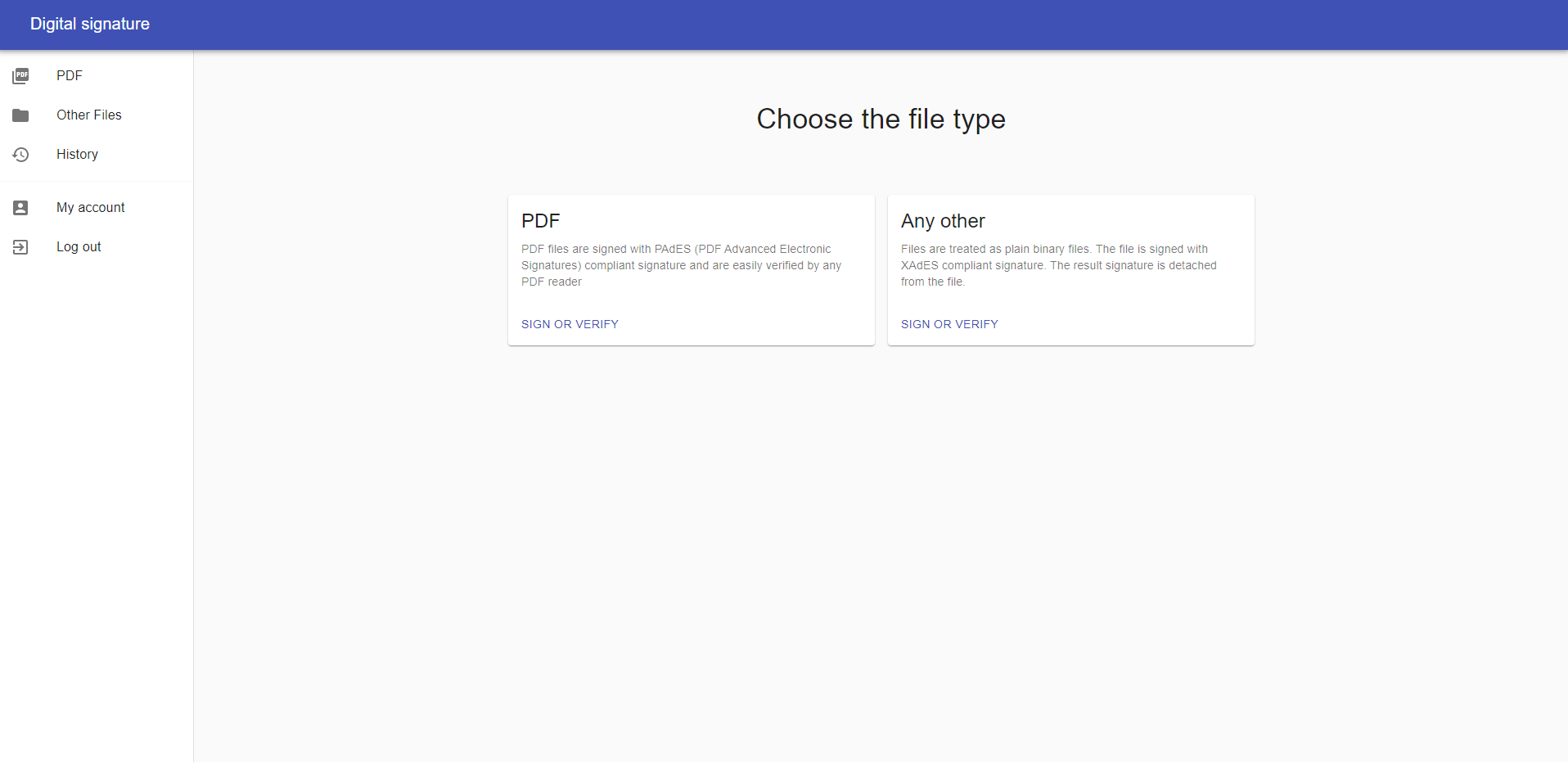
Web aplikacija je sučelje sustava za digitalno potpisivanje. Sva interakcija korisnika odvija se putem web aplikacije. U nastavku je dan pregled sučelja web aplikacije.



