Digitalne vjerodajnice u skladu s europskim digitalnim identitetom

Galić, Bruno

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1516

DIGITALNE VJERODAJNICE U SKLADU S EUROPSKIM DIGITALNIM IDENTITETOM

Bruno Galić

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1516

DIGITALNE VJERODAJNICE U SKLADU S EUROPSKIM DIGITALNIM IDENTITETOM

Bruno Galić

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 4. ožujka 2024.

ZAVRŠNI ZADATAK br. 1516

Pristupnik:	**Bruno Galić (0036537414)**
Studij:	Elektrotehnika i informacijska tehnologija i Računarstvo
Modul:	Računarstvo
Mentor:	izv. prof. dr. sc. Ante Đerek

Zadatak: **Digitalne vjerodajnice u skladu s europskim digitalnim identitetom**

Opis zadatka:

U svrhu jačanja interoperabilnosti digitalnog identiteta između zemalja članica EU, Europska komisija je usvojila preporuku kojom poziva zemlje članice da rade na razvoju specifikacija, arhitekture, praksi, smjernica i alata vezanih uz europski digitalni identitet (EUDI). U sklopu završnog rada potrebno je istražiti EUDI arhitekturu i referentni okvir, te javno dostupne arhitekture i standarde pojedinih zemalja članica uključujući Njemačku i Italiju. Na temelju istraživanja, potrebno je i izgraditi jednostavan prototip sustava za izdavanje ili prezentaciju digitalnih vjerodajnica. Radu je potrebno priložiti izvorni kôd razvijenih i korištenih programa, citirati korištenu literaturu i navesti dobivenu pomoć.

Rok za predaju rada: 14. lipnja 2024.

Želim se zahvaliti svom mentoru izv. prof. dr. sc. Anti Đereku na susretljivosti i svoj pomoći koju mi je pružao tijekom završnog rada.

Sadržaj

1. Uvod

Prema informacijama sa službene stranice Europske Unije [1], inicijativa za razvoj Europskog digitalnog identiteta pokrenuta je s ciljem da bude dostupna svim građanima i poslovnim subjektima koji žele potvrditi svoj identitet ili pružiti određene osobne informacije. Ovaj sustav omogućuje korištenje osobnog digitalnog novčanika za *online* i *offline* pristup javnim i privatnim uslugama diljem EU.

Ključne prednosti EU digitalnog identiteta, uključuju [1]:

- Pravo svake osobe s osobnom iskaznicom na digitalni identitet priznat u cijeloj EU.
- Jednostavan i siguran način kontrole dijeljenja osobnih informacija s uslugama koje ih zahtijevaju.
- Operativnost putem digitalnih novčanika dostupnih na mobilnim aplikacijama i drugim uređajima.

Kako je navedeno na stranici Europske Unije [1], EU digitalni identitet je potreban zbog postojećih nedostataka u sustavima digitalne identifikacije koje nude vlade država članica. Ovi sustavi često nisu dostupni cijelom stanovništvu, ograničeni su i ne omogućuju prekogranični pristup. Korištenje EU digitalnog identiteta omogućit će građanima dokazivanje identiteta, dijeljenje digitalnih dokumenata te potvrdu specifičnih osobnih informacija diljem EU, uz punu kontrolu nad dijeljenjem podataka. Korištenje će obuhvaćati razne slučajeve poput pristupa javnim uslugama, otvaranja bankovnih računa, prijave na sveučilišta, pohrane medicinskih recepata te iznajmljivanja automobila pomoću digitalne vozačke dozvole.

U svibnju 2023. godine pokrenuta su četiri velika pilot-projekta s ciljem testiranja EU digitalnog novčanika [2]. Jedan od projekata je NOBID, konzorcij koji okuplja nordijske

i baltičke zemlje, zajedno s Italijom i Njemačkom, kako bi proveli opsežna testiranja primjene EU digitalnog identiteta za autorizaciju plaćanja proizvoda i usluga [2].

Prva tri poglavlja rada pružaju pregled razvoja Europskog digitalnog identiteta, ističući važnost standardiziranih protokola za provjeru i izdavanje digitalnih vjerodajnica kao što su OID4VCI i OID4VP. Naglašena je potreba za sigurnim i interoperabilnim sustavima koji omogućuju pouzdanu identifikaciju i autentifikaciju korisnika putem digitalnih kanala.

Ključni dio rada obuhvaća detaljan implementacije prototipa sustava za izdavanje digitalnih osobnih iskaznica. Implementacija je realizirana koristeći tehnologije poput Node.js za postavljanje serverskog okruženja i web aplikacije, TLS protokola za rad s certifikatima osobnih iskaznica, te REST API-ja za integraciju s Walt ID sustavom za izdavanje vjerodajnica. Opisan je proces prikupljanja podataka s fizičke osobne iskaznice putem čitača pametnih kartica te njihovo pretvaranje u digitalnu vjerodajnicu koje se može izdati, pohraniti i prezentirati putem QR koda.

Dodatno, rad istražuje Walt ID platformu kao ključnu komponentu za upravljanje digitalnim novčanicima i verifikaciju vjerodajnica, te opisuje integraciju s SD-JWT standardom za selektivno otkrivanje osobnih podataka.

Svrha rada je pružiti cjelovit pregled implementacije sustava za izdavanje digitalnih osobnih iskaznica temeljenih na modernim tehnologijama. Kroz praktični primjer izdavanja vjerodajnice i njezine verifikacije, demonstrirana je funkcionalnost sustava.

Struktura rada sadrži pet poglavlja. Poglavlje *Europski digitalni identitet* 2. opisuje arhitekturu, primjene i zahtjeve sustava. Poglavlje *OpenID* 3. razmatra jednu od ključnih tehnologija za sigurnost digitalnih novčanika. Poglavlje *Implementacija prototipa za izdavanje digitalne osobne iskaznice* 4. pruža opis implementacije i prikaz procesa izdavanja osobne iskaznice.

2. Europski digitalni identitet

2.1. Europski digitalni novčanik

Ovo poglavlje se temelji na informacijama iz izvora [3], naslovljenog *"Everything you need to know about the EUDI Wallet"*.

Europski digitalni identitet (EUDI) predstavlja inicijativu Europske unije koja pokušava unaprijediti način na koji građani i tvrtke unutar EU verificiraju svoj identitet. Ključni dio ove inicijative je EUDI novčanik, koji je dio nove eIDAS 2.0 regulative, i omogućit će sigurno i jednostavno pohranjivanje i dijeljenje digitalnih vjerodajnica.

EUDI novčanik je besplatna mobilna aplikacija koja će omogućiti korisnicima da pohrane i dijele digitalne vjerodajnice, kao što su osobne iskaznice, putovnice, diplome, zdravstveni zapisi i drugi dokumenti. Kroz ovu aplikaciju korisnici će imati kontrolu nad svojim podacima, tako što će odlučivati koje informacije žele podijeliti.

EUDI novčanik neće zamijeniti postojeće fizičke dokumente, već će pružiti novi, praktičniji način za digitalno pohranjivanje i prenošenje tih dokumenata.

Prema izvoru [3], organizacije unutar EU će morati prihvatiti EUDI novčanike kao novi način autentifikacije. To uključuje pružatelje usluga u sektorima poput transporta, energetike, bankarstva, financija, zdravstva, telekomunikacija i obrazovanja. Iako korištenje EUDI novčanika neće biti obavezno, cilj je da preko 80% Europljana koristi digitalne novčanike do 2030. godine.

EUDI novčanik donosi mnoge prednosti za organizacije i korisnike. Organizacijama povećava sigurnost, poboljšava korisničko iskustvo, smanjuje troškove i administrativno opterećenje, te smanjuje vjerojatnost prijevare koristeći naprednu kriptografiju. Za korisnike, EUDI novčanik olakšava verifikaciju identiteta, omogućava prekograničnu in-

teroperabilnost, pruža veću privatnost i kontrolu nad osobnim podacima, te osigurava visoku razinu sigurnosti zahvaljujući snažnoj enkripciji.

