Kdo in zakaj potrebuje Program nagrajevanja za varnostne hrošče?

Denis Tomašević

Nicehash, Maribor, Slovenija
denis@nicehash.com

V Sloveniji je že precej uveljavljeno iskanje ranljivosti z varnostnimi pregledi, ki se izvajajo enkrat letno (kampanjski pristop, ki ga predpisujejo regulatorji). Ti pregledi so dragi zaradi svojega obsega in omejenega števila strokovnjakov v Sloveniji, stanejo pa enako, ne glede na to, ali ima rešitev tisoč ranljivosti ali nobene. Program Security Bug Bounty omogoča pokritost 365 dni v letu in neomejen nabor strokovnjakov z vsega sveta za ceno, ki je sorazmerna trenutni varnostni kondiciji rešitve. Vsebina prispevka bo uporabna tako za tiste, ki bi radi začeli iskati varnostne ranljivosti (kot glavni ali dodatni vir prihodka), kot za tiste, ki ranljivosti ustvarjajo (razvijalci, arhitekti, upravljavci rešitev …), pa tudi za tiste, ki bi morali skrbeti za varno delovanje rešitev (vodje razvoja ter strokovnjaki za informacijsko varnost in skladnost z regulatornimi okviri).

Ključne besede:
Bug Bounty
vdorno testiranje (PenTest)
kibernetska varnost
varnostne ranljivosti
CrowdSource varnostno testiranje

Univerzitetna založba Univerze v Mariboru

ISBN 978-961-299-188-3
DOI https://doi.org/10.18690/um.feri.7.2026.12

1 Kdo in zakaj potrebuje PenTest?

Varnostni pregled z izvajanjem vdornih testov (PenTest), v katerem izvajalec uporablja enake metode in tehnike kot dejanski napadalci, je najučinkovitejše preverjanje trenutnega varovanja aplikacije, platforme ali informacijskega sistema.

Testiranje s simulacijo napadov zahteva veliko strokovnega znanja in aktivno spremljanje novih ranljivosti ter načinov zlorabe, izvedba PenTesta na produkcijskem okolju pa je tvegana, saj uspešen napad lahko ogrozi integriteto ali zaupnost podatkov uporabnikov, zato je PenTest priporočljivo izvajati na kopiji produkcijskega okolja brez dejanskih podatkov (testno okolje). Ne glede na to je izvedba določenega nabora vdornih testov na produkcijskem okolju smiselna in potrebna (brez agresivnih testov), ker lahko odkrije ranljivosti, ki so posledica nedosledne konfiguracije ali posebnosti produkcijskega okolja, vendar je takšne teste smiselno omejiti na nujni minimum in jih izvajati na posebnih uporabniških računih.

PenTest v resnici potrebuje vsaka organizacija, ki ji je pomembna dejanska varnost svojih uporabnikov in podatkov, če je pripravljena sprejeti in uporabiti rezultate za izboljšanje svoje varnosti. Slika v tako »nastavljenem ogledalu« pogosto ni prijetna.

2 Najeti PenTest tim

Najpogosteje naročnik PenTesta najame zunanjo ekipo, specializirano za izvedbo vdornih testov.

Pri izbiri izvajalca PenTesta organizacija pogosto preverja strokovna znanja potencialnih izvajalcev (različne strokovne certifikate, medijsko prisotnost, strokovne reference in priporočila drugih naročnikov ...), o izbiri izvajalca pa pogosto odločata razpoložljivost izvajalca v izbranem terminu in cena.

Za uspešno izvedbo PenTesta je izjemno pomembno vzpostaviti zaupanje ter odprto komunikacijo med naročnikom, izvajalcem in dobaviteljem/upravljalcem aplikacije/platforme/informacijskega sistema. Glavni izziv najetega PenTesta je omejen čas, ki ga ima izvajalec PenTesta na voljo za izvedbo projekta (in ravno vloženi čas neposredno določa tudi ceno projekta). Naročnik testiranja od izvajalca pravzaprav najame ekipo varnostnih strokovnjakov za zelo omejen čas, v katerem mora ta spoznati delovanje naročnikovega sistema, poiskati ranljivosti, izvesti vdorne teste, ter pripraviti in predstaviti poročilo o testiranju. V praksi to pomeni, da izvajalec porabi za dejansko vdorno testiranje le približno polovico projektnega oziroma plačanega časa in pogosto ne more temeljito preveriti celotne funkcionalnosti ali obsega projekta, torej opravi le "vzorčno testiranje" (v nasprotju z napadalci, ki imajo na voljo neomejen čas). Če je motiv naročnika predvsem pridobitev potrdila o izvedenem PenTestu (ker to zahteva zakonodaja, regulator ali certifikat ...) in ne dejansko izboljšanje varnosti, ali če dobavitelj/upravljalec aplikacije/platforme/informacijskega sistema test doživlja kot napad na svojo integriteto namesto priložnost za izboljšanje, pogosto pride do prikrivanja informacij (»če so strokovnjaki, bodo že ugotovili ...«). Posledično se dejanski čas, ki ga izvajalec nameni ključni dejavnosti testiranja, še zmanjša, s tem pa se zmanjša dodana vrednost celotnega projekta.

Dodatni izziv najetega testiranja je, da se praviloma izvaja le v določenih (predpisanih) časovnih intervalih, na primer enkrat letno, čeprav je vsem jasno, da je v današnjem času popolnoma nerealno pričakovati, da bo naročnikovo okolje ostalo nespremenjeno do naslednjega PenTesta. Tudi če bi bilo okolje naročnika popolnoma statično, se okoli njega vse nenehno spreminja: pojavljajo se nove ranljivosti in novi načini njihove zlorabe.

3 Interni PenTest tim

Naročnik se lahko odloči, da bo za testiranje varnosti aplikacij/platforme/informacijskega sistema vzpostavil lasten interni tim strokovnjakov, kar je pogosta praksa pri organizacijah z visokim varnostnim tveganjem.

Glavna prednost internega tima je možnost njegovega sodelovanja že pri načrtovanju varnostne arhitekture, izbiri in postavitvi varnostnih ukrepov ter pri nadzoru njihovega delovanja, in nenazadnje neposrednem dostopu do informacij naročnika, kot so interni dnevniki dogodkov, funkcijske specifikacije in celo izvorna koda produktov. Dobro poznavanje implementirane tehnologije, varnostnih ukrepov, varnostnih incidentov in morebitnih odprtih ranljivosti omogoča interni ekipi za PenTest hitro, sprotno in učinkovito izvedbo testiranja, ker pa je interni tim del organizacije naročnika, je pogosto lažje vzpostaviti ali celo vsiliti potrebno zaupanje in sodelovanje z drugimi deležniki.

Žal si takšen interni tim strokovnjakov lahko privoščijo le redke organizacije, saj je pridobivanje in vzdrževanje strokovnjakov za kibernetsko varnost zelo zahtevno in povezano z visokimi stroški. Dobri strokovnjaki za vdorno testiranje potrebujejo veliko izkušenj in stalnega izobraževanja, zato se pogosto ozko specializirajo, kar pa v današnjem času, ko so platforme in informacijski sistemi kompleksni, pomeni, da celovito in kakovostno vdorno testiranje lahko pogosto izvede le večja ekipa strokovnjakov različnih profilov, hkrati pa so takšni kadri izjemno iskani, dragi in jih je težko obdržati.

4 CrowdSource PenTesti

CrowdSource platforme že poldrugo desetletje omogočajo organizacijam izvajanje varnostnih pregledov z množico varnostnih raziskovalcev z zelo različnim naborom in ravnjo znanja.

Raznolikost raziskovalcev je hkrati največja prednost in največja pomanjkljivost takšnega testiranja, saj prihaja do velike razlike v kakovosti posameznih poročil in tudi do velikega števila neveljavnih ali zelo splošnih ugotovitev, ki nimajo prave dodane vrednosti.

Praktično vse CrowdSource platforme naročniku ponujajo možnost uporabe njihove triažne storitve in/ali umetne inteligence za pregled in preverjanje poročil, za preverjanje navedb, izločanje neveljavnih poročil ter vsebinsko in oblikovno ureditev veljavnih poročil v profesionalno in uporabno obliko.

CrowdSource platforme naročnikom ponujajo tako postavitev odprtega programa za določen čas kot tudi izvedbo različnih kampanj (na primer pred izidom nove različice) ali celo "časovni najem" strokovnjakov izbranega profila (primerljivo z najetim PenTest timom).

Največja razlika uporabe CrowdSource platforme v primerjavi z najetim/internim timom je način plačila, saj naročnik plača nagrado (Bug Bounty) za prijavljeno ranljivost glede na ugotovljeno tveganje potrjene ranljivosti, pri najetem ali internem timu pa plača pavšalni znesek ne ne glede na rezultat oziroma uspešnost testiranja.

Naročnik sam določa višino nagrad za posamezne kategorije tveganj in obseg programa Bug Bounty (katere domene, naprave, funkcionalnosti in ranljivosti so vključene v program in katere ne).

CrowdSource platforme sicer opravijo določena preverjanja raziskovalcev (KYC), vendar v zelo omejenem obsegu, zato je stopnja zaupanja med naročnikom in raziskovalci minimalna. Če naročnik želi omogočiti njemu »neznanim« raziskovalcem izvajanje varnostnih testiranj, je zelo priporočljivo, da jim omogoči dostop do testnega okolja, ki je verodostojna kopija njegovega produkcijskega okolja.

CrowdSource platforme so tudi okolje, v katerem se kalijo novi varnostni strokovnjaki, nekateri najboljši izvajalci vdornih testov vso kariero delujejo le prek tovrstnih platform, saj zaslužek na teh platformah lahko presega najbolj plačana podobna delovna mesta, sami pa lahko izbirajo, kdaj, koliko in kaj bodo testirali.

5 Avtomatizirani PenTesti

Uporaba avtomatiziranih varnostnih testiranj je zelo pogosta, priročna in cenovno ugodna metoda za iskanje ranljivosti. Na voljo je veliko različnih programov in platform, ki imajo navadno nabor že pripravljenih testov, nekateri pa omogočajo tudi dodajanje novih testov. Naročnik navadno izbere svoj nabor testov in interval ponavljanja, nekatere rešitve pa omogočajo tudi polavtomatizirano testiranje, pri katerem uporabnik ročno uporablja spletno aplikacijo prek preglednega posredniškega strežnika, hkrati pa se izvajajo različni testi na vsaki obiskani spletni strani, aplikacija pa si lahko zapomni vnesene vrednosti in »pot« skozi aplikacijo za naslednje ponovitve.

Enostavnost uporabe in nizka cena so glavne prednosti avtomatiziranega testiranja, ki pa na področju vdornih testov dolgo časa ni bilo primerljivo s testiranjem strokovnjakov, dokler v svet avtomatiziranega vdornega testiranja ni vstopila umetna inteligenca.

Rezultati vdornih testov, vodenih z najnovejšimi modeli umetne inteligence že presegajo najboljše time strokovnjakov, kar ne preseneča, saj lahko UI v kratkem času opravi bistveno več testov in tako odpravi največjo omejitev najetega PenTesta – omejeni čas strokovnjakov.