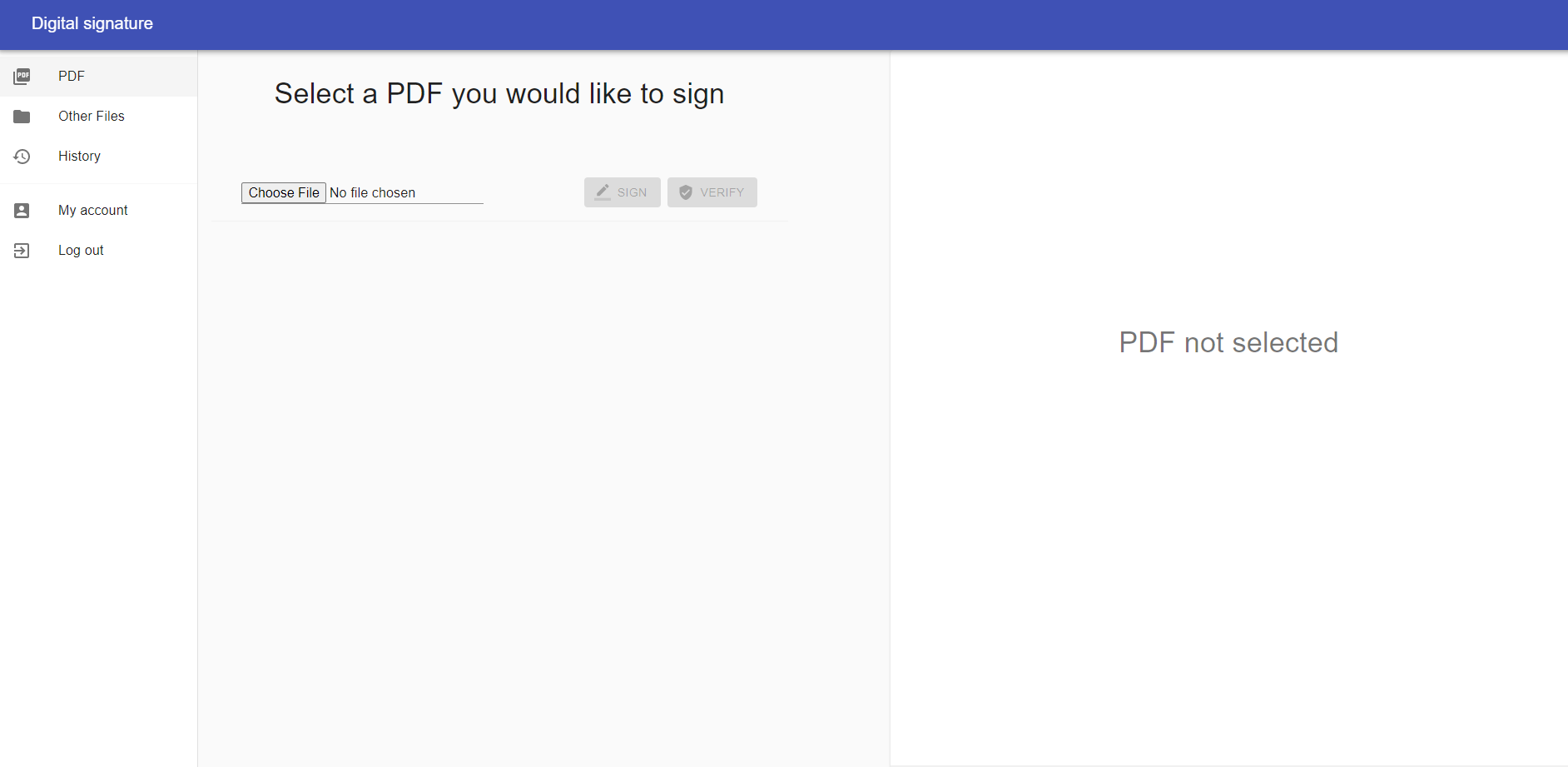
Slika 6.2 Prijava u sustav



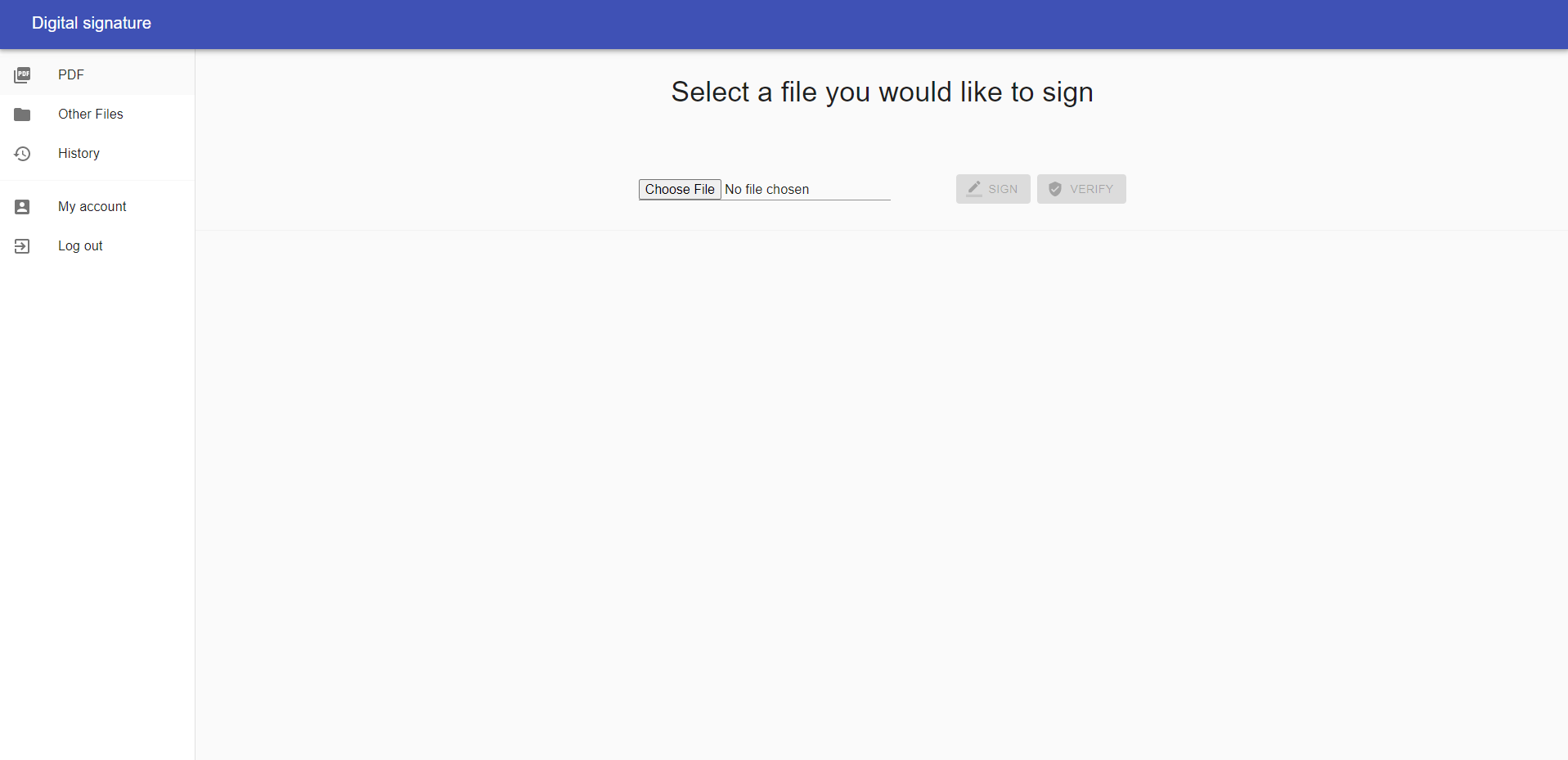
Slika 6.3 Registracija



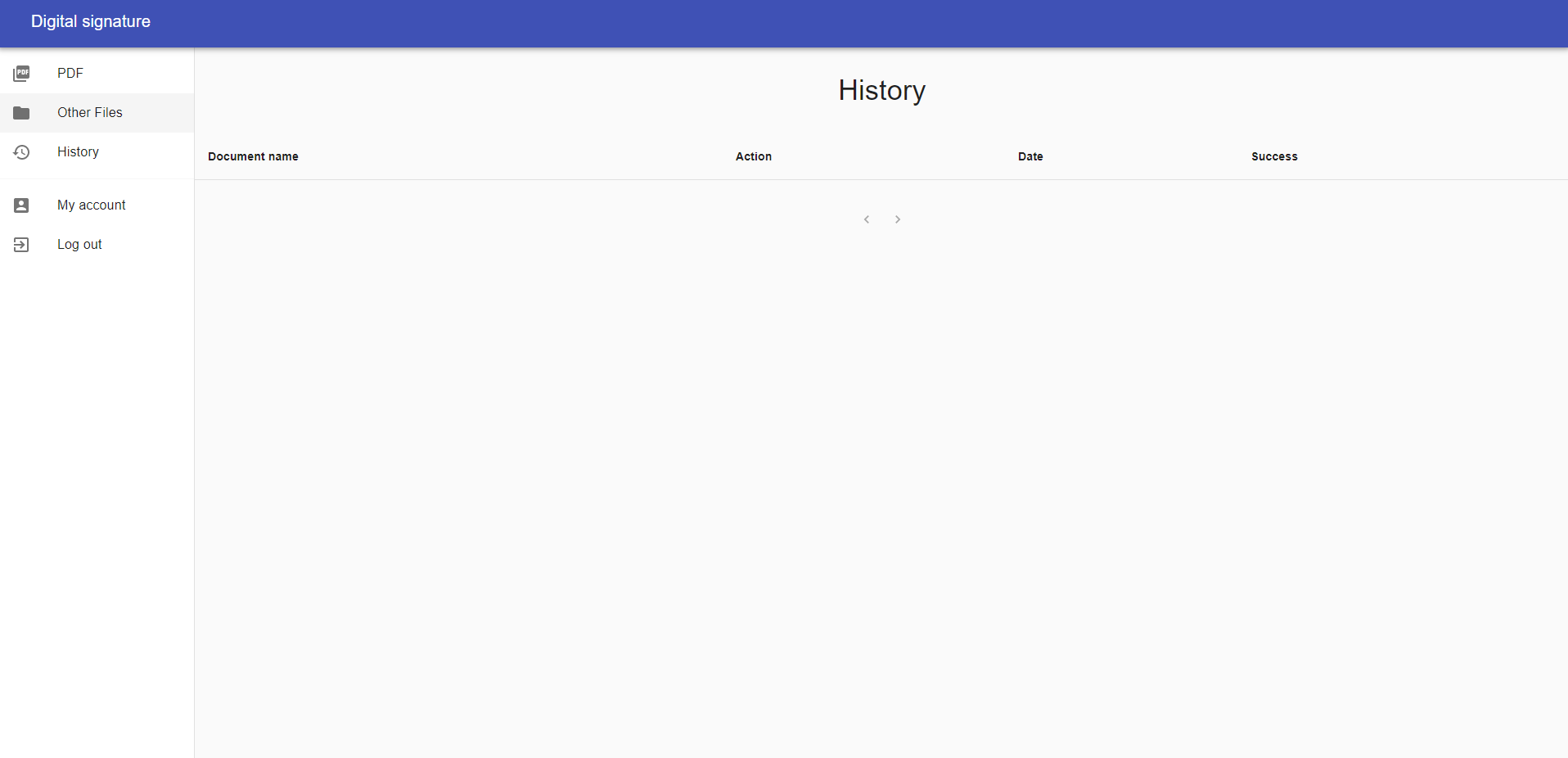
Slika 6.4 Naslovna stranica



Slika 6.5 Potpisivanje i verifikacija PDF dokumenata



Slika 6.6 Potpisivanje i verifikacija binarnih datoteka



Slika 6.7 Povijest

Slika na kojoj se prikazuje tekst

Opis je automatski generiran

Slika 6.8 Upravljanje osobnim podatcima

## Servis za potpisivanje

Servis za potpisivanje koristi DSS razvojni okvir za