2.2. Referentni okvir arhitekture digitalnog identiteta

U svibnju 2024. godine, Europska unija objavila je verziju 1.3.0 dokumenta o Arhitekturi i referentnom okviru EUDI digitalnog novčanika [4]. Ovo poglavlje daje sažet pregled osnovne arhitekture sustava, kako je opisano u četvrtom poglavlju tog dokumenta.

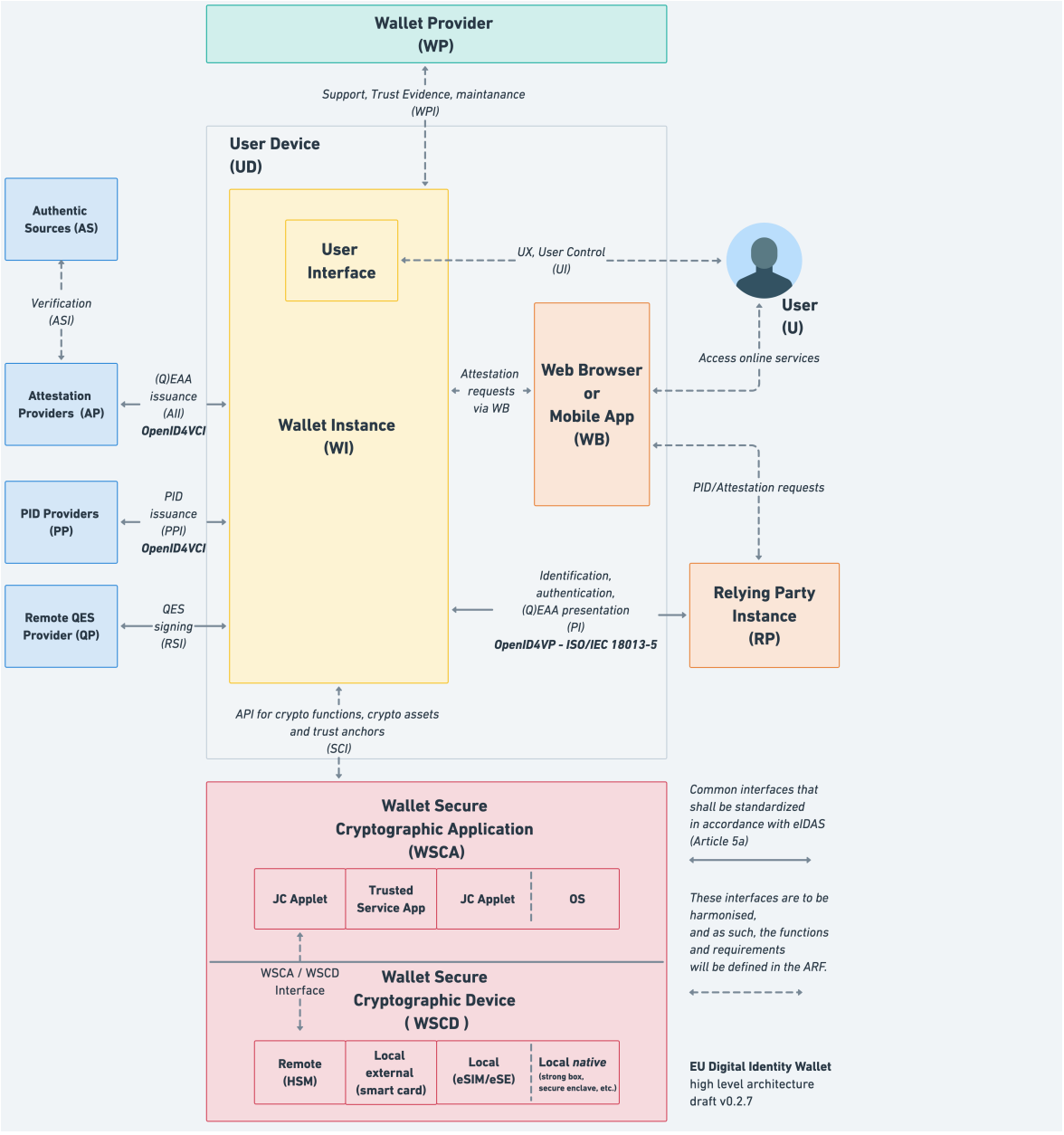
Korisnik se nalazi u središtu EUDI digitalnog novčanika, kao temeljno načelo dizajna. Novčanik treba biti intuitivan i jednostavan za korištenje, s integracijom s postojećim obrascima uporabe. Korisnici trebaju imati jasan nadzor nad svojim podacima i privatnošću, s transparentnim informacijama o tome koji se podaci dijele i s kim. Također, novčanik treba biti pristupačan i uključiv, prilagođen korisnicima različitih tehničkih razina i sposobnosti.

EUDI novčanik prioritizira interoperabilnost. To osigurava da novčanik jednako funkcionira u svim članicama Europske unije.

Zaštita i privatnost korisničkih podataka je temelj arhitekture novčanika. Načelo minimizacije podataka kontrolira prikupljanje osobnih podataka, osiguravajući da se prikuplja samo ono što je nužno.

Arhitektura EUDI novčanika koristi načelo definiranja sigurnih početnih postavki. To znači da su sigurnosna razmatranja ugrađena u dizajn novčanika. Tijekom cijelog procesa, potencijalne ranjivosti se identificiraju i ublažavaju. Primjenjuju se sigurne prakse programiranja, a sama arhitektura minimizira površine napada razdvajanjem osjetljivih podataka i kontrolom pristupa.

Sljedeća slika prikazuje ključne komponente i sučelja unutar arhitekture EUDI novčanika. U nastavku se nalaze opisi elemenata sa slike.



Slika 2.1. Prikaz EUDI arhitekture [4]

- Korisnički uređaj (UD) sadrži instancu novčanika, to je na primjer mobilni uređaj.
- Instanca novčanika (WI) je aplikacija novčanika instalirana na korisničkom uređaju.
- Sigurni kriptografski uređaj (WSCD) je pouzdani hardver koji pruža sigurno okruženje za pohranu kriptografskih sredstava i izvođenje kritičnih funkcija, može ga koristiti više instanci novčanika.

- Sigurna kriptografska aplikacija (WSCA) je sigurna aplikacija koja koristi sigurni kriptografski uređaj za upravljanje sredstvima poput ključeva za određenu instancu novčanika. Komunikaciju s instancom novčanika omogućuje sigurno kriptografsko sučelje (SCI).
- Backend pružatelja novčanika (WP) je aplikacija za podršku, održavanje i izdavanje ovjera putem sučelja pružatelja novčanika (WPI).
- Sučelje pružatelja novčanika (WPI) predstavlja komunikaciju između instance novčanika i pružatelja novčanika.
- Korisničko sučelje (UI) je interakcija između korisnika i instance novčanika.
- Prezentacijsko sučelje (PI) omogućuje prezentaciju i provjeru valjanosti dokumenata u novčaniku.
- Sučelje za izdavanje PID-a (PPI) je sučelje koje omogućuje izdavanje osobnih dokumenata u instancu novčanika. Napravljeno je na temelju OpenID4VCI protokola opisanog u kasnijem poglavlju.
- Sučelje za izdavanje vjerodajnica (AII) je također bazirano na OpenID4VCI protokolu i omogućuje korisniku da preko instance novčanika zatraži novi dokument.
- Sučelje za udaljeno potpisivanje (RSI) služi za udaljeno elektroničko potpisivanje.

2.3. Vjerodajnice

Nastavak opisuje osnove EUDI vjerodajnica kako je navedeno u petom poglavlju dokumenta o Arhitekturi i referentnom okviru EUDI digitalnog novčanika [4].

Prema izvoru [5], provjerljive vjerodajnice (VC) su digitalna i kriptografski zaštićena verzija papirnatih i digitalnih vjerodajnica koje na siguran i pouzdan način dokazuju identitet ili kvalifikacije fizičke osobe. Njihova glavna prednost u odnosu na fizičke vjerodajnice je to što su digitalno potpisane, što ih čini otpornima na manipulacije i provjerljivima.

