Umestitev digitalnih (EU) denarnic v ekosistem sodobnih IKT rešitev

Špela Čučko, Muhamed Turkanović

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
spela.cucko@um.si, muhamed.turkanovic@um.si

Sinopsis Evropska komisija je junija 2021 predlagala novo uredbo eIDAS 2.0, s katero si prizadeva zagotoviti zaupanja vredno, varno in široko uporabno evropsko digitalno identiteto, ki bo vsem Evropejcem omogočila digitalno dokazovanje svoje identitete z namenom dostopanja do digitalnih storitev po vsej Evropski uniji. V okviru uredbe je izdala zahtevo, da morajo države članice EU do leta 2023 svojim državljanom ponuditi kriptografsko varno digitalno denarnico z EU digitalno identiteto, ki naj bi poleg identifikacije, overjanja, avtorizacije in dostopanja do javnih in / ali zasebnih storitev, omogočala tudi varno shranjevanje, upravljanje in deljenje identitetnih podatkov in poverilnic. Kljub prizadevanju za vpeljavo takšne denarnice obstaja še vedno veliko nejasnosti in odprtih vprašanj glede tehničnih podrobnosti. Poleg tega pa se mnogim postavljajo vprašanja o tem, kaj pravzaprav so digitalne denarnice, komu so namenjene, kakšne scenarije uporabe podpirajo ter kako bodo podpirale digitalne procese in z njimi povezano digitalno preobrazbo v trenutnem, širšem ekosistemu IKT rešitev in storitev. V prispevku bomo tako predstavili tehnično ozadje denarnic digitalnih identitet v okviru Evropske digitalne identitete in posodobljene Uredbe eIDAS. Opredelili bomo osnovne koncepte in tipe denarnic, opisali njihove funkcionalne zahteve, predstavili številne scenarije uporabe ter raziskali interakcije denarnic z obstoječimi IKT rešitvami ob upoštevanju standardov in dobrih praks na področju upravljanja identitet.

Ključne besede:
digitalna identiteta
digitalne denarnice
Evropska komisija
digitalizacija
interoperabilnost
preverljive poverilnice
samoupravljana identiteta

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-639-6
DOI https://doi.org/10.18690/um.feri.10.2022.3

1 Uvod

Po enoletnem posvetovanju z državami članicami, je junija 2021 Evropska komisija izdala obsežno poročilo o analizi Uredbe eIDAS (storitev elektronske identifikacije in zaupanja), kjer je hkrati naznanila korak naprej k eIDAS 2.0 oz. prenovi in modernizaciji v smeri t. i. ogrodja Evropske digitalne identitete. Posebej velja izpostaviti, da eIDAS 2.0 predvideva zasnovo in nastajanje t. i. digitalnih EU denarnic za upravljanje z dokumenti. Sklenjen je bil tudi akcijski načrt, ki veleva, da morajo do septembra 2023 vse države članice EU svojim državljanom ponuditi digitalno denarnico z EU digitalno identiteto, kar prinaša mnogo prednosti, kot so digitalizacija javnih procesov tudi na nivoju EU, nadzor nad deljenjem lastnih podatkov, preprostejše dokazovanje (digitalne) identitete itn. Pri čemer se postavlja vprašanje o tem, kaj točno so digitalne denarnice oz., kdo, kako in zakaj bi jih uporabljal, kakšne so njihove tehnične podrobnosti ter kako bodo omogočale omenjene prednosti v trenutnem, širšem ekosistemu IKT rešitev in storitev.

V prispevku bomo predstavili tehnično ozadje digitalnih denarnic v okviru Evropske digitalne identitete in posodobljene Uredbe eIDAS. Začeli bomo s predstavitvijo osnovnih konceptov in tipov digitalnih denarnic, s pogledom na funkcionalnosti, ki naj bi jih omogočale (digitalno podpisovanje, overjanje na osnovi QR oznak, selektivno vendar preverljivo deljenje informacij itn.). Poznamo številne tipe digitalnih denarnic, od oblačnih do denarnic, ki temeljijo na konceptu samoupravljanih in decentraliziranih identitet (angl. Self-Sovereign Identity - SSI). Zaradi fokusa na digitalno identiteto morajo digitalne denarnice podpirati upravljanje in nadzorovanje le teh, pri čemer morejo omogočati varno shranjevanje in upravljanje identifikatorjev, zasebnih ključev, podatkov in poverilnic, ki naj bi bile zaščitene in popolnoma pod nadzorom uporabnika. Poleg omenjenega pa naj bi omogočale tudi shranjevanje in upravljanje digitalnih dokumentov (kot so npr. osebna izkaznica, diploma, bančna kartica, vozniško dovoljene, certifikat cepljenja), ki so povezani z digitalnimi identitetami. Dokumenti bodo shranjeni v obliki t. i. preverljivih poverilnic (angl. Verifiable Credentials - VC), ki omogočajo preprost nadzor, preverjanje in selektivno razkritje informacij.