Čeprav so v tem trenutku nekatere države omejile javni dostop do določenih modelov umetne inteligence, je vsem jasno, da bo ta način testiranja vse bolj priljubljen in dostopen.

6 Hibridni PenTesti

Učinkovita in varna uporaba avtomatiziranih orodij za vdorne teste še vedno zahteva veliko znanja, zato vedno več ponudnikov najetih PenTestov naročnikom omogoča izvajanje določenega nabora testov z umetno inteligenco v kombinaciji z ročnim strokovnim testiranjem. Takšna hibridna kombinacija izvajanja vdornih testov je lahko hitrejša, bolj kakovostna in finančno ugodnejša od uporabe samo avtomatiziranega ali samo najetega testiranja.

7 Naključni PenTesti

Uporabnik neke aplikacije/platforme/informacijskega sistema je lahko hkrati varnostni raziskovalec. Uporabniki pogosto prvi opazijo napake in anomalije pri uporabi aplikacije, vendar bodisi ne razumejo možnih posledic naključno odkrite ranljivosti, bodisi nimajo interesa, da vložijo svoj čas v njeno dokumentiranje in prijavo.

Organizacija seveda ne more spremeniti svojih uporabnikov v varnostne strokovnjake, lahko pa motivira tiste uporabnike, ki potrebna znanja že imajo, da prijavijo zaznane napake.

8 Kateri način vdornega testiranja izbrati?

Odgovor mora poiskati vsaka organizacija zase glede na svojo oceno tveganja in svojo »zrelost«. Priporočljiva je uporaba vseh navedenih načinov, vendar ne vseh hkrati.

Prve vdorne teste je najprimerneje izvesti z najetim timom, saj tak pregled ne zahteva veliko internih virov, naročnik lahko poročilo testiranja posreduje upravljalcu/dobavitelju ranljive opreme, izvajalec testov pa lahko opravi kontrolni pregled učinkovitosti implementiranih korektivnih ukrepov.

Za drugo izvedbo najetih vdornih testov je priporočljivo izbrati drugega izvajalca, saj drugačen pristop k testiranju in drugačen nabor strokovnjakov pogosto zagotovi drugačen »vzorec vdornih testov« in odkrije dodatne ranljivosti.

Po odpravi ranljivosti, ugotovljenih pri prvi in drugi izvedbi vdornih testov, (seveda ob ustrezni kakovosti njihove izvedbe) lahko pričakujemo, da bodo identificirane in odpravljene tiste največje in najbolj očitne ranljivosti, kar je pravi čas za vzpostavitev programa nagrajevanja za varnostne hrošče, ki je osnova za CrowdSource in naključno testiranje.

Evropske digitalne denarnice EUDIW in EBW: od regulative do prakse

Martin Domajnko, Vid Keršič, Muhamed Turkanović

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
martin.domajnko1@um.si, vid.kersic@um.si, muhamed.turkanovic@um.si

V prispevku predstavljamo evropski okvir digitalne identitete s poudarkom na evropski denarnici za digitalno identiteto (EUDI) za fizične osebe in predlagani evropski poslovni denarnici (EBW) za pravne osebe. Osredotočamo se tako na regulativni okvir, vloge udeležencev in model zaupanja, na katerem temeljijo denarnice, kot tudi na tehnično arhitekturo, vključno z digitalnimi poverilnicami, formatoma SD-JWT VC in mdoc ter protokoloma OpenID4VCI in OpenID4VP. Praktično uporabo digitalnih denarnic prikažemo z referenčno implementacijo izdajatelja in preveritelja digitalnih poverilnic ter primerom prijave v spletno storitev z EUDI denarnico. V razpravi primerjamo stopnjo zrelosti obeh okvirov ter obravnavamo možnosti in zahteve za vključevanje organizacij v nastajajoči ekosistem evropskih digitalnih denarnic.

Ključne besede:
digitalna identiteta
digitalna poverilnica
eIDAS 2.0
evropska denarnica za digitalno identiteto
evropska poslovna denarnica

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-299-188-3
DOI https://doi.org/10.18690/um.feri.7.2026.13

1 Uvod

Hitra digitalizacija družbe spreminja način, kako dostopamo do storitev, sklepamo posle ter dokazujemo različne podatke o sebi. Pri uporabi spletnih storitev skoraj vedno uporabljamo neko obliko digitalne identitete, ki je praviloma vezana na posamezno platformo in temelji na uporabniškem računu z uporabniškim imenom in geslom. Del razdrobljenosti zmanjšujejo sistemi enotne prijave (angl. Single Sign-On, SSO), pri katerih se uporabnik z istim računom prijavlja v več storitev, vendar tudi ti, četudi temeljijo na t. i. federativnem modelu digitalne identitete, običajno temeljijo na centraliziranem ponudniku (digitalne identitete) [1]. Hkrati se digitalizirajo različne poverilnice, vstopnice, letalske karte ipd., pri čemer pomemben del teh funkcionalnosti zagotavljajo izolirane aplikacije in lastniške denarnice ponudnikov, kot sta Apple Wallet in Google Wallet [2, 3]. Digitalne identitete in poverilnice zato praviloma niso prenosljive med platformami, njihova uporabnost pa je odvisna od pravil in tehničnih zmožnosti posameznega ponudnika.

Takšna razdrobljenost je posebej problematična v Evropski uniji (EU), kjer poleg nacionalnih sistemov elektronske identifikacije velik del pogosto uporabljenih digitalnih identitet zagotavljajo zasebna tehnološka podjetja, večinoma s sedežem zunaj EU. Posledično ni enotnega načina za uporabo digitalne identitete in izmenjavo digitalnih poverilnic med državami članicami, javnimi organi ter zasebnimi ponudniki storitev [4]. To zmanjšuje tudi čezmejno interoperabilnost, povečuje stroške integracije in ustvarja odvisnost od posameznih tehnoloških ponudnikov, uporabnikom pa otežuje nadzor nad lastnimi podatki. Prvotna uredba eIDAS iz leta 2014 je sicer vzpostavila pravni okvir za elektronsko identifikacijo in storitve zaupanja, vendar ni zagotovila enotne, uporabniško nadzorovane rešitve za hrambo in izmenjavo različnih digitalnih poverilnic [4, 5]. Še manj celovito je bilo urejeno področje digitalne identitete pravnih oseb. Digitalni certifikati, elektronski podpisi in elektronski žigi omogočajo overjanje ter zagotavljanje pristnosti in celovitosti dokumentov, vendar ne predstavljajo celovite poslovne digitalne identitete, ki bi podpirala upravljanje organizacijskih podatkov, vlog, pooblastil in različnih poslovnih poverilnic.

Evropska komisija je zato leta 2021 predlagala prenovo uredbe eIDAS, ki sta jo Evropski parlament in Svet EU leta 2024 sprejela kot Uredbo (EU) 2024/1183 o vzpostavitvi evropskega okvira za digitalno identiteto, pogosto poimenovano eIDAS 2.0 [6]. Eden izmed njenih osrednjih elementov je evropska denarnica za digitalno identiteto (angl. European Digital Identity Wallet, EUDI Wallet, v nadaljevanju: EUDI denarnica), ki naj bi fizičnim osebam omogočila varno prejemanje, hrambo in uporabo identifikacijskih podatkov ter drugih digitalnih poverilnic v javnih in zasebnih storitvah po celotni EU [6, 7, 8]. Države članice morajo zagotoviti najmanj eno EUDI denarnico, vse rešitve pa morajo temeljiti na skupnih standardih, protokolih in modelu zaupanja [6, 9, 10]. Okvir tako ni vezan na enega tehnološkega ponudnika, saj lahko denarnice zagotovijo države članice, pooblaščeni izvajalci ali priznani zasebni ponudniki, njihovo delovanje pa urejajo skupne evropske in nacionalne zahteve [6, 11]. Kot nadgradnjo tega pristopa za pravne osebe je Evropska komisija novembra 2025 predlagala še uredbo o evropskih poslovnih denarnicah (angl. European Business Wallet, EBW), namenjenih digitalizaciji poslovnih interakcij med podjetji in javnimi organi [12]. Ker zakonodajni postopek za EBW še poteka, gre za novejši in manj dokončno opredeljen okvir, ki se bo v nadaljevanju še tehnično in pravno razvijal [13, 14].

V prispevku predstavljamo evropski okvir digitalnih identitet s poudarkom na digitalni denarnici za fizične osebe (EUDI) in predlagani digitalni denarnici za pravne osebe (EBW). Najprej predstavimo njune ključne značilnosti, vloge udeležencev in razlike med osebno ter poslovno uporabo. Nato opišemo tehnično arhitekturo ekosistema, vključno z digitalnimi poverilnicami, podprtimi formati, protokoli ter značilnimi poteki izdajanja in preverjanja. V nadaljevanju predstavimo referenčno implementacijo platforme LutraID, ki organizacijam omogoča vključevanje funkcionalnosti izdajanja in preverjanja digitalnih poverilnic v obstoječe informacijske sisteme. Delovanje prikažemo na primeru prijave v spletno storitev z EUDI denarnico, v razpravi pa obravnavamo možnosti uporabe, omejitve in pripravljenost organizacij na prihajajoči ekosistem evropskih digitalnih denarnic.

2 Evropski okvir digitalnih identitet

V tem poglavju najprej predstavimo razvoj in regulativni okvir digitalne identitete, nato pa ločeno in podrobneje obravnavamo evropsko denarnico za digitalno identiteto (EUDIW) ter evropsko poslovno denarnico (EBW).

2.1. Razvoj in regulativni okvir digitalne identitete

Digitalna identiteta se je v zadnjih desetletjih razvijala skupaj z rastjo spletnih storitev in nastajanjem novih pristopov k upravljanju identitet. Prvi sistemi so bili večinoma centralizirani, pri čemer je vsak ponudnik sam upravljal uporabniške račune in podatke. Takšen model je povzročil veliko število ločenih računov in podatkovnih silosov, koncentracija osebnih podatkov pri posameznih ponudnikih pa je povečala varnostna tveganja ter omejila nadzor uporabnikov nad lastnimi podatki [15]. Federativni modeli so del teh težav naslovili z uporabo iste identitete pri več storitvah, med drugim s standardom OAuth 2.0 in nato OpenID Connect [16]. Vendar so hkrati povečali odvisnost od osrednjega ponudnika identitete, ki predstavlja enotno točko zaupanja in morebitno enotno točko odpovedi [15]. Naslednji korak v razvoju predstavljajo uporabniško nadzorovani modeli, kot je samoupravljana identiteta (angl. self-sovereign identity, SSI), ki temelji na decentraliziranih identifikatorjih in preverljivih poverilnicah [15, 17, 18, 19]. Evropski regulativni okvir in posledično EUDI denarnica povzemata nekatere principe takšnih modelov, vendar temeljita na reguliranem evropskem modelu zaupanja.