EUDI arhitektura razlikuje četiri vrste vjerodajnica ovisno o pravnom statusu izda-

vatelja:

- Podaci o identifikaciji osobe (PID): Skup podataka koji se izdaju u skladu sa zakonom Europske unije ili članice. To su informacije koje omogućuju utvrđivanje identiteta fizičke ili pravne osobe.
- Kvalificirana digitalna vjerodajnica atributa (QEAA): Vjerodajnica koju izdaje kvalificirani pružatelj.
- Digitalna vjerodajnica atributa izdana od strane javne vlasti odgovornog za autentični izvor (PuB-EAA).
- Nekvalificirana digitalna vjerodajnica: Ova vjerodajnica obuhvaća sve ostale digitalne vjerodajnice koje nisu kvalificirane prema propisima Europske unije ili članica.

Svaka vjerodajnica sadrži shemu atributa koja definira strukturu, informaciju o formatu podataka i mehanizam provjere.

Trenutno su dostupni neki standardizirani formati vjerodajnica:

- ISO/IEC 18013-5: Definira shemu atributa, format podataka i mehanizme dokaza za mobilne vozačke dozvole (mDL), ali se može koristiti i s drugim shemama atributa.
- Selektivno otkrivanje za JWT-ove (SD-JWT): Definira mehanizam dokaza sličan onome u [ISO/IEC 18013-5], ali za drugačiji format podataka.
- W3C model provjerljivih vjerodajnica v1.1 [W3C VC DM v1.1]: Definira generičku shemu atributa neovisnu o formatima podataka i mehanizmima dokaza, dok verzija 2.0 uvodi zahtjeve za format i preporuke za mehanizme dokaza.

3. OpenID

3.1. Oauth 2.0

Ovo poglavlje ukratko opisuje OAuth 2.0 protokol zbog njegove ključne uloge u OpenID specifikacijama. Informacije o protokolu su preuzete sa službene OAuth 2.0 stranice [6].

OAuth 2.0 (*Open Authorization*) je standardni protokol dizajniran za omogućavanje web stranicama ili aplikacijama pristup resursima koji se nalaze na drugim web aplikacijama u ime korisnika. OAuth 2.0 pruža pristup uz suglasnost i ograničava radnje koje klijentska aplikacija može izvršiti nad resursima u ime korisnika, a da nikada izravno ne dijeli korisničke podatke.

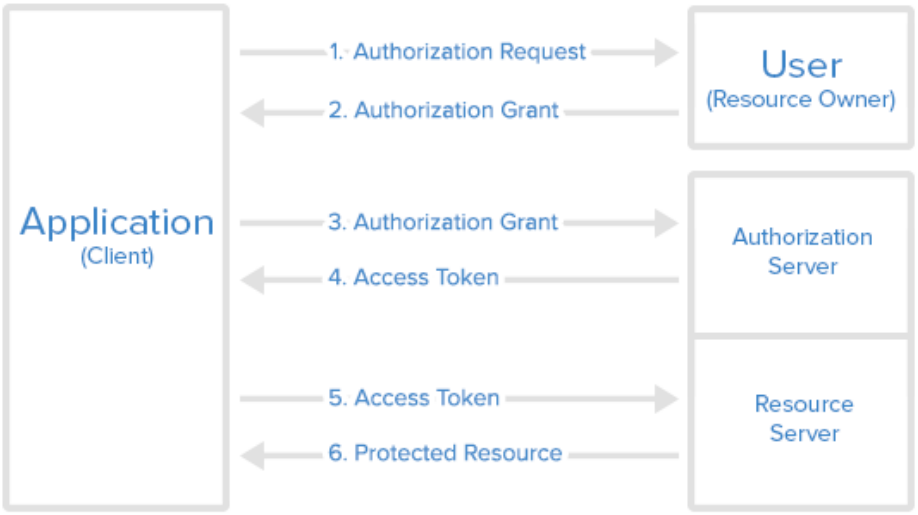
OAuth 2.0 koristi pristupne tokene. Pristupni token je podatak koji predstavlja ovlast za pristup resursima u ime krajnjeg korisnika. OAuth 2.0 ne definira specifičan format pristupnih token-a. Međutim, u nekim kontekstima, često se koristi *JSON Web Token* (JWT) format. Pristupni tokeni mogu imati datum isteka.

Proces autorizacije počinje kada klijent zatraži dopuštenje za pristup određenim resursima od autorizacijskog poslužitelja. Klijent pritom pruža svoje identifikacijske podatke, uključujući svoj identifikacijski broj i klijentsku tajnu. Također specificira resurse kojima želi pristupiti i URI za preusmjeravanje na koji će poslužitelj autorizacije poslati pristupni token ili autorizacijski kod.

Nakon što klijent zatraži autorizaciju, poslužitelj autorizacije autentificira klijenta i provjerava je li zatraženi pristup odobren od strane korisnika. Ako je pristup odobren, poslužitelj autorizacije generira pristupni token ili autorizacijski kod te ih vraća klijentu. Pristupni token omogućuje klijentu da pristupi resursima na poslužitelju resursa bez potrebe za ponovnom autentifikacijom.

Klijent zatim koristi pristupni token kako bi pristupio resursima na poslužitelju resursa. Pristupni token se šalje poslužitelju resursa u svakom zahtjevu za pristupom resursima, gdje se provjerava njegova valjanost i dopušteni opsezi resursa. Na taj način, OAuth 2.0 omogućuje siguran i kontroliran pristup resursima na drugim web aplikacijama u ime korisnika, čuvajući pritom privatnost i sigurnost korisničkih podataka.

Slika 3.1. ukratko prikazuje opisani proces autorizacije.



Slika 3.1. Prikaz OAuth 2.0 procesa [7]

3.2. OpenID za izdavanje provjerljivih vjerodajnica

OID4VCI (*OpenID for verified credentials issuance*) specifikacija definira proces izdavanja provjerljivih isprava putem definiranih API-ja. Taj proces uključuje nekoliko koraka kako je navedeno u izvoru [8].

Prvo, digitalni novčanik korisnika otkriva mogućnosti izdavatelja vjerodajnica putem poznate konfiguracije, obično kao JSON dokument na domeni izdavatelja. Taj dokument sadrži metapodatke o izdavatelju, poput endpointa za izdavanje vjerodajnica, endpointa za autorizaciju i ostalih detalja važnih za komunikaciju između korisnika i izdavatelja.

Na primjer, student skenira QR kod koji je postavljen na web stranici fakulteta. QR kod vodi do JSON dokumenta koji sadrži URL-ove potrebne za komunikaciju s API-jem za izdavanje.

Nakon toga, izdavatelj šalje poziv za izdavanje isprava, obično u obliku QR koda ili NFC-a. Taj poziv sadrži bitne informacije o ispravi koja se nudi, namjerama izdavatelja te upućuje na endpointe za upravljanje procesom izdavanja.

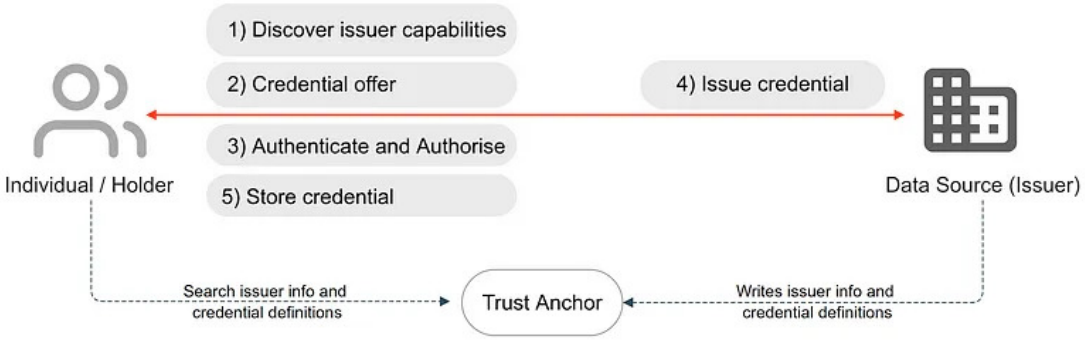
Zatim slijedi korak autentifikacije i autorizacije, u kojem digitalni novčanik komunicira s izdavateljevim endpointima kako bi pokrenuo proces izdavanja. To uključuje inicijaciju OAuth zahtjeva za autorizaciju te dobivanje autorizacijskog koda od autentifikacijskog poslužitelja.