implementaciju izrade i provjere valjanosti digitalnih potpisa. Ovaj servis ne sadrži podatke o korisnicima te njihovim podatcima i certifikatima. Ovaj servis implementira PAdES i XAdES vrste potpisivanja s bilo kojom od četiri razine potpisa.

Servis nije izložen na javnoj mreži te mu nije moguće direktno pristupiti. Komunikaciju s ovim servisom izvršava servis za upravljanje digitalnim potpisima u privatnoj mreži.

## Servis za upravljanje digitalnim potpisima

Servis za upravljanje digitalnim potpisima implementira REST API koji omogućuje izvršavanje željenih operacija na sustav. Web aplikacija koristi ovaj servis za izvršavanje svih radnji. Ovaj servis je izložen na javnoj mreži pa je moguća direktna konzumacija njegovih funkcionalnosti kroz bilo koji REST klijent.

Ovaj servis upravlja popratnim informacijama i funkcionalnostima poput upravljanje korisnicima i njihovim ulogama, upravljanje povijesti operacija, itd. Pored toga, ovaj servis pruža jednostavan pogled na uslugu digitalnog potpisivanja te omogućava korištenje ove usluge bez poznavanja detalja o digitalnim potpisima.

## CRL poslužitelj

CRL poslužitelj je dio PKI koji je odgovoran za posluživanje liste opoziva. Implementirani sustav daje primjer privatnog PKI. U slučaju da se koristi certifikat koji nije izdao testni CA, ovaj CRL poslužitelj neće biti korišten, već će biti korišten onaj poslužitelj koji je naveden u samom certifikatu.

Teoretski bi ovaj poslužitelj mogao služiti kao posrednik (engl. *proxy*) preko kojeg se dohvaćaju sve ostale liste opoziva, ali to je van opsega implementacije ovog sustava.