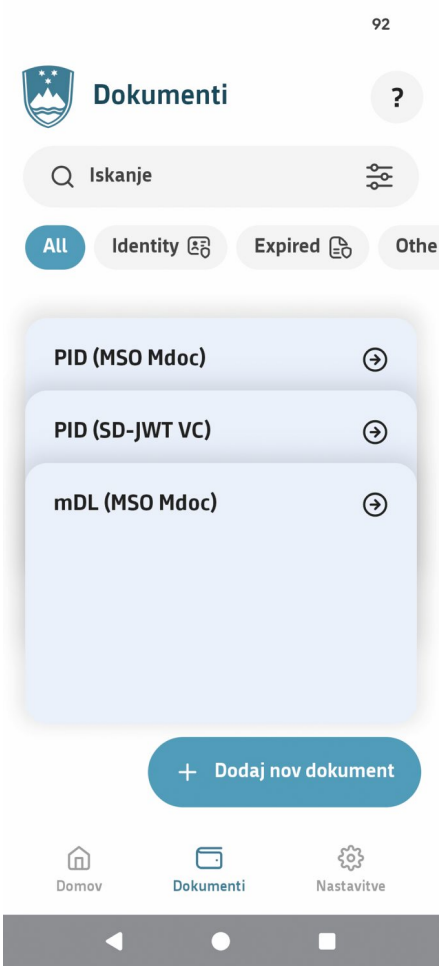
Prvotna uredba eIDAS je omogočila čezmejno priznavanje priglašenih nacionalnih sistemov elektronske identifikacije ter uredila storitve zaupanja, kot so elektronski podpisi, žigi in časovni žigi [5]. Njena uporaba je bila omejena predvsem na javne spletne storitve, prav tako pa ni zagotavljala enotnega načina za izmenjavo dodatnih digitalnih poverilnic [4]. Prenovljeni okvir eIDAS 2.0 zato uvaja EUDI denarnice, osebne identifikacijske podatke in elektronska potrdila atributov ter uporabo digitalne identitete razširja na javni in zasebni sektor [6, 7, 8, 20]. Evropska komisija je novi okvir predlagala leta 2021, Uredba (EU) 2024/1183 pa je bila sprejeta leta 2024 [4, 6, 21]. Države članice morajo do konca leta 2026 zagotoviti najmanj eno EUDI denarnico, ki mora biti interoperabilna z rešitvami drugih držav članic [6, 9]. Ekosistem vključuje države članice, ponudnike denarnic, izdajatelje digitalnih poverilnic, uporabnike, zanašajoče se stranke in tehnične posrednike. Model zaupanja dopolnjujejo ponudniki storitev zaupanja, registri ter organi za certificiranje in nadzor [9, 10, 11, 22].

Evropska komisija je novembra 2025 predlagala še evropske poslovne denarnice, namenjene gospodarskim subjektom, samozaposlenim in javnim organom [12]. Svet EU je junija 2026 sprejel pogajalsko stališče, zakonodajni postopek pa še ni zaključen [13, 14]. Ekosistem poslovnih denarnic vključuje lastnika poslovne denarnice, njene pooblaščene uporabnike, ponudnike denarnic, izdajatelje poverilnic in zanašajoče se stranke. Poleg identitete organizacije mora zato podpirati tudi preverjanje identitete uporabnika, njegove vloge in pooblastila za izvedbo konkretnega dejanja [13].

2.2. EUDIW – digitalna denarnica za fizične osebe

EUDI denarnica je rešitev pod nadzorom uporabnika, namenjena varnemu prejemanju, shranjevanju, upravljanju in uporabi identifikacijskih podatkov osebe (angl. Person Identification Data, PID) ter elektronskih potrdil o atributih (angl. Electronic Attestations of Attributes, EAA), kot so mobilno vozniško dovoljenje, kartica zdravstvenega zavarovanja, poverilnica o izobrazbi ali poverilnica o sklenjenem zavarovanju [6, 7]. Glede na status izdajatelja in pravni režim izdaje so lahko takšna potrdila nekvalificirana EAA, kvalificirana elektronska potrdila o atributih (angl. Qualified Electronic Attestations of Attributes, QEAA), ki jih kot kvalificirano storitev zaupanja izdajajo kvalificirani ponudniki storitev zaupanja, ali elektronska potrdila o atributih javnega sektorja (angl. Public Sector Body Electronic Attestation of Attributes, PuB-EAA). PuB-EAA izda organ javnega sektorja, odgovoren za avtentični vir, torej uradno oziroma pravno priznano primarno evidenco, v kateri se vodijo potrjeni atributi, ali drug organ javnega sektorja, ki ga država članica določi za izdajo takšnih potrdil v njegovem imenu. Vrsta oziroma vsebina potrdila sama po sebi zato še ne določa, ali gre za nekvalificirano EAA, QEAA ali PuB-EAA. Ključne razlike med posameznimi vrstami digitalnih poverilnic povzema tabela 1. Za PID, EAA in sorodne kriptografsko preverljive zapise v nadaljevanju uporabljamo krovni tehnični izraz digitalne poverilnice. Denarnica omogoča

identifikacijo, avtentikacijo, elektronsko podpisovanje in selektivno razkrivanje podatkov [8]. Uporabnik lahko tako pri dokazovanju polnoletnosti razkrije le v poverilnici že vsebovano kriptografsko preverljivo trditev, na primer, da dosega zahtevano starost, ne pa tudi datuma rojstva ali celotnega osebnega dokumenta. Na sliki 1 je prikazan primer, kakšna bi lahko bila videti slovenska evropska denarnica za digitalno identiteto.



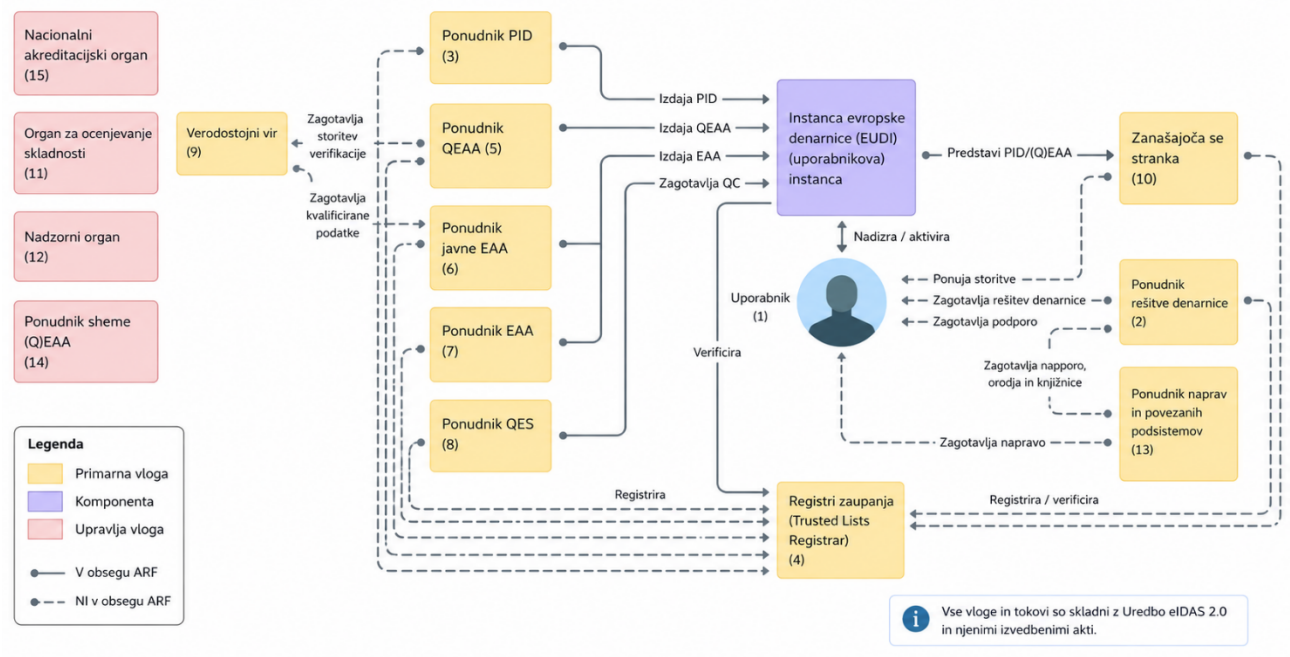
Slika 1: Simbolični prikaz slovenske evropske denarnice za digitalno identiteto. Zajem zaslona [23]

Tabela 1: Vrste digitalnih poverilnic v ekosistemu EUDI denarnice

Vrsta poverilnice	**Izdajatelj**	**Pravni režim**	**Primer**
PID	država članica oziroma pooblaščeni subjekt na podlagi avtentičnega vira	obvezna sestavina EUDI denarnice po eIDAS 2.0	osebni identifikacijski podatki (ime, priimek, datum rojstva)
EAA (nekvalificirano)	katerikoli izdajatelj, tudi zasebni	ni kvalificirana storitev zaupanja	članska izkaznica, digitalna zavarovalna polica
QEAA	kvalificirani ponudnik storitev zaupanja	kvalificirana storitev zaupanja	kartica zdravstvenega zavarovanja
PuB-EAA	organ javnega sektorja, odgovoren za avtentični vir	enakovreden pravni učinek kot QEAA	mobilno vozniško dovoljenje

Osnovni model izmenjave vključuje izdajatelja poverilnic, uporabnika denarnice in **zanašajočo se stranko** (angl. Relying Party) [9]. Vloge posameznih udeležencev in njihove medsebojne povezave so prikazane na sliki 2.

Izdajatelj pripravi in kriptografsko podpiše digitalno poverilnico, uporabnik pa jo hrani pod svojim nadzorom ter odloča o njeni uporabi. Zanašajoča se stranka, na primer banka, mobilni operater ali javni organ, zahteva le podatke, potrebne za izvedbo konkretne storitve. Pri tem je treba razlikovati med zanašajočo se stranko, ki določi namen in obseg obdelave, ter **tehničnim preveriteljem**, ki pripravi zahtevek in preveri izdajatelja, podpis, veljavnost in status poverilnice ter njeno vezavo na uporabnika. Pred uporabo se zanašajoča se stranka registrira pri **pristojnem registracijskem organu** v državi članici svoje ustanovitve ter navede namen uporabe in atribute, ki jih namerava zahtevati. Če preverjanje v njenem imenu izvaja druga entiteta, ta nastopa kot **posrednik** (angl. intermediary) in se kot zanašajoča se stranka registrira v državi članici svoje ustanovitve. Njuno razmerje mora biti dokazano in evidentirano, denarnica pa uporabniku prikaže obe entiteti. Posrednik po posredovanju podatkov ne sme hraniti vsebine transakcije [22]. Zaupanje je organizirano večnivojsko: države članice vzdržujejo nacionalne registre in zaupanja vredne sezname, Evropska komisija pa zagotavlja skupno infrastrukturo za objavo in dostop do seznamov zaupanja vrednih entitet (angl. List of Trusted Entities, LoTE) ter objavlja seznam zaupanja vrednih seznamov EU (angl. List of Trusted Lists, LOTL). V LoTE so objavljena sidra zaupanja za preverjanje izdajateljev poverilnic ter izdajateljev dostopnih in registracijskih certifikatov. Zanašajoče se stranke in posredniki vanje niso vključeni neposredno, temveč se denarnici avtenticirajo z dostopnim certifikatom, njihov registrirani namen in obseg zahtevanih atributov pa se preverita z registracijskim certifikatom ali neposredno v registru. Preverjanje vključuje tudi veljavnost oziroma morebitni preklic (angl. revocation) certifikatov [10].