Primjer može biti student koji je zatražio izdavanje diplome. Fakultet (izdavatelj) šalje poziv za izdavanje diplome u obliku QR koda. Korisnik skenira QR kod svojim digitalnim novčanikom, koji zatim pokreće autentifikaciju putem OAuth zahtjeva. Nakon što korisnik unese svoje vjerodajnice i dobije autorizacijski kod, fakultet izdaje digitalnu diplomu.

Kada je korisnik autoriziran, digitalni novčanik dobiva valjani pristupni token, koji se koristi za izdavanje vjerodajnice. Vjerodajnica se izdaje putem odgovarajućeg *endpoint*-a, a korisnik je može zatražiti više puta ili za različite svrhe.

Na kraju, izdana isprava se pohranjuje u digitalni novčanik korisnika za buduće prezentacije i korištenje. Ovaj proces omogućuje korisnicima da imaju kontrolu nad svojim provjerljivim ispravama i olakšava njihovo korištenje u različitim kontekstima.

Slika 3.2. ilustrira korake OID4VCI specifikacije.



Slika 3.2. Proces izdavanja vjerodajnice [8]

3.3. OpenID za provjerljive prezentacije

OID4VP (*OpenID for verifiable presentations*) definira specifikaciju usmjerenu na korištenje vjerodajnica za autentifikaciju korisnika. Informacije o protokolu su preuzete iz izvora [8].

Ova metodologija omogućuje korisnicima da pokažu kontrolu nad decentraliziranim identifikatorom (DID) i autentificiraju se s uslugom, eliminirajući potrebu za centraliziranim pružateljem identiteta.

Prema [8], protokol OID4VP omogućuje izravnu upotrebu vjerodajnica za autentikaciju, naglašavajući korisnički pristup. Protokol je pažljivo dizajniran kako bi smanjio nepotrebno otkrivanje osobnih informacija tijekom cijelog procesa. Korisnicima se omogućuje izravna prezentacija njihovih provjerljivih isprava pouzdanoj strani, što povećava privatnost i korisničku autonomiju u dijeljenju podataka.

OID4VP omogućuje strukturirano otkrivanje sposobnosti i konfiguracija provjerivača putem strojno čitljivog formata. To djeluje kao nacrt koji detaljno opisuje kako digitalni novčanici trebaju komunicirati s provjerivačima. Ovaj konfiguracijski dokument je smješten na dobro definiranom URI endpointu na domeni provjerivača i kodiran je u JSON formatu, otkrivajući bitne informacije o provjerivaču.

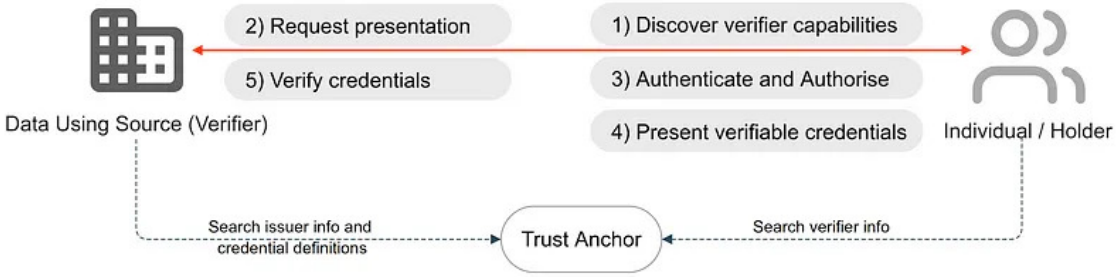
Zahtjev za prezentaciju obično je enkapsuliran unutar QR koda ili NFC uređaja, generiran od strane provjerivača, i sadrži strukturirani skup zahtjeva i uputa koji detaljno opisuju specifične provjerljive vjerodajnice ili tvrdnje tražene od nositelja. Nakon što korisnik skenira QR kod ili koristi NFC uređaj, zahtjev za prezentaciju se izvlači i obrađuje. Ovaj zahtjev sadrži definiciju prezentacije definiranu od strane provjerivača. Provjerljiva prezentacija (VP) se konstruira na temelju definicije prezentacije. Nakon potvrde razmjene podataka, token se vraća provjerivaču. Nakon što primi token, provjerivač može kriptografski provjeriti autentičnost prezentiranih isprava i, ako je potrebno, provjeriti status opoziva isprave u registru opoziva.

Na primjer, student koristi svoj digitalni novčanik da se prijavi na fakultetski portal. Fakultet (provjerivač) generira QR kod koji student skenira pomoću digitalnog novčanika. QR kod sadrži zahtjev za prezentaciju diplome. Digitalni novčanik studenta gene-

rira provjerljivu prezentaciju na temelju pohranjene digitalne diplome i šalje je natrag fakultetu. Fakultet zatim kriptografski provjerava autentičnost diplome, osiguravajući da je diploma stvarna i da nije opozvana.

OID4VP omogućuje fleksibilnost u različitim scenarijima, uključujući *online*, *offline*, i *in-person* provjere. Na primjer, student može koristiti svoj digitalni novčanik za *online* autentifikaciju putem vjerodajnice na web stranici koja traži pristup određenim podacima. Alternativno, student može koristiti svoj mobilni uređaj za *offline* prezentaciju vjerodajnice putem NFC-a pri fizičkom susretu s provjerivačem.

Slika 3.3. ilustrira korake OID4VP specifikacije.



Slika 3.3. Proces provjere vjerodajnice [8]

4. Implementacija prototipa za izdavanje digitalne osobne iskaznice

Ovo poglavlje opisuje implementaciju sustava za izdavanje i provjeru digitalnih vjerodajnica. Cilj implementacije bio je razviti funkcionalan prototip koji omogućuje korisnicima jednostavno preuzimanje i pohranu vjerodajnica u digitalne novčanike te njihovu sigurnu i pouzdanu provjeru. Kao primjer vjerodajnice u sustavu izabrana je osobna iskaznica zbog mogućnosti čitanja osobnih podataka s certifikata.

Jedan od izazova bio je pravilno filtriranje i očitavanje certifikata. Konkretno, problem je predstavljala neispravna verzija TLS protokola. Kada verzija nije bila ispravno određena u kodu servera, server je odbijao certifikat e-osobne iskaznice, što je bilo teško dijagnosticirati. Uz pomoć mentora, verzija TLS-a je postavljena na 1.2, čime je problem riješen.

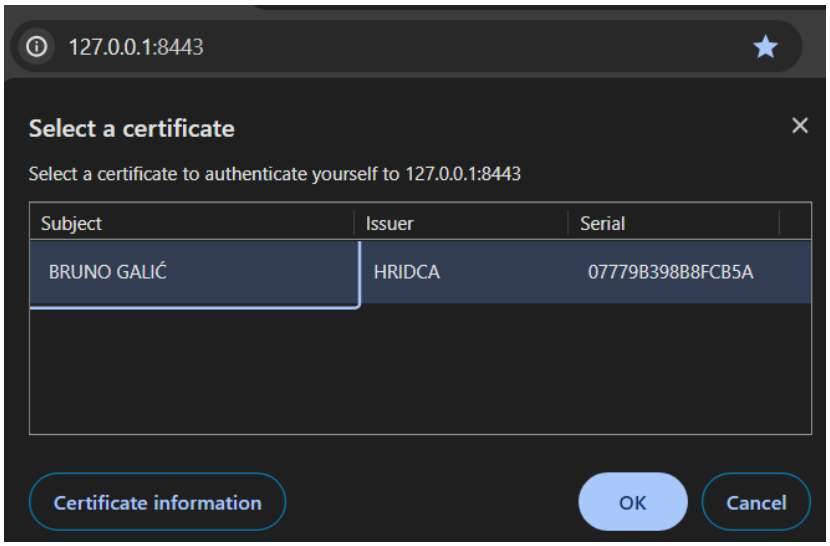
Za implementaciju sustava korištene su sljedeće tehnologije:

- Node.js za postavljanje servera i web stranicu
- TLS protokol za rad s certifikatom e-osobne
- REST API za pozivanje Walt id API-ja za izdavanje
- QR kod tehnologija za pretvaranje adrese u QR kod koji se može očitati kamerom
- OID4VCI protokol za izdavanje vjerodajnice
- OID4VP za prezentaciju i provjeru vjerodajnice

U nastavku se nalazi opis korištenja prototipa te tehnički detalji implementacije.