## OCSP poslužitelj

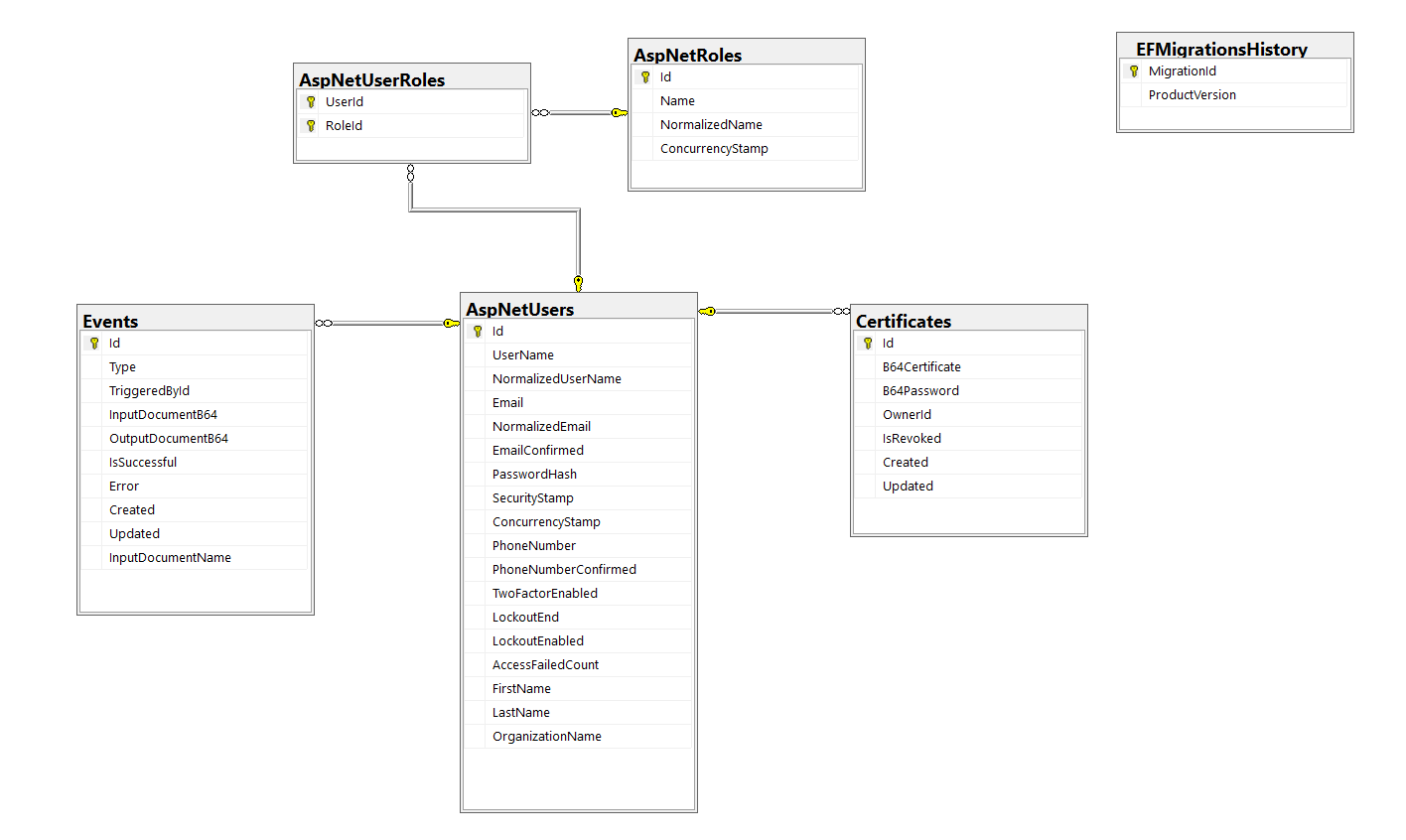
OCSP poslužitelj je dio PKI koji je odgovoran za davanje odgovora na upit o valjanosti certifikata. Slično kao CRL poslužitelj, biti će pozvan samo kada se radi provjera valjanosti certifikata kojeg je izdao testni CA.

Moguće je pohraniti OCSP odgovore u privremenu memoriju u kratkom roku, ali to je van opsega implementacije ovog sustava.

## Baza podataka

Baza podataka služi za pohranu svih potrebnih podataka usluge za digitalno potpisivanje. Sustav koristi SQL Server relacijsku bazu podataka, ali uz minimalne modifikacije moguće je koristiti i druge relacijske baze podataka uz pomoć apstrakcijskog sloja na aplikacijskoj razini.

Slika 6.2 prikazuje relacijski model baze podataka generiran Microsoft SQL Server Management Studio alatom.



Slika 6.9 Relacijski model baze podataka

Baza podataka, između ostalog, pohranjuje i korisničke certifikate u enkriptiranom obliku. Poboljšanje u sigurnosnom smislu bi bilo korištenje HSM-a za pohranu certifikata.

Na tržištu postoji široka ponuda fizičkih i HSM-ova u oblaku. EU definira popis HSM-ova koji upadaju u kategoriju QSCD pa je uz pomoć njih moguće izraditi QES i time dodatno podići razinu sigurnosti sustava i pruženih usluga.

# 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

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

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

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

[12] CEF digital: „Digital Signature Service Documentation v5.8, 7.2.2021.“, s Interneta, <https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html>, 20.8.2021.

[13] W3C: „XML Advanced Electronic Signatures, 20.2.2003“, s Interneta, https://www.w3.org/TR/XAdES/ , 20.8.2021.

[14] ISO 32000-1:2008: „Document management – Portable document format – Part 1: PDF 1.7“, srpanj 2008.

[15] ETSI TS 102 778-1: „Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview – a framework document for PAdES“, V.1.1.1, srpanj 2009.