Slika 2: Vloge in tokovi v ekosistemu evropske denarnice za digitalno identiteto v skladu z Uredbo eIDAS 2.0. [9]

EUDI denarnica ni ena sama evropska aplikacija, temveč skupen ekosistem, zasnovan na enotnih predpisih, arhitekturnem in referenčnem okviru (angl. Architecture and Reference Framework, ARF) ter skupnih standardih in specifikacijah. ARF je skupna tehnična osnova za vloge, model zaupanja, zahteve in interoperabilnost [9]. Države članice morajo do konca leta 2026 zagotoviti najmanj eno EUDI denarnico, rešitev pa lahko zagotovi država neposredno, pooblaščeni izvajalec ali priznani zasebni ponudnik. Pred produkcijsko uporabo morajo biti rešitve certificirane v skladu s skupnimi zahtevami in nacionalnimi certifikacijskimi shemami [6, 11, 24]. Razvoj in integracijsko preizkušanje podpirajo tudi nacionalna testna okolja oziroma peskovniki, med njimi francoski France Identité Playground in nemški EUDI Wallet Sandbox programa SPRIND. Interoperabilnost se preverja tudi v velikih evropskih pilotnih projektih. Skupno šest pilotov je preizkušalo več kot enajst vsakdanjih primerov uporabe, pri čemer je sodelovalo več kot 550 zasebnih podjetij in javnih organov iz 26 držav članic ter Norveške, Islandije in Ukrajine. Med prvimi štirimi piloti je POTENTIAL obravnaval e-upravo, bančništvo, telekomunikacije, mobilna

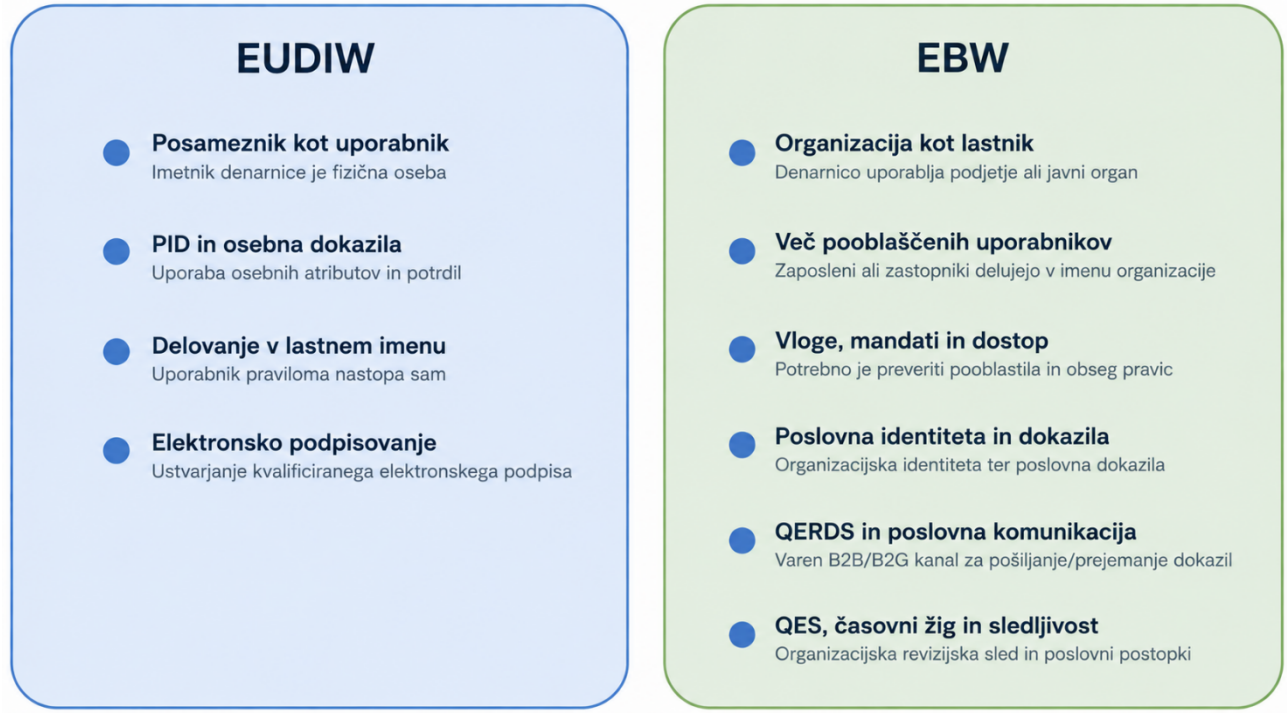
vozniška dovoljenja, elektronsko podpisovanje in zdravstvo. Nadaljnje preizkušanje poteka v projektih APTITUDE in WE BUILD, pri čemer je slednji osredotočen zlasti na poslovne in plačilne scenarije B2B, B2G in B2C [25, 26].

2.3. EBW – poslovna denarnica za pravne osebe

Lastnik EBW je gospodarski subjekt ali organ javnega sektorja, denarnico pa v njegovem imenu uporabljajo pooblaščeni uporabniki oziroma **zastopniki**. To so lahko zakoniti zastopnik, zaposleni, zunanji računovodja ali drug izvajalec, ki mu je lastnik dodelil ustrezne pravice. Ključna razlika v primerjavi z EUDI denarnico je zato podpora več uporabnikom ter upravljanje njihovih vlog in pooblastil [13]. Posameznemu uporabniku je mogoče dovoliti na primer vpogled v dokumente, predložitev poverilnic, ali podpisovanje, njegove pravice pa pozneje omejiti ali preklicati. Vsaka izvedena operacija mora biti sledljivo povezana z organizacijo, uporabnikom in uporabljeno avtorizacijo. Pri tem je treba razlikovati med tehnično avtorizacijo za uporabo funkcij denarnice in pravnim pooblastilom, ki ga lahko za posamezno dejanje zahteva evropska ali nacionalna zakonodaja.

Osrednji element poslovne identitete so **identifikacijski podatki lastnika EBW** (angl. European Business Wallet owner identification data, **EBW-OID**) [13]. Ti podatki morajo vsebovati najmanj uradno ime gospodarskega subjekta oziroma organa javnega sektorja in njegov enolični identifikator. Kadar je gospodarskemu subjektu že dodeljen evropski enolični identifikator (angl. European Unique Identifier, EUID), se kot identifikator uporabi ta. EBW-OID identificira organizacijo, ne pa osebe, ki v njenem imenu izvede dejanje. Preveritelj mora zato pri posamezni poslovni operaciji ločeno preveriti identiteto lastnika denarnice, identiteto uporabnika in njegovo upravičenje za konkretno dejanje.

Ključne razlike med osebno uporabo EUDI denarnice in predlaganim modelom EBW povzema slika 3. Pri EUDI denarnici je imetnik fizična oseba, ki uporablja PID in druge osebne poverilnice, praviloma deluje v svojem imenu ter lahko ustvarja kvalificirane elektronske podpise. Pri EBW je lastnik organizacija, v njenem imenu pa lahko deluje več pooblaščenih uporabnikov. Poslovna denarnica mora zato poleg identitete organizacije podpirati tudi poslovne poverilnice, preverjanje vlog in mandatov, omejevanje dostopa, pravno zanesljivo poslovno komunikacijo ter sledljivost izvedenih dejanj.



Slika 3: Primerjava EUDIW in EBW.

Funkcije, povzete na sliki 3, se v predlaganem modelu povezujejo v celovit poslovni postopek. Predlog med drugim predvideva varno izmenjavo podatkov med EBW, EUDIW in zanašajočimi se strankami ter uporabo elektronskih podpisov, časovnih žigov in kvalificirane storitve elektronske priporočene dostave (angl. Qualified Electronic Registered Delivery Service, QERDS) [13]. Kot konkreten primer uporabe lahko obravnavamo vključitev novega čezmejnega dobavitelja. Njegov pooblaščeni uporabnik bi lahko posredoval EBW-OID, zahtevana dovoljenja ali potrdila in podatke o svojem pooblastilu. Naročnik bi preveril identiteto dobavitelja in upravičenost zastopnika, nato pa bi pooblaščena oseba pogodbo elektronsko podpisala oziroma bi jo organizacija opremila z elektronskim žigom in časovnim žigom. Izmenjava dokumentacije bi lahko prek QERDS potekala tako pri poslovanju med podjetji (angl. business-to-business, B2B) kot pri postopkih med podjetjem in javnim organom (angl. business-to-government, B2G), izvedena dejanja pa bi bila zabeležena v organizacijski revizijski sledi.

Takšne scenarije obravnava tudi evropski pilotni projekt WE BUILD, ki povezuje več kot 200 javnih in zasebnih organizacij iz 28 držav ter preizkuša uporabo evropskih digitalnih denarnic v interakcijah med podjetji (angl. business-to-business, B2B), med podjetji in javnimi organi (angl. business-to-government, B2G) ter med podjetji in potrošniki (angl. business-to-consumer, B2C). Med obravnavanimi primeri uporabe so preverjanje strank (angl. Know Your Customer, KYC), dobaviteljev (angl. Know Your Supplier, KYS) in poslovnih subjektov (angl. Know Your Business, KYB), digitalno zastopanje podjetja, elektronsko izdajanje računov ter poslovna in potrošniška plačila. V projektu sodelujejo javni organi, poslovni registri, banke, ponudniki denarnic, ponudniki storitev zaupanja in velika tehnološka podjetja. Področje plačil vodi Mastercard, posamezne primere uporabe pa med drugim vodita Bundesanzeiger in OpenPeppol, medtem ko Signicat vodi skupino za testiranje. Med vidnejšimi sodelujočimi iz finančnega in tehnološkega sektorja je tudi Visa Europe [26].

3 Arhitektura

Tehnična arhitektura ekosistema ločuje poslovni pomen digitalne poverilnice, njen zapis in kriptografsko zaščito, protokol izmenjave ter konkretni uporabniški tok. Takšna razdelitev je pomembna, ker isti tip poverilnice lahko uporablja več formatov in načinov predložitve, isti protokol pa lahko podpira različne vrste poverilnic. V nadaljevanju zato najprej predstavimo ključne artefakte, nato protokole in nazadnje značilne poteke izdaje ter preverjanja.

3.1. Artefakti

V ekosistemu evropskih denarnic se podatki ne izmenjujejo kot poljubni dokumenti, temveč kot standardizirani in kriptografsko zaščiteni artefakti. Pri tem je koristno ločiti vsebino poverilnice od njenega tehničnega zapisa: PID, mobilno vozniško dovoljenje ali poverilnica o starosti opredeljujejo, kaj dokazujemo, medtem ko SD-JWT VC in mdoc določata, kako so podatki strukturirani, digitalno podpisani, selektivno razkriti in preverjeni.