4.1. Korištenje prototipa

Proces započinje stavljanjem e-osobne iskaznice u čitač pametnih kartica. Korisnik potom posjećuje stranicu za izdavanje vjerodajnice, gdje se prilikom učitavanja stranice koristi certifikat e-osobne iskaznice.

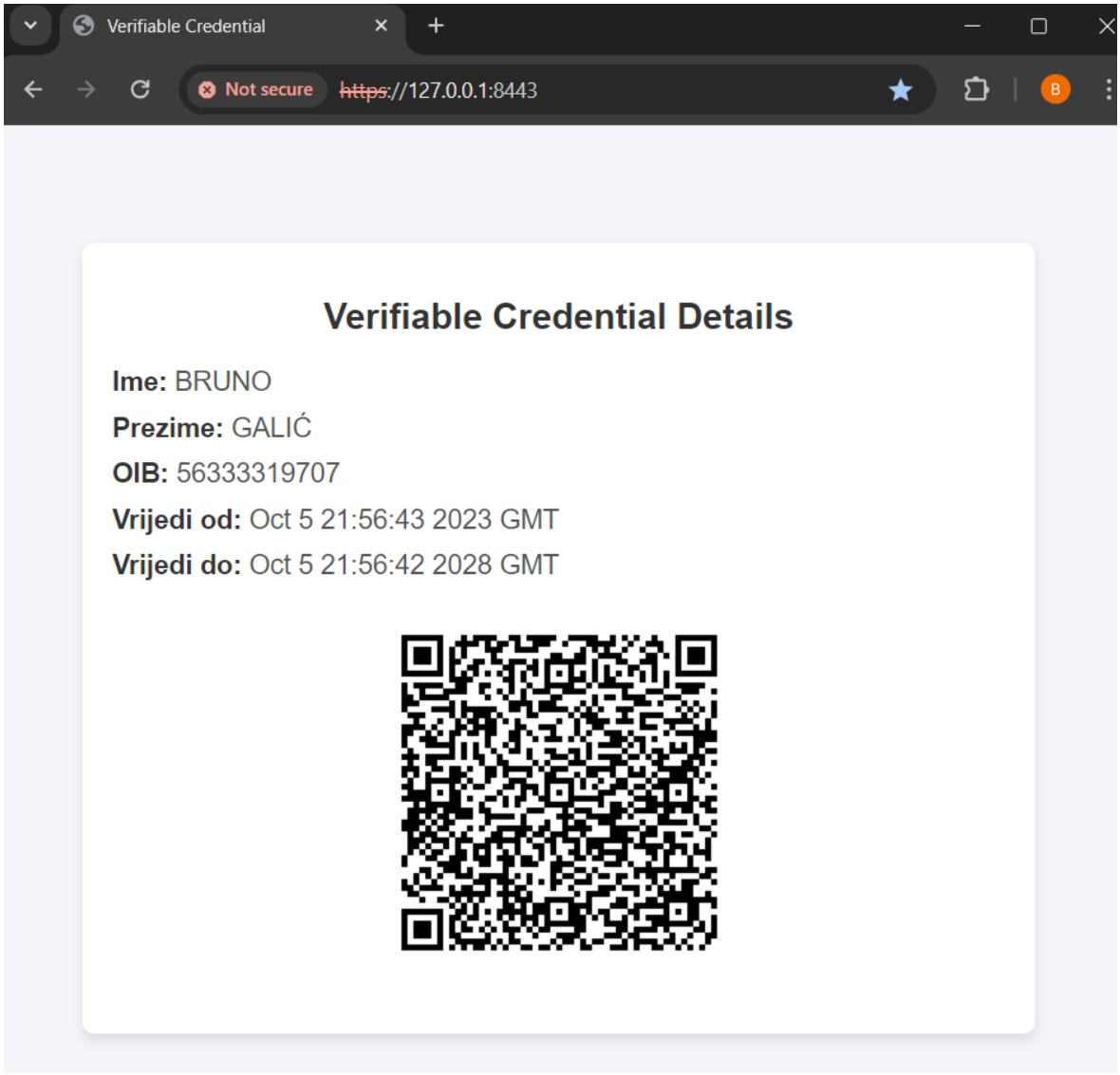


Slika 4.1. Odabir certifikata

Nakon unosa PIN-a e-osobne, korisnik pristupa stranici.

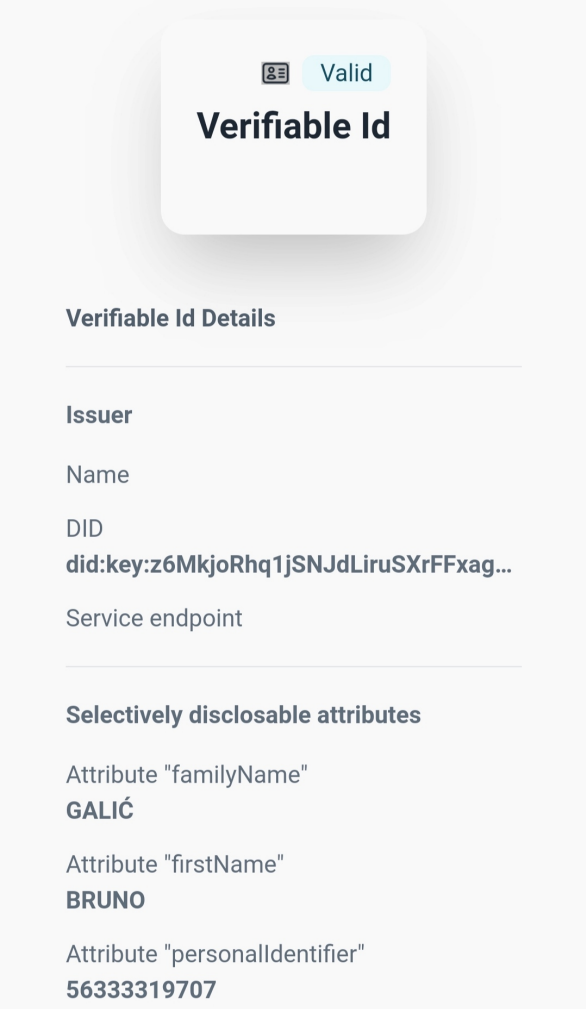
Stranica tada izvlači osnovne podatke iz certifikata osobne iskaznice, upisuje ih u vjerodajnicu i šalje API poziv Walt ID izdavatelju. Kao odgovor dobiva link za izdavanje vjerodajnice.

Stranica zatim pretvara ovaj link u QR kod i prikazuje ga zajedno s osnovnim podacima.



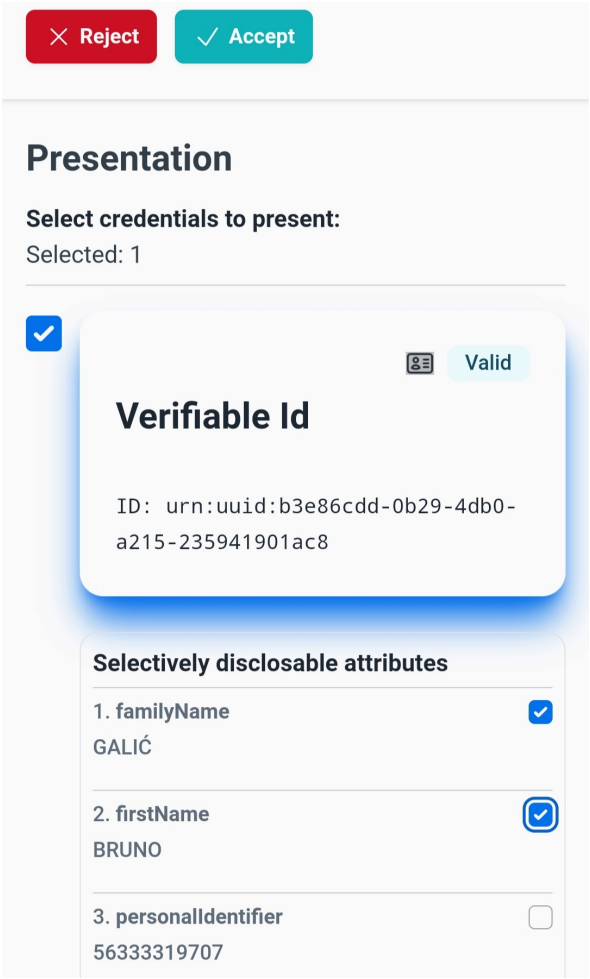
Slika 4.2. Prikaz prototipa za izdavanje vjerodajnica

Korisnik skenira QR kod Walt ID novčanikom i tako preuzima izdanu vjerodajnicu. Vjerodajnica se sprema u korisnikov novčanik, spremna za prezentaciju i provjeru.