V prispevku bomo predstavili tudi številne scenarije uporabe, ki bodo razsvetlili prihodnje načine digitalnih procesov in s tem povezane digitalne preobrazbe. Prav tako bomo predstavili nujnost posodobitve trenutnih IKT rešitev in storitev z namenom doseganja kompatibilnosti z novimi pristopi (overjanja, avtorizacije, komunikacije, izmenjave dokumentov). Pri tem se bomo sklicevali na obstoječe in nove standarde (DID in VC – W3C) in predloge le teh ter določene nove dobre prakse.

2 Digitalne identitete

Digitalna identiteta predstavlja ključen element digitalnih interakcij. Predstavlja sredstvo za identifikacijo, overjanje in avtorizacijo ter omogoča dostopanje do spletnih storitev. Poznamo različne modele upravljanja identitet (angl. Identity Management - IdM), pri čemer večina vključuje tri entitete, in sicer *uporabnika* oz. imetnika identitete, *ponudnika identitete* (angl. Identity Provider - IdP) oz. ponudnika/izdajatelja identitetnih atributov in *ponudnika storitev* (angl. Service Provider - SP) oz. preveritelja (Slika 1).

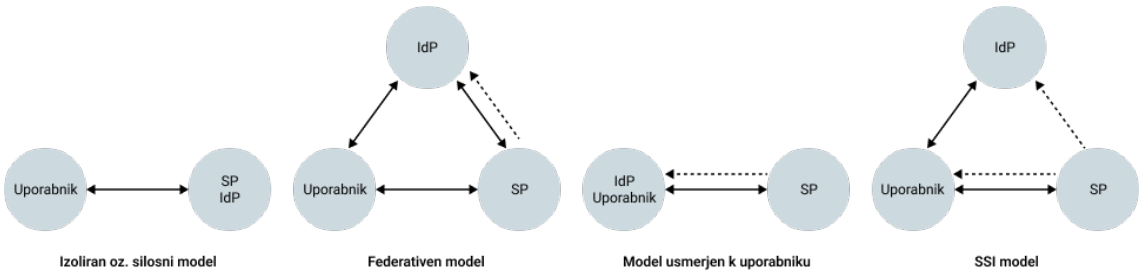
Uporabnik je praviloma fizična oseba z vsaj eno digitalno identiteto, ki želi izvesti digitalno transakcijo in / ali dostopati do storitev. *Ponudnik identitete* je entiteta, ki je zadolžena za administracijo in upravljanje digitalne identitete ter za izvajanje identifikacije in overjanja. Za vsakega novega uporabnika registrira identifikatorje in atribute ter skladno s svojo politiko preveri resničnost podanih identitetnih podatkov (npr. preverjanje osebne izkaznice, dokaz o prejemu elektronske pošte ipd.). *Ponudnik storitev* je entiteta, ki uporabniku zagotavlja storitev in se zanaša na ponudnika identitete za identifikacijo in overjanje uporabnika [1].

Najenostavnejši in najgosteje uporabljen model IdM predstavlja t. i. *izoliran oz. silosni model* (angl. Isolated or Silo Model), ki vključuje zgolj dve entiteti, uporabnika in SP, ki je poleg zagotavljanja storitev, odgovoren tudi za administracijo, shranjevanje ter upravljanje identitetnih podatkov. Uporabnik si mora posledično ustvariti identitetno oz. uporabniški račun pri vsakem izmed SP, kar zahteva večkraten vnos identitetnih podatkov [4],

predstavlja nekonsistentno uporabniško izkušnjo in veliko obremenitev za uporabnika [2] ter prinaša varnostna tveganja, povezana tudi z uporabo podobnih ali enakih gesel z nizko entropijo v različnih sistemih [1, 3, 4].

Rešitev omenjenega problema predstavlja *centraliziran federativen model*, ki uvaja zunanjega IdP, ki služi kot posrednik med uporabnikom in različnimi SP