[16] Housley, R et al: „RFC5642 Cryptographic Message Syntax (CMS)“, rujan 2009.

[17] ETSI TS 119 312: „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites“, V1.2.1, svibanj 2017.

[18] SOG-IS Crypto Working Group: „SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms“, Version 1.2, siječanj 2020.

[19] CEF Digital: „Digital Signature Service – DSS“, s Interneta, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Signature+Service+-++DSS>, 21.8.2021.

[20] Barette, O.: „Qualified electronic siagnature (QES) validation algorithm“, V1.03, 9.9.2019.

# 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

AdES – Advanced Electronic Signature

ETSI – European Telecommunications Standards Institute

XAdES – XML AdES

PAdES – PDF AdES

CAdES – CMS AdES

CMS – Cryptographic Message Syntax

DER – Distinguished Encoding Rules

BER – Basic Encoding Rules

ASN.1 – Abstract Syntax Notation One

DSS – Digital Signature Services

HSM – Hardware Security Module

# 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](#_Toc80719576)

[Slika 2.2 Digitalni certifikat web stranice FESB-a 6](#_Toc80719577)

[Slika 2.3 Lanac certifikata 7](#_Toc80719578)

[Slika 3.1 Vremenska traka razvoja eIDAS uredbe (izvor: https://www.eid.as/, preuzeto 17.8.2021.) 9](#_Toc80719579)

[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](#_Toc80719580)

[Slika 4.1 XAdES dijagram 15](#_Toc80719581)

[Slika 4.2 XAdES-Baseline-B XML struktura 16](#_Toc80719582)

[Slika 4.3 ISO32000-1 PDF potpis 19](#_Toc80719583)

[Slika 4.4 Rječnik potpisa 20](#_Toc80719584)

[Slika 4.5 Identifikator vrste sadržaja 22](#_Toc80719585)

[Slika 4.6 Definicija ContentInfo tipa 22](#_Toc80719586)

[Slika 4.7 Osnovni CMS tip-vrijednost format 23](#_Toc80719587)

[Slika 4.8 CMS Signed-Data tip formata 23](#_Toc80719588)

[Slika 5.1 Stvaranje DSS dokumenta u memoriji 28](#_Toc80719589)

[Slika 5.2 Stvaranje PKCS12 objekta za potpisivanje 30](#_Toc80719590)

[Slika 5.3 Potpisivanje PDF dokumenta 30](#_Toc80719591)

[Slika 5.4 Primjer XAdES-Baseline-B potpisa 32](#_Toc80719592)

[Slika 5.5 Pojednostavljeni process provjere valjanosti potpisa u DSS-u (izvor: https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#\_validation\_process, preuzeto 22.8.2021.) 34](#_Toc80719593)

[Slika 5.6 Provjera valjanosti potpisa binarne datoteke 35](#_Toc80719594)

[Slika 5.7 Stvaranje CertificateVerifier objekta 35](#_Toc80719595)

[Slika 5.8 Primjer jednostavnog izvještaja 36](#_Toc80719596)

[Slika 5.9 Dodavanje privatnog CA u pouzdane izvore 38](#_Toc80719597)

[Slika 5.10 Stvaranje objekata za dohvaćanje informacija o opozivu 39](#_Toc80719598)

[Slika 6.1 Arhitektura sustava 40](#_Toc80719599)

[Slika 6.2 Prijava u sustav 41](#_Toc80719600)

[Slika 6.3 Registracija 41](#_Toc80719601)

[Slika 6.4 Naslovna stranica 42](#_Toc80719602)

[Slika 6.5 Potpisivanje i verifikacija PDF dokumenata 42](#_Toc80719603)

[Slika 6.6 Potpisivanje i verifikacija binarnih datoteka 43](#_Toc80719604)

[Slika 6.7 Povijest 43](#_Toc80719605)

[Slika 6.8 Upravljanje osobnim podatcima 44](#_Toc80719606)

[Slika 6.9 Relacijski model baze podataka 46](#_Toc80719607)