Slika 4.3. Vjerodajnica u novčaniku korisnika

Provjera se može izvršiti putem Walt ID web stranice koristeći selektivno otkrivanje (*selective disclosure*).



Slika 4.4. *Selective disclosure*

4.2. Opis implementacije

Implementacija prototipa sastoji se od nekoliko ključnih komponenti koje zajedno omogućuju izdavanje vjerodajnice korisniku.

Prva komponenta je Node.js server. Server je zadužen za upravljanje certifikatima, dohvaćanje potrebnih podataka, pozivanje *Issuance* API-ja te prikaz QR koda korisniku.

Druga važna komponenta je Walt ID sustav. Ovaj sustav implementira prototip digitalnog novčanika te nudi API-je za izdavanje i provjeru vjerodajnica. Walt ID sustav osigurava da vjerodajnice budu pohranjene i upravljane na siguran način, omogućujući

korisnicima jednostavan pristup i upravljanje.

Konačno, tu je i sama *verifiable ID* vjerodajnica. Ova digitalna vjerodajnica omogućuje korisnicima pouzdanu identifikaciju. *Verifiable ID* vjerodajnica koristi standardizirane protokole i metode kako bi se osigurala njena autentičnost i integritet.

Svaka od ovih komponenti bit će detaljno opisana u sljedećim poglavljima.

4.3. Node.js

Node.js je JavaScript izvršno okruženje koje je odabrano za ovaj prototip zbog svoje jednostavnosti u razvoju i lake prenosivosti, odnosno dobre integracije s Docker kontejnerima. Aplikacija koristi nekoliko modula: *express* kao okvir za izgradnju web aplikacija, *https* modul za sigurne HTTPS veze, *fs* modul za rad s datotekama, *axios* za poziv API-ja, *ejs* za prikaz HTML predložaka i *qrcode* za pretvaranje poveznice u QR kod.

Prvi korak je postavljanje opcija za HTTPS server. Konfiguracija, prikazana na sljedećoj slici, uključuje *atribute key* i *cert* koji se koriste za enkriptiranu komunikaciju između klijenta i servera. Atribut *ca (Certificate Authority)* definira popis certifikata kojima server vjeruje. U ovom slučaju, postavljeno je da server prihvaća samo certifikate e-osobne [9]. Atribut *requestCert: true* označuje da server zahtjeva certifikat od klijenta, *secureProtocol* definira verziju TLS protokola koju server koristi.

```
const options = {
  key: fs.readFileSync("privatni_kljuc.pem"),
  cert: fs.readFileSync("javni_kljuc.pem"),
  ca: fs.readFileSync("lista_certifikata_povjerenja.crt"),
  requestCert: true,
  rejectUnauthorized: true,
  secureProtocol: "TLSv1_2_method",
};
```

Slika 4.5. HTTPS konfiguracija

Nakon postavljanja opcija za HTTPS server, sljedeći korak je dohvaćanje osnovnih informacija iz certifikata. Ove informacije obuhvaćaju ime, prezime, OIB, datum izdavanja i datum do kada osobna iskaznica vrijedi. Nakon što su ovi podaci dobiveni, koriste se za kreiranje *verifiable ID* vjerodajnice, koja će biti detaljnije opisana kasnije.

```
app.get("/", (req, res) => {
  const cert = req.socket.getPeerCertificate();
  console.log(cert);
  const userName = cert.subject.GN;
  const userSurname = cert.subject.SN;
  const userOib = cert.subject.serialNumber.replace(/\D/g, "");
  const validFrom = cert.valid_from;
  const validTo = cert.valid_to;
```

Slika 4.6. Dohvaćanje podataka iz certifikata

Posljednji korak servera je pozvati Walt Id API za izdavanje [10] kako bi se izdala *verifiable ID* vjerodajnica. Nakon što API uspješno odgovori, server generira QR kod koji sadrži vraćenu poveznicu za izdavanje vjerodajnice. Korisniku se tada prikazuje ovaj QR kod kako bi mogao pristupiti vjerodajnici.

4.4. VerifiableId vjerodajnica

Za prototip sustava je odabrana Walt Id VerifiableId [11] vjerodajnica prikazana na sljedećoj slici.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "type": [
    "VerifiableCredential",
    "VerifiableAttestation",
    "VerifiableId"
  ],
  "credentialSchema": {
    "id": "https://api.preprod.ebsi.eu/trusted-schemas-registry/v1/schemas/0xb77f8516a965631b4f1
    "type": "FullJsonSchemaValidator2021"
  },
  "credentialSubject": {
    "currentAddress": [
      "1 Boulevard de la Liberté, 59800 Lille"
    ],
    "dateOfBirth": "1993-04-08",
    "familyName": "DOE",
    "firstName": "Jane",
    "gender": "FEMALE",
    "id": "did:ebsi:2AEMAqXWKYMu1JHPAgGcga4dxu7ThgfgN95VyJBJGZbSJUtp",
    "nameAndFamilyNameAtBirth": "Jane DOE",
    "personalIdentifier": "0904008084H",
    "placeOfBirth": "LILLE, FRANCE"
  },
  "evidence": [
    {
      "documentPresence": [
        "Physical"
      ],
      "evidenceDocument": [
        "Passport"
      ],
      "subjectPresence": "Physical",
      "type": [
        "DocumentVerification"
      ],
      "verifier": "did:ebsi:2A9BZ9SUe6BatacSpvs1V5CdjHvLpQ7bEsi2Jb6LdHKnQxaN"
    }
  ],
  "id": "urn:uuid:3add94f4-28ec-42a1-8704-4e4aa51006b4",
  "issued": "2021-08-31T00:00:00Z",
  "issuer": "did:ebsi:2A9BZ9SUe6BatacSpvs1V5CdjHvLpQ7bEsi2Jb6LdHKnQxaN",
  "validFrom": "2021-08-31T00:00:00Z",
  "issuanceDate": "2021-08-31T00:00:00Z"
}
```


Slika 4.7. VerifiableId vjerodajnica [11]

Vjerodajnica služi za digitalno predstavljanje osobnih podataka. Podaci koji se nalaze unutar nje preuzeti su s certifikata, kao što je prethodno spomenuto. Temelji se na W3C [12] specifikaciji i koristi W3 kontekst koji definira strukturu i tipove podataka unutar vjerodajnice.

Najvažniji dio vjerodajnice je *credentialSubject*, gdje su sadržani osobni podaci. Ovdje su navedeni osnovni podaci poput imena, prezimena, adrese, datuma rođenja i osobnog identifikatora.

Uz *credentialSubject*, postoji i dio *evidence* koji sadrži potvrdu o ispravnosti osobnih podataka. Ovdje bi se mogla nalaziti informacija o izvornom dokumentu, poput osobne iskaznice koja je sadržala certifikat.

Ostali dijelovi vjerodajnice uključuju vremenske oznake izdavanja, identifikacijski broj i identifikator izdavača, koji pomažu u provjeri autentičnosti vjerodajnice i njezinog izvora.

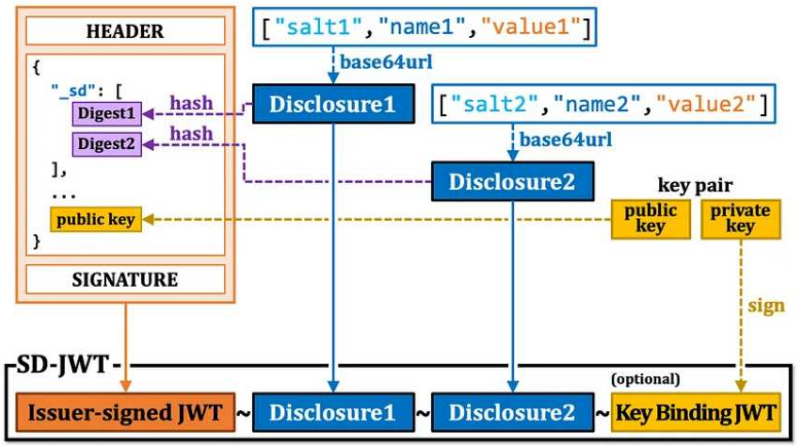
Za izdavanje je korišten SD-JWT dokument. SD-JWT je digitalno potpisani JSON dokument koji podržava selekciju podataka koji se žele provjeriti [13]. To znači da korisnik koji posjeduje vjerodajnicu može birati koje će podatke dati na provjeru, na primjer, može dati dozvolu za ime i prezime, ali zabraniti OIB.