Med ključnimi tehničnimi formati sta SD-JWT VC in mdoc. Mehanizem SD-JWT za selektivno razkrivanje trditev v JWT je standardiziran v RFC 9901, medtem ko je profil digitalnih poverilnic SD-JWT VC ob pripravi prispevka še aktiven osnutek IETF [27, 28]. Format mdoc uporablja CBOR in COSE ter podpira tudi vezavo poverilnice na napravo. ISO/IEC 18013-5 opredeljuje mobilno vozniško dovoljenje (angl. mobile Driving Licence, mDL), zapisano v formatu mdoc, in njegovo izmenjavo z bralnikom v neposredni bližini. ISO/IEC TS 18013-7 to dopolnjuje s predložitvijo mDL na daljavo prek interneta [29, 30]. SD-JWT VC in mdoc sta torej tehnična formata, mDL pa konkreten tip digitalne poverilnice.

Za posamezne vrste digitalnih poverilnic splošni tehnični format in protokol sama po sebi nista dovolj. Njihovo vsebino in uporabo dodatno opredeljujejo namenska pravila (angl. attestation rulebooks). Ta določajo strukturo in semantiko atributov, sheme ter njihovo preslikavo v podprte tehnične formate, zahteve glede zaupanja in ravni zagotovila ter postopke izdaje, preverjanja in preklica. V trenutni dokumentaciji ARF sta kot samostojna dokumenta navedena pravilnik za PID (PID Rulebook) in pravilnik za mobilno vozniško dovoljenje (mDL

Rulebook). Enotna pravila omogočajo, da izdajatelji, EUDI denarnice in preveritelji v različnih državah isto vrsto poverilnice razumejo in obdelajo na interoperabilen način [9].

Podatki PID so temeljna identifikacijska poverilnica EUDI denarnice. Vsebujejo jedrne podatke iz uradnega oziroma avtentičnega vira, s katerimi je mogoče zanesljivo identificirati fizično osebo. PID se lahko izda v formatu SD-JWT VC ali mdoc, kar omogoča uporabo istega poslovnega nabora podatkov v različnih načinih predložitve [7, 9]. Poslovni ekvivalent PID so identifikacijski podatki lastnika poslovne denarnice oziroma EBW-OID. Gre za preverljiv nabor podatkov o organizaciji, ki se izda kot elektronsko potrdilo atributov v enem od podprtih formatov [13].

Poseben primer namenske poverilnice je evropska rešitev za preverjanje starosti (angl. Age Verification), zasnovana kot prehodna, z EUDI denarnico združljiva rešitev. Uporabniku omogoča, da brez razkritja identitete ali datuma rojstva predloži samo zahtevano informacijo, na primer dokaz, da je starejši od 18 let. Primer ponazarja načelo najmanjšega obsega podatkov: za izvedbo storitve pogosto ni potreben celoten PID, temveč le minimalni preverjeni atribut [31].

3.2. Protokoli

Za izdajo digitalnih poverilnic se uporablja OpenID for Verifiable Credential Issuance (OpenID4VCI), ki določa z OAuth 2.0 zaščiteno komunikacijo med izdajateljem in denarnico [32, 33]. Podpira avtorizacijski kodni tok, pri katerem se uporabnik overi med postopkom izdaje, ter predavtorizirani kodni tok, kadar ga je izdajatelj identificiral že prej. Denarnica pridobi metapodatke izdajatelja in ponudbo poverilnice, nato pridobi dostopni žeton ter z dokazom o posedovanju ustreznega ključa zahteva izdajo.

Predložitev digitalnih poverilnic ureja OpenID for Verifiable Presentations (OpenID4VP) [34]. Preveritelj z jezikom Digital Credentials Query Language (DCQL) opredeli zahtevane vrste poverilnic in atribute, denarnica pa preveri zahtevek ter uporabniku prikaže podatke, ki naj bi jih razkril. Odgovor je vezan na konkretnega preveritelja in sejo, s čimer se zmanjšuje možnost ponovne uporabe prestreženega odgovora v drugem kontekstu.

Pri poverilnicah v formatu mdoc standard ISO/IEC 18013-5 določa predvsem preverjanje ob fizični prisotnosti (angl. proximity verification), pri katerem denarnica in bralnik vzpostavita neposreden, šifriran komunikacijski kanal [29]. ISO/IEC TS 18013-7 opredeljuje oddaljeno predložitev mdoc prek interneta [30]. Profil OpenID4VC High Assurance Interoperability Profile (HAIP) dodatno omeji možnosti OpenID4VCI, OpenID4VP, SD-JWT VC in mdoc na skupen nabor varnih nastavitev, s čimer izboljšuje interoperabilnost implementacij z višjimi zahtevami glede zagotovila [35].

Za EBW končni protokolni profil še ni določen. Predlagani okvir zahteva skupne vmesnike za izdajo, zahtevanje, preverjanje in selektivno predložitev poverilnic ter avtomatizirano komunikacijo med poslovnimi denarnicami in EUDI denarnicami [13]. Iz teh zahtev je mogoče sklepati, da bo smiselna ponovna uporaba dela jedra OpenID4VCI in OpenID4VP, dopolnjenega z organizacijsko identiteto, preverjanjem pooblastil, elektronskimi žigi in komunikacijo med informacijskimi sistemi brez neposrednega sodelovanja uporabnika. Končna rešitev bo odvisna od sprejetega besedila uredbe, izvedbenih aktov in tehničnih specifikacij.

3.3. Tokovi

V nadaljevanju so povzeti štirje značilni poteki uporabe denarnic: (1) izdaja poverilnice, (2) preverjanje na daljavo, (3) preverjanje ob fizični prisotnosti ter (4) poslovna izmenjava s poslovno denarnico.

Postopek izdaje digitalne poverilnice se začne s ponudbo izdajatelja ali zahtevo, ki jo sproži denarnica [32]. Denarnica pridobi metapodatke izdajatelja, uporabnik pa se po potrebi prijavi oziroma vnese predhodno odobreno kodo. Nato denarnica pridobi dostopni žeton in dokaže nadzor nad pripadajočim zasebnim ključem. Izdajatelj pripravi in podpiše poverilnico ter jo posreduje denarnici, uporabnik pa potrdi njeno shranitev.

Pri preverjanju na daljavo ponudnik storitve pripravi zahtevek, ki vključuje namen uporabe in najmanjši potrebni nabor podatkov. Kadar postopek poteka na isti napravi, se zahtevek odpre prek povezave, pri uporabi dveh naprav pa se prikaže kot QR-koda. EUDI denarnica preveri tehnično veljavnost zahtevka in podatke o zanašajoči se stranki [22], uporabniku prikaže zahtevane podatke ter po njegovi potrditvi pripravi odgovor. Preveritelj nato preveri podpis izdajatelja, veljavnost in status poverilnice, svežost odgovora ter vezanost poverilnice na denarnico oziroma imetnika [34].

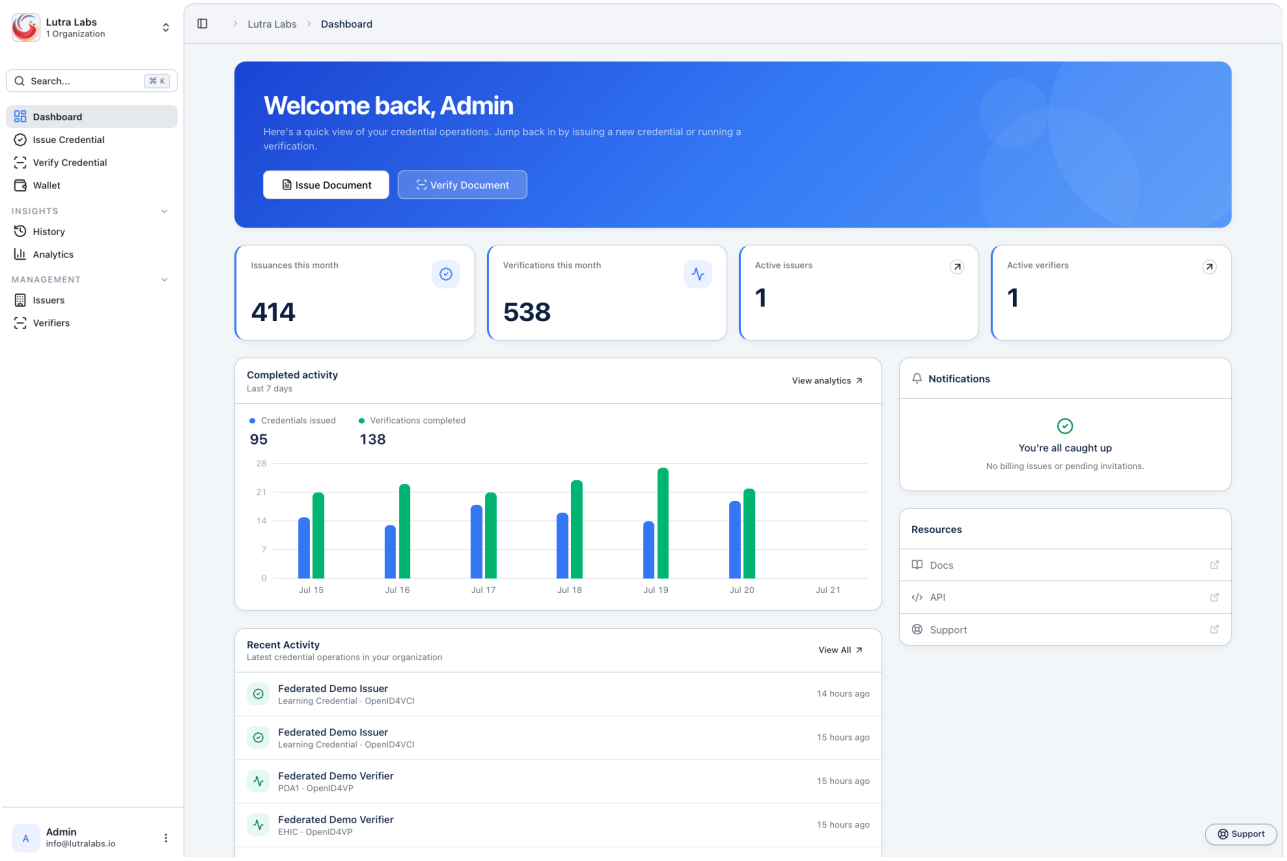
Pri preverjanju ob fizični prisotnosti uporabnika se postopek začne z odčitavanjem QR-kode ali uporabo tehnologije NFC. EUDI denarnica in bralnik nato vzpostavita šifrirano lokalno povezavo, prek katere bralnik zahteva izbrane podatke, uporabnik pa njihovo predložitev potrdi. Osnovno kriptografsko preverjanje je mogoče opraviti brez neposredne povezave z izdajateljem, kar je pomembno predvsem na mestih z omejeno povezljivostjo [29].