```
selectiveDisclosure: {
  fields: {
    credentialSubject: {
      sd: false,
      children: {
        fields: {
          familyName: { sd: true },
          firstName: { sd: true },
          personalIdentifier: { sd: true },
        },
```

Slika 4.8. SD dodatak vjerodajnici

Prema izvoru [14], u SD-JWT-u, umjesto jednostavnog potpisivanja svih podataka zajedno, struktura se prilagođava kako bi se omogućilo selektivno otkrivanje informacija. To se postiže tako da se sažete informacije o nasumičnoj soli, ključu i vrijednosti svakog podatka spremaju unutar strukture koja se potpisuje. Budući da ova struktura sadrži sažete podatke, iz nje nije moguće izvući izvorne informacije. Informacije o soli, ključu i vrijednosti podataka koje se žele otkriti enkodirane su u *base64url* formatu i pridružuju se uz strukturu i potpis, osiguravajući tako sigurnost i valjanost SD-JWT-a. Ukratko, provjera valjanosti SD-JWT-a se provodi tako što se prvo provjeri potpis strukture koja sadrži sažete informacije o soli, ključu i vrijednosti svakog podatka. Nakon toga, provjeravaju se podaci koji su enkodirani u *base64url* formatu i pridruženi uz strukturu i potpis. Ovaj

postupak, ilustriran sljedećom slikom, osigurava integritet i valjanost SD-JWT-a, omogućujući selektivno otkrivanje informacija uz visoku razinu sigurnosti.



Slika 4.9. SD-JWT struktura [14]

4.5. walt.id

Walt.id je open-source infrastruktura za digitalni identitet i digitalne novčanike.

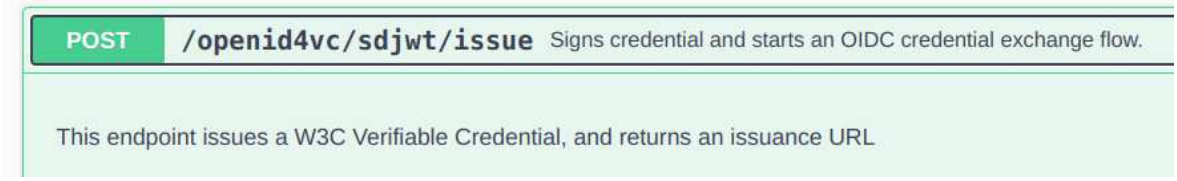
Walt.id pruža Kotlin knjižnicu [15] za implementaciju modela podataka i protokola specifikacija OpenID za provjerljive vjerodajnice, uključujući OID4VCI, OID4VP i SIOPv2.

Kotlin *Multiplatform* SD-JWT knjižnica [16] osmišljena je za stvaranje JSON Web Tokena (JWT) s podrškom za selektivno otkrivanje (*selective disclosure*). Ova funkcionalnost omogućuje da se određeni dijelovi JWT korisničkih podataka otkriju ili sakriju ovisno o zahtjevima interakcije među stranama.

Kotlin *Multiplatform* knjižnica za *Verifiable Credentials* [15] omogućava kreiranje i potpisivanje W3Cv1.1 i W3Cv2.0 vjerodajnica (JWT, SD-JWT) koristeći JWS shemu potpisa, te pruža statička i dinamički konfigurabilna svojstva za upravljanje i validaciju politika vjerodajnica i prezentacija. Knjižnica se oslanja na walt.id komponente kao što su waltid-sd-jwt za SD-JWT povezane procese, waltid-did za DID povezane operacije, te waltid-crypto za ključne kriptografske operacije.

Za izdavanje vjerodajnice korišten je Walt ID SD-JWT issuer API na razvojnom poslužitelju. API prima vjerodajnicu prikazanu u prethodnom poglavlju i vraća URL za

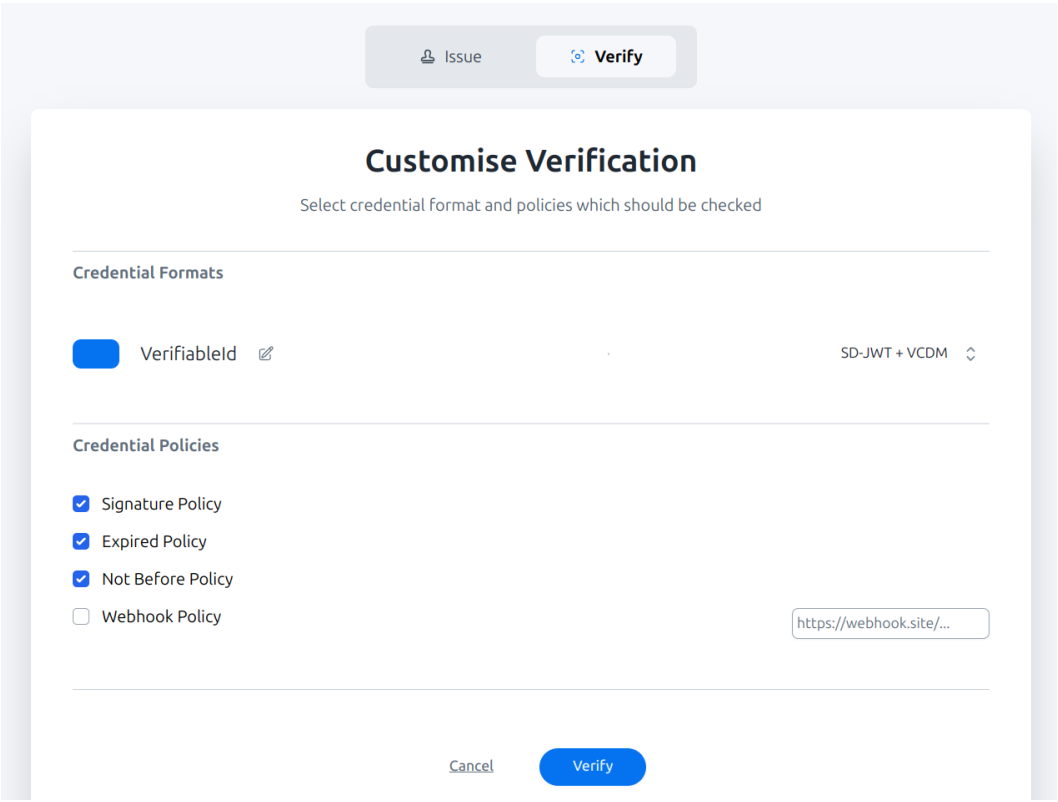
izdavanje vjerodajnice.



Slika 4.10. SD-JWT issuer API [17]

Kao novčanik korištena je javno dostupna implementacija novčanika. Web novčanik [18] je platforma koja se temelji na dostupnim knjižnicama Walt ID-a te pruža raznolike funkcionalnosti, uključujući razmjenu vjerodajnica. Nudi kompletnu implementaciju procesa izdavanja, pohranu vjerodajnica te njihovu provjeru.

Konačno za provjeru možemo iskoristiti Walt ID portal [19] koji nudi provjeru vjerodajnice.



Slika 4.11. Walt Id portal za provjeru vjerodajnica [19]

5. Zaključak

Ovaj rad proučava implementaciju i arhitekturu Europskog digitalnog novčanika, s naglaskom na pilot-projekte provedene u Njemačkoj i Italiji. Prema arhitekturi je uspješno razvijen prototip *offline* sustava za izdavanje digitalnih osobnih iskaznica, to jest sustava koji bi se, na primjer, koristio u policijskoj postaji. Prototip omogućuje korisnicima jednostavan proces izdavanja vjerodajnica putem čitanja certifikata s fizičke osobne iskaznice, prikupljanjem osobnih podataka te generiranja QR koda koji se koristi za izdavanje digitalne osobne iskaznice. Ovaj proces je integriran s Walt ID sustavom, pružajući korisnicima siguran način pohrane i prezentacije vjerodajnica.

Iako je prototip uspješno implementiran, postoji prostor za daljnje unapređenje. Primjerice, moguće je proširiti funkcionalnosti sustava putem EOI *middleware* aplikacije za uključivanje više podataka. Trenutna verifikacija vjerodajnica oslanja se na njihovu valjanost, no postoji potreba za dodatnom provjerom ispravnosti identiteta korisnika putem biometrijskih podataka poput slike.

Još jedna značajna mogućnost za unaprjeđenje je konceptualizacija online procesa za izdavanje digitalnih osobnih iskaznica, pri čemu bi se posebna pažnja posvetila verifikaciji identiteta osobe koja zahtijeva izdavanje, kao i osiguranju pouzdane komunikacije između korisnika i izdavača.

Dodatno, važno je naglasiti da trenutni sustav predstavlja prototip koji samo ilustrira proces izdavanja. Kako bi se smanjila ovisnost o Walt ID platformi, potrebna je reimplementacija sustava od samih temelja, koristeći stabilne knjižnice niže razine. Ovo bi moglo uključivati izradu digitalne vjerodajnice koja bi izravno odgovarala osobnoj iskaznici u Republici Hrvatskoj, te izgradnju novčanika kao prave mobilne aplikacije. Postojeće implementacije u Njemačkoj i Italiji bi dosta olakšale takav pristup.

Sveukupno, ciljevi ovog istraživanja su ostvareni, te se prototip sada može koristiti u svrhu daljnjeg istraživanja i kao jednostavan primjer za buduće implementacije.