Poslovni poteki poleg preverjanja digitalne poverilnice zahtevajo tudi preverjanje identitete organizacije, vloge uporabnika in njegovega upravičenja za konkretno dejanje [13]. Postopek lahko sproži pooblaščena oseba ali zaledni informacijski sistem. Pri vključevanju poslovnega partnerja si poslovni denarnici lahko izmenjata zahtevane podatke o organizaciji in poverilnice o zastopanju. Pri postopkih pred javnimi organi lahko poslovna denarnica posreduje poverilnice in elektronsko vlogo, ki jo pooblaščena oseba po potrebi podpiše oziroma organizacija opremi z elektronskim žigom. Organ lahko po istem varnem kanalu pošlje potrdilo o prejemu, poziv ali odločbo. Če v imenu organizacije nastopa fizična oseba, se njena identiteta lahko dokaže z EUDI denarnico, identiteta organizacije z EBW-OID, upravičenje fizične osebe pa z digitalno poverilnico o organizacijski vlogi, zastopanju ali pooblastilu. Pred samodejno izmenjavo med poslovnima denarnicama je treba preveriti politiko dostopa, identiteto druge organizacije ter veljavnost elektronskega žiga oziroma podpisa. Rutinske izmenjave, na primer elektronskih računov ali podatkov v oskrbovalni verigi, lahko sproži zaledni sistem. Pri občutljivejših dejanjih se lahko zahteva dodatna potrditev pooblaščene osebe. Pomembni koraki se zabeležijo v revizijski sledi [13, 26].

4 Od okvira k praksi: vključevanje organizacij in referenčna implementacija

Organizacije se lahko v ekosistem EUDI denarnice vključijo na več načinov. Nastopajo lahko kot izdajatelji digitalnih poverilnic, na primer licenc, dovoljenj, članstev, poslovnih atributov ali rezultatov preverjanj strank (KYC) in poslovnih subjektov (KYB); kot zanašajoče se stranke, ki za izvedbo storitve zahtevajo preverjene podatke; ali kot ponudniki podpornih platform in infrastrukture [9]. Posamezna organizacija lahko hkrati združuje več vlog, vendar mora za vsako jasno določiti pravni namen, zahtevane podatke, model zaupanja in odgovornosti [22].

Za praktični prikaz predstavljenih konceptov bomo predstavili platformo LutraID, katere uporabniški vmesnik je prikazan na sliki 4. Gre za strežniško rešitev, ki organizacijam omogoča, da izdajanje in preverjanje digitalnih poverilnic vključijo v svoje informacijske sisteme, ne da bi morale v vsaki poslovni aplikaciji znova implementirati protokolne tokove, kriptografske operacije in upravljanje profilov. Platforma ponuja spletni upravljalni vmesnik za nastavitev organizacije, izdajateljev in preveriteljev, vrst poverilnic ter profilov izdajanja in preverjanja. Izdajo in preverjanje je mogoče sprožiti neposredno prek uporabniškega vmesnika ali iz obstoječega sistema prek programskega vmesnika REST. Na ravni organizacije je podprto tudi upravljanje članov in njihovih vlog. Skrbnik organizacije ima dostop do vseh nastavitev, operaterske vloge pa uporabniški vmesnik omejijo na ključna vsakodnevna opravila, kot sta izdajanje in preverjanje digitalnih poverilnic.

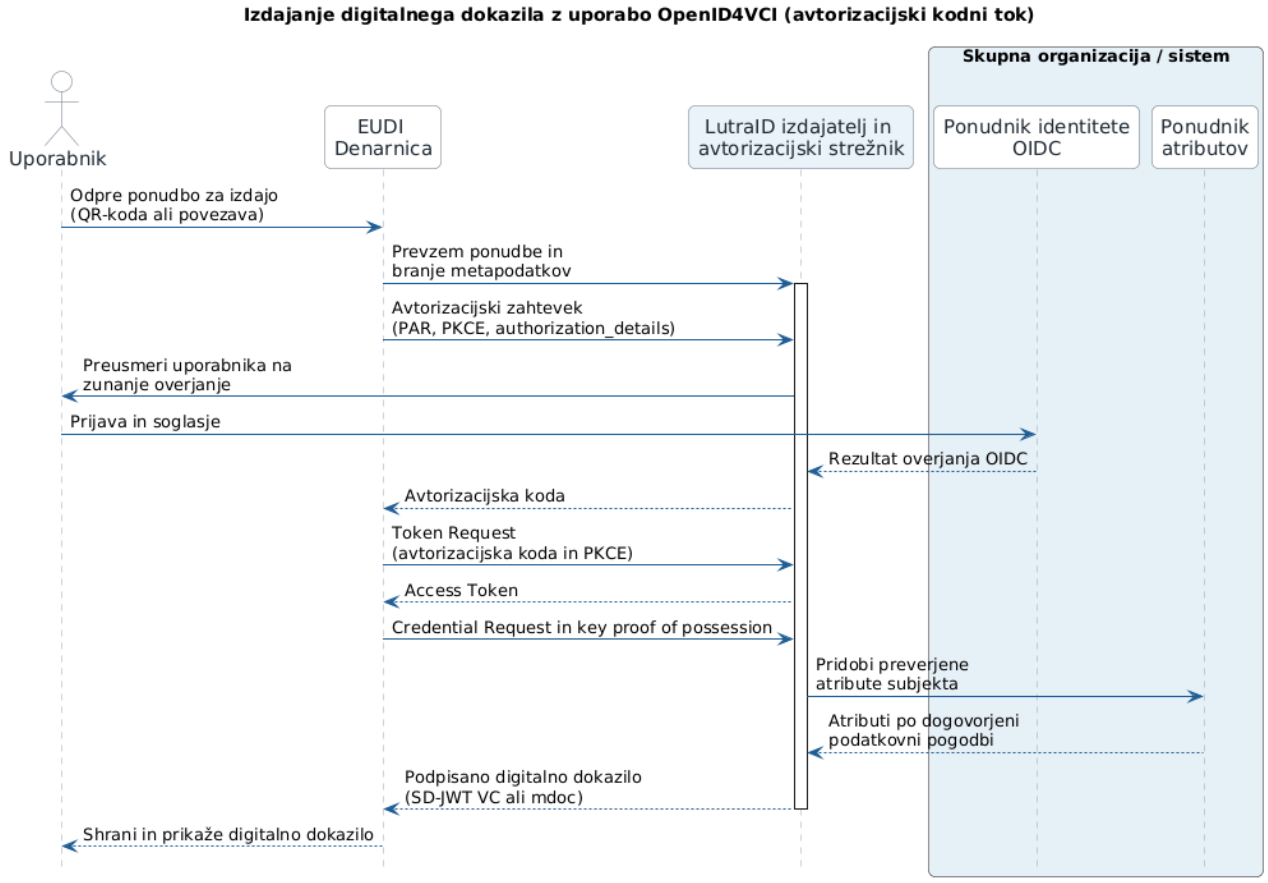


Slika 4: Uporabniški vmesnik platforme LutraID

Platforma je zasnovana kot domensko organiziran modularni monolit, dopolnjen z ločenimi storitvami za obdelavo opravil v ozadju. Funkcionalna področja so ločena na ravni izvorne kode, zaledna aplikacija pa se namešča in izvaja kot celota ter uporablja skupno podatkovno bazo. Takšna zasnova poenostavlja razvoj in upravljanje, hkrati pa omogoča poznejšo izločitev posameznih modulov v samostojne storitve. Uporabniški vmesnik temelji na ogrodju Next.js, zaledni del pa na ogrodju Hono. Za avtentikacijo in upravljanje uporabnikov se uporablja Better Auth, podpora za enotno prijavo (SSO) in protokol System for Cross-domain Identity Management (SCIM) pa organizacijam omogoča povezavo z obstoječimi sistemi za upravljanje identitet in dostopov. Kriptografske operacije se lahko izvajajo prek storitve AWS KMS, pri čemer zasebni ključi ostanejo zaščiteni v strojnem varnostnem modulu (angl. Hardware Security Module, HSM). Za varno hrambo in upravljanje aplikacijskih skrivnosti se uporablja HashiCorp Vault.

Pred izdajo skrbnik organizacije ustvari izdajatelja in mu dodeli ustrezen profil izdajanja. Uporabi lahko enega od vnaprej pripravljenih profilov, na primer za PID ali mobilno vozniško dovoljenje (mDL), oziroma pripravi lasten profil za drugo vrsto poverilnice. Operater nato izbere profil, vnese podatke prejemnika in sproži postopek, platforma pa pripravi ponudbo za prevzem v obliki povezave ali QR-kode. Potek izdaje digitalne poverilnice v platformi LutraID je prikazan na sliki 5. Uporabnik ponudbo odpre v EUDI denarnici, ki nato pridobi njeno vsebino in metapodatke izdajatelja ter začne avtorizacijski kodni tok. LutraID uporabnika preusmeri k zunanjemu ponudniku identitete OIDC (angl. OpenID Connect), kjer se uporabnik overi in po potrebi poda soglasje. Po uspešnem overjanju denarnica prejme avtorizacijsko kodo, jo skupaj z dokazom PKCE (angl. Proof Key for Code Exchange) zamenja za dostopni žeton ter pošlje zahtevo za izdajo z dokazom o posedovanju pripadajočega zasebnega ključa. LutraID od ponudnika atributov pridobi preverjene podatke o prejemniku, pripravi in kriptografsko podpiše digitalno poverilnico v formatu SD-JWT VC ali mdoc ter jo posreduje denarnici. Denarnica poverilnico shrani in jo prikaže uporabniku. V uporabniškem vmesniku je mogoče spremljati trenutno stanje postopka in pregledati zgodovino izvedenih korakov. Enak postopek je mogoče sprožiti prek programskega

vmesnika REST, kar omogoča, da podatke o prejemniku zagotovi obstoječi poslovni sistem, LutraID pa izvede protokolni in kriptografski del izdaje.