Literatura

[1] Directorate-General for Communication, "European Digital Identity", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en, [Stranica posjećena 30. svibnja 2024.].

[2] Directorate-General for Communications Networks, Content and Technology, "EU Digital Identity Wallet Pilot implementation", https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation, travanj 2024., [Stranica posjećena 30. svibnja 2024.].

[3] Gataca, "Everything you need to know about the EUDI Wallet", https://gataca.io/blog/eudi-wallet/, ožujak 2024., [Stranica posjećena 30. svibnja 2024.].

[4] Official GitHub Organization of the European Digital Identity project, "European Digital Identity Wallet Architecture and Reference Framework", https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md, svibanj 2024., [Stranica posjećena 30. svibnja 2024.].

[5] Wikipedia, "Verifiable credentials", https://en.wikipedia.org/wiki/Verifiable_credentials, ožujak 2024., [Stranica posjećena 30. svibnja 2024.].

[6] Okta, "What is OAuth 2.0?" https://auth0.com/intro-to-iam/what-is-oauth-2, [Stranica posjećena 30. svibnja 2024.].

[7] Mitchell Anicas, "An Introduction to OAuth 2", https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2, srpanj 2021., [Stranica posjećena 30. svibnja 2024.].

[8] Lal Chandran, “EUDI wallets with OpenID for verifiable credentials”, https://medium.com/value-of-trust/eudi-wallets-with-openid-for-verifiable-credentials-6131c8098e0d, studeni 2023., [Stranica posjećena 30. svibnja 2024.].

[9] eOsobna HR, “Certifikati AKDCA Root i HRIDCA”, https://www.eid.hr/hr/certifikati/certifikati-akdca-root-i-hridca, [Stranica posjećena 30. svibnja 2024.].

[10] walt.id, “Walt ID API za izdavanje vjerodajnica”, https://issuer.portal.walt.id/openid4vc/sdjwt/issue, [Stranica posjećena 30. svibnja 2024.].

[11] ——, “VerifiableId”, https://credentials.walt.id/credentials/verifiableid, [Stranica posjećena 30. svibnja 2024.].

[12] W3C, “About W3C web standards”, https://www.w3.org/standards/about/, [Stranica posjećena 30. svibnja 2024.].

[13] EBSI, “Selective Disclosure with SD-JWT”, https://hub.ebsi.eu/vc-framework/did/selective-disclosure-sd-jwt, veljača 2024., [Stranica posjećena 30. svibnja 2024.].

[14] Takahiko Kawasaki, “Issuing verifiable credentials in the SD-JWT VC and mdoc/mDL formats, mandated in eIDAS 2.0”, https://darutk.medium.com/oid4vci-demo-87a232cfcc2a, veljača 2024., [Stranica posjećena 30. svibnja 2024.].

[15] walt.id, “OpenID4VC - Kotlin multiplatform library”, https://github.com/walt-id/waltid-identity/blob/main/waltid-openid4vc/README.md, ožujak 2024., [Stranica posjećena 30. svibnja 2024.].

[16] ——, “Kotlin Multiplatform SD-JWT library”, https://github.com/walt-id/waltid-identity/blob/main/waltid-sdjwt/README.md, svibanj 2024., [Stranica posjećena 30. svibnja 2024.].

[17] ——, “Walt ID API server za testiranje”, https://issuer.portal.walt.id/swagger/index.html, [Stranica posjećena 30. svibnja 2024.].

[18] ——, “Walt ID novčanik”, https://wallet.walt.id/, [Stranica posjećena 30. svibnja 2024.].

[19] ——, “Walt ID portal za provjeru vjerodajnice”, https://portal.walt.id/credentials?ids=VerifiableId&mode=verification, [Stranica posjećena 30. svibnja 2024.].

Sažetak

Digitalne vjerodajnice u skladu s europskim digitalnim identitetom

Bruno Galić

Cilj uvođenja Europskog digitalnog identiteta je olakšati prijenos i provjeru važnih dokumenata unutar EU-a. Ovaj rad predstavlja implementaciju prototipa sustava za izdavanje digitalne osobne iskaznice, temeljenog na certifikatima pametne osobne iskaznice u Republici Hrvatskoj. Opisana je arhitektura i referentni okvir EUDI digitalnog novčanika, uključujući strukturu, komponente i sučelja sustava. Kroz ovaj rad ističu se ključne prednosti EUDI-a, poput poboljšane sigurnosti, jednostavnosti upotrebe i interoperabilnosti, kao i propisane specifikacije za izdavanje i provjeru vjerodajnica, OID4VCI i OID4VP. Rad sadrži detaljan opis implementacije prototipa i primjer izdavanja vjerodajnice.

Ključne riječi: Europski digitalni identitet; Provjerljiva vjerodajnica; Digitalni novčanik; Digitalna osobna iskaznica

Abstract

Verifiable credentials compatible with the european digital identity framework

Bruno Galić

The aim of introducing the European Digital Identity is to simplify the transfer and verification of important documents within the EU. This paper presents the implementation of a prototype system for issuing a digital identity credential, based on the certificates of the smart identity card in the Republic of Croatia. It details the architecture and reference framework of the EUDI digital wallet, covering the system's structure, components, and interfaces. The key advantages of EUDI are also highlighted, such as improved security, ease of use, and interoperability, as well as the prescribed specifications for issuing and verifying credentials, OID4VCI and OID4VP. The paper contains a detailed description of the prototype implementation and an example of credential issuance.

Keywords: European Digital Identity; Verifiable Credential; Digital Wallet; Digital Identity Credential