Slika 5: Izdajanje digitalne poverilnice v platformi LutraID prek OpenID4VCI z avtorizacijskim kodnim tokom

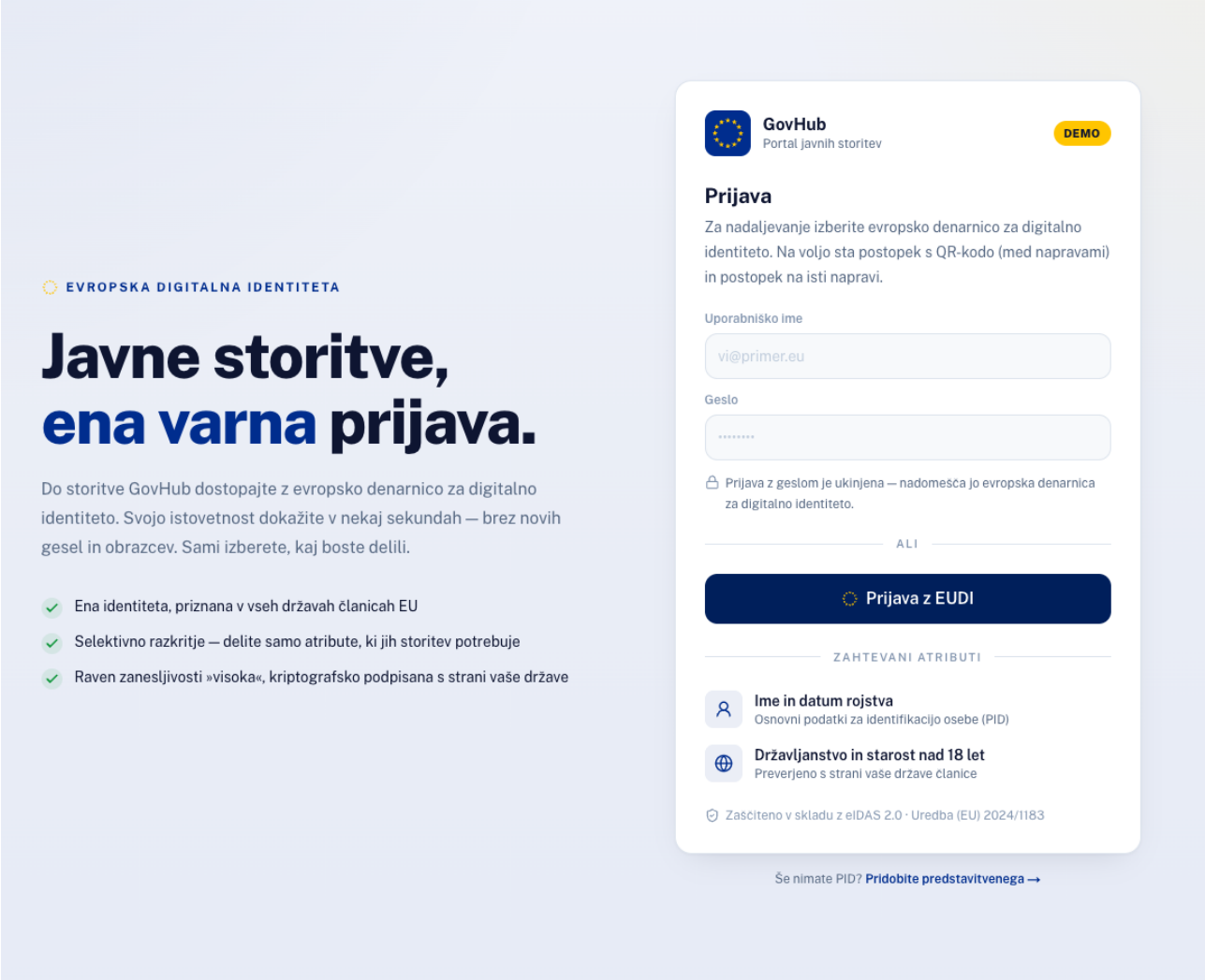
Pri preverjanju skrbnik pripravi profil preverjanja in določi zahtevane vrste poverilnic ter atribute. Operater nato sproži zahtevo, ki jo uporabnik odpre v EUDI denarnici in potrdi. Po uspešnem preverjanju platforma prikaže strukturiran rezultat ali ga prek programskega vmesnika posreduje povezanemu poslovnemu sistemu. Poslovna aplikacija tako prejme le rezultat preverjanja in dovoljene podatke, ne pa nujno celotne digitalne poverilnice.

Isto arhitekturo je mogoče v prihodnje razširiti za podporo poslovnim denarnicam, predvsem z upravljanjem organizacijskih identitet, več uporabnikov, zastopnikov, vlog in pooblastil, elektronskih žigov ter komunikacije med denarnicami in zalednimi informacijskimi sistemi. Jedro za izdajanje, preverjanje in povezovanje s poslovnimi sistemi lahko pri tem v veliki meri ostane nespremenjeno, dopolniti pa ga bo treba z zahtevami, ki bodo določene v končnem pravnem in tehničnem okviru [13].

Čeprav se standardi še razvijajo, se lahko organizacije na uvedbo pripravijo že zdaj. Smiselno je popisati postopke, v katerih danes ročno zbirajo ali preverjajo identifikacijske podatke, določiti, ali bodo nastopale kot izdajatelj ali zanašajoča se stranka, ter opredeliti najmanjši potreben nabor atributov, pravne podlage, vire zaupanja, upravljanje ključev in certifikatov, zahteve revizijske sledi ter integracijske točke. Takšna priprava ostane uporabna tudi ob poznejših spremembah posameznih protokolnih profilov.

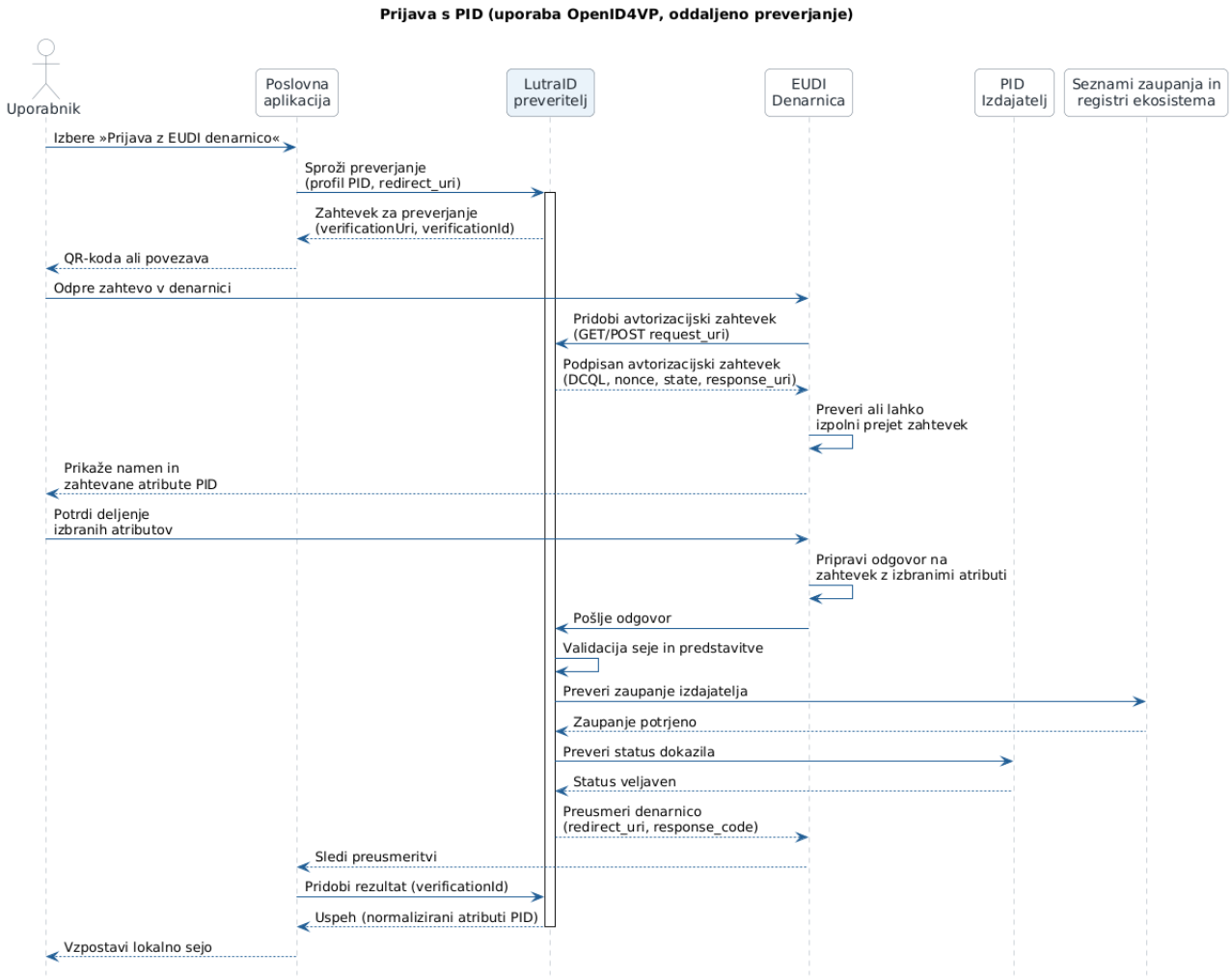
5 Primer uporabe: prijava z EUDI denarnico

Kot osnovni primer uporabe obravnavamo prijavo v spletno storitev s preverjanjem PID, katere začetni korak je prikazan na sliki 6. Namesto uporabniškega imena, gesla in ročnega prepisovanja podatkov ponudnik storitve uporabniku ponudi možnost »Prijava z EUDI denarnico«. V tem postopku poslovna aplikacija nastopa kot *zanašajoča se stranka*, LutraID pa kot *tehnični preveritelj*, ki v njenem imenu pripravi zahtevo OpenID4VP in preveri prejeti odgovor.



Slika 6: Uporabniški vmesnik spletne storitve z možnostjo prijave z EUDI denarnico.

Potek prijave s PID je prikazan na sliki 7. Ko uporabnik izbere prijavo z EUDI denarnico, poslovna aplikacija v platformi LutraID sproži preverjanje z izbranim profilom PID. LutraID pripravi identifikator postopka in zahtevek za preverjanje, ki ga poslovna aplikacija uporabniku prikaže kot povezavo ali QR-kodo. EUDI denarnica nato pridobi podpisani avtorizacijski zahtevek, ki vsebuje zahtevane atribute, namen uporabe ter vrednosti za vezavo odgovora na konkretnega preveritelja in sejo. Denarnica preveri, ali lahko zahtevo izpolni, uporabniku prikaže podatke o zanašajoči se stranki, namen in zahtevane atribute ter po njegovi potrditvi pripravi in pošlje odgovor. LutraID preveri veljavnost seje in prejete predstavitve, zaupanje v izdajatelja, kriptografske podpise, status poverilnice ter njeno vezavo na denarnico oziroma imetnika. Po uspešni validaciji denarnico preusmeri nazaj v poslovno aplikacijo, ta pa z identifikatorjem postopka pridobi strukturiran rezultat in normalizirane atribute PID. Poslovna aplikacija nato vzpostavi lokalno uporabniško sejo ali prejete podatke uporabi za povezavo z obstoječim računom.



Slika 7: Prijava s PID prek OpenID4VP pri oddaljenem preverjanju v platformi LutraID

Enak način preverjanja je mogoče uporabiti tudi pri zahtevnejših postopkih, v katerih mora ponudnik storitve pridobiti več preverjenih podatkov ali povezati podatke iz več digitalnih poverilnic. Pri odpiranju bančnega računa lahko banka od uporabnika zahteva PID ter po potrebi dodatne poverilnice o naslovu prebivališča, davčnem rezidentstvu ali drugih podatkih, potrebnih za izvedbo postopka KYC. Pri registraciji eSIM mobilni operater s PID preveri identiteto uporabnika in druge zakonsko zahtevane atribute, preverjene podatke pa lahko neposredno uporabi v postopku sklenitve pogodbe in aktivacije storitve [25]. Pri najemu vozila ponudnik zahteva kombinirano predstavitev PID in mDL, na podlagi katere preveri identiteto uporabnika, veljavnost vozniškega dovoljenja in ustrezno kategorijo vozila [29]. Uporabnik pri tem razkrije samo podatke, potrebne za posamezno storitev. Postopek se lahko izvede na daljavo pred aktivacijo storitve oziroma prevzemom vozila ali neposredno na poslovalnici oziroma mestu prevzema [30].

6 Razprava in sklep

V prispevku smo predstavili evropsko denarnico za digitalno identiteto in evropsko poslovno denarnico. EUDI denarnica je namenjena predvsem fizičnim osebam ter jim omogoča hrambo in uporabo osebnih identifikacijskih podatkov in drugih digitalnih poverilnic. EBW je namenjena pravnim osebam, samozaposlenim in javnim organom, pri čemer denarnico v imenu organizacije uporabljajo pooblaščeni uporabniki oziroma zastopniki. Obe rešitvi sledita cilju vzpostavitve interoperabilnega evropskega ekosistema za varno čezmejno identifikacijo in izmenjavo preverjenih podatkov. Opisali smo njune vloge, tehnično arhitekturo, uporabljene formate in protokole

ter postopke izdajanja in preverjanja digitalnih poverilnic, praktično uporabo pa smo prikazali z referenčno implementacijo platforme LutraID in primerom prijave v spletno storitev z EUDI denarnico.

Okvir EUDI denarnic je že precej zrel, saj so pravne zahteve, vloge udeležencev, tehnična arhitektura ter osnovni tokovi izdajanja in preverjanja v večini opredeljeni v izvedbenih uredbah, specifikaciji ARF in specifikacijah OpenID4VC. Prvi val velikih evropskih pilotnih projektov, ki je potekal do leta 2025, je rešitve preizkušal na področjih elektronske uprave, bančništva, telekomunikacij, mobilnih vozniških dovoljenj, elektronskega podpisovanja, zdravstva, izobraževanja in plačil [25]. Države članice morajo najmanj eno EUDI denarnico zagotoviti do konca leta 2026, zato se okvir in njegova uporaba že približujeta širši produkcijski uvedbi [6, 24].

Po drugi strani je stopnja zrelosti EBW nižja, saj je Evropska komisija predlog uredbe predstavila novembra 2025, Svet EU pa je svoje pogajalsko stališče sprejel junija 2026 [12, 14]. Končno besedilo uredbe v času priprave prispevka še ni sprejeto, države članice pa si prizadevajo doseči končni dogovor do konca leta 2026 [14]. Po sprejetju bo treba podrobneje opredeliti izvedbene akte, tehnično arhitekturo, protokole, formate in model zaupanja za poslovne denarnice. Pomembno vlogo ima projekt WE BUILD, ki se je začel septembra 2025 in bo predvidoma potekal 24 mesecev, do leta 2027 [26]. Projekt razvija in preizkuša primere uporabe na področjih poslovanja, dobavnih verig in plačil, vključno z identifikacijo organizacij, pravnim zastopanjem in izmenjavo podatkov. Njegovi rezultati lahko tako prispevajo k nadaljnjemu oblikovanju tehničnih zahtev in praktični uvedbi EBW ekosistema.

V prihodnje bo zanimivo spremljati nadaljnji razvoj EUDI denarnic, zlasti vključevanje dokazov brez razkritja znanja (angl. zero-knowledge proofs, ZKP), ki omogočajo dokazovanje trditev o podatkih brez razkritja njihovih dejanskih vrednosti ter s tem zagotavljajo večjo zasebnost uporabnikov. Od začetka leta 2027 bo pomembno tudi, kako hitro se bodo EUDI denarnice uveljavile v praksi in kakšna bo njihova razširjenost med državami članicami, ponudniki storitev in uporabniki. Pri EBW bo nadaljnji razvoj odvisen predvsem od sprejetja končne uredbe, izvedbenih aktov in tehničnih specifikacij ter rezultatov projekta WE BUILD. Pomembno bo tudi spremljati dejansko uvedbo poslovnih denarnic v državah članicah in možnosti njihove interoperabilnosti s primerljivimi rešitvami zunaj EU.

Literatura

[1] F. Alaca in P. C. van Oorschot, »Comparative Analysis and Framework Evaluating Web Single Sign-on Systems«, ACM Computing Surveys, let. 53, št. 5, čl. 112, str. 1–34, 2020. https://doi.org/10.1145/3409452

[2] Apple, »Security of IDs in Apple Wallet«, Apple Platform Security, 7. 5. 2024, obiskano 21. 7. 2026. https://support.apple.com/guide/security/security-of-ids-in-apple-wallet-secb569bf393/web

[3] Google, »Identity«, Google Wallet, obiskano 21. 7. 2026. https://developers.google.com/wallet/identity

[4] Evropska komisija, »SWD(2021) 124 final: Impact Assessment Report accompanying the Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity«, 3. 6. 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124

[5] Evropski parlament in Svet Evropske unije, »Uredba (EU) št. 910/2014 z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu ter razveljavitvi Direktive 1999/93/ES«, 2014. https://eur-lex.europa.eu/eli/reg/2014/910/oj

[6] Evropski parlament in Svet Evropske unije, »Uredba (EU) 2024/1183 z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto«, 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[7] Evropska komisija, »Izvedbena uredba Komisije (EU) 2024/2977 glede osebnih identifikacijskih podatkov in elektronskih potrdil atributov«, 2024. https://eur-lex.europa.eu/eli/reg_impl/2024/2977/oj

[8] Evropska komisija, »Izvedbena uredba Komisije (EU) 2024/2979 glede celovitosti in jedrnih funkcionalnosti evropskih denarnic za digitalno identiteto«, 2024. https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj

[9] European Digital Identity Cooperation Group, »European Digital Identity Wallet - Architecture and Reference Framework«, različica 2.9.0, 21. 5. 2026. https://eudi.dev/latest/

[10] Evropska komisija, »Izvedbena uredba Komisije (EU) 2024/2982 glede protokolov in vmesnikov evropskega okvira za digitalno identiteto«, 2024. https://eur-lex.europa.eu/eli/reg_impl/2024/2982/oj

[11] Evropska komisija, »Izvedbena uredba Komisije (EU) 2024/2981 glede certificiranja evropskih denarnic za digitalno identiteto«, 2024. https://eur-lex.europa.eu/eli/reg_impl/2024/2981/oj

[12] Evropska komisija, »COM(2025) 838 final: Proposal for a Regulation on the establishment of European Business Wallets«, 19. 11. 2025. https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:52025PC0838

[13] Svet Evropske unije, »Proposal for a Regulation on the establishment of European Business Wallets - General approach«, dokument ST 7659/26, 22. 5. 2026. https://data.consilium.europa.eu/doc/document/ST-7659-2026-INIT/en/pdf

[14] Svet Evropske unije, »Evropske poslovne denarnice: Svet sprejel pogajalsko stališče«, 9. 6. 2026. https://www.consilium.europa.eu/sl/press/press-releases/2026/06/09/european-business-wallets-council-adopts-negotiating-position/

[15] R. Soltani, U. T. Nguyen in A. An, »A Survey of Self-Sovereign Identity Ecosystem«, Security and Communication Networks, let. 2021, čl. 8873429, 26 str., 2021. https://doi.org/10.1155/2021/8873429

[16] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros in C. Mortimore, »OpenID Connect Core 1.0 incorporating errata set 2«, OpenID Foundation, 15. 12. 2023. https://openid.net/specs/openid-connect-core-1_0.html

[17] A. Preukschat in D. Reed, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials, Manning, 2021. https://www.manning.com/books/self-sovereign-identity

[18] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović in M. Turkanović, »Towards the Classification of Self-Sovereign Identity Properties«, IEEE Access, let. 10, str. 88306–88329, 2022. https://doi.org/10.1109/ACCESS.2022.3199414

[19] Š. Čučko in M. Turkanović, »Decentralized and Self-Sovereign Identity: Systematic Mapping Study«, IEEE Access, let. 9, str. 139009–139027, 2021. https://doi.org/10.1109/ACCESS.2021.3117588

[20] Š. Čučko in M. Turkanović, »Umestitev digitalnih (EU) denarnic v ekosistem sodobnih IKT rešitev«, v OTS 2022: sodobne informacijske tehnologije in storitve: zbornik petindvajsete konference, Maribor, Univerza v Mariboru, Univerzitetna založba, 2022, str. 24–41. https://dk.um.si/IzpisGradiva.php?id=82880

[21] M. Turkanović, »Tehnično ozadje digitalnih denarnic in verig blokov v okvirju evropske digitalne identitete in posodobljene Uredbe eIDAS«, predstavitev na 5. mednarodni konferenci o e-identifikaciji in e-storitvah zaupanja, Zeides 2021, 21. 10. 2021.

[22] Evropska komisija, »Izvedbena uredba Komisije (EU) 2025/848 glede informacij za registracijo zanašajočih se strank pri EUDI denarnicah«, 2025. https://eur-lex.europa.eu/eli/reg_impl/2025/848/oj

[23] M. Huš, »Prihaja evropska digitalna denarnica«, Monitor, 30. 12. 2025. https://www.monitor.si/clanek/prihaja-evropska-digitalna-denarnica/245727/

[24] Evropska komisija, »European Digital Identity (EUDI) Regulation«, posodobljeno 22. 6. 2026, obiskano 21. 7. 2026. https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

[25] Evropska komisija, »What are the Large Scale Pilot Projects«, posodobljeno 27. 11. 2025, obiskano 21. 7. 2026. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects

[26] WE BUILD Consortium, »Wallet Ecosystem for Business and payments Use cases on Identification, Legal representation and Data sharing«, obiskano 21. 7. 2026. https://www.webuildconsortium.eu/

[27] D. Fett, K. Yasuda in B. Campbell, »RFC 9901: Selective Disclosure for JSON Web Tokens«, IETF, november 2025. https://www.rfc-editor.org/rfc/rfc9901.html

[28] O. Terbu, D. Fett in B. Campbell, »SD-JWT-based Verifiable Digital Credentials (SD-JWT VC)«, draft-ietf-oauth-sd-jwt-vc-17, IETF, 6. 7. 2026. https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/

[29] ISO, »ISO/IEC 18013-5:2021 - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence application«, 2021. https://www.iso.org/standard/69084.html

[30] ISO, »ISO/IEC TS 18013-7:2025 - Personal identification - ISO-compliant driving licence - Part 7: Mobile driving licence add-on functions«, 2025. https://www.iso.org/standard/91154.html

[31] Evropska komisija, »The EU approach to age verification«, obiskano 21. 7. 2026. https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification

[32] OpenID Foundation, »OpenID for Verifiable Credential Issuance 1.0«, 16. 9. 2025. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[33] M. Domajnko, V. Keršič in M. Turkanović, »OID4VC: izdajanje in deljenje preverljivih poverilnic na osnovi OpenID Connect«, v OTS 2023: sodobne informacijske tehnologije in storitve: zbornik 26. konference, Maribor, Univerza v Mariboru, Univerzitetna založba, 2023, str. 149–163. https://press.um.si/index.php/ump/catalog/book/804

[34] OpenID Foundation, »OpenID for Verifiable Presentations 1.0«, 9. 7. 2025. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[35] OpenID Foundation, »OpenID4VC High Assurance Interoperability Profile 1.0«, končna specifikacija, 24. 12. 2025. https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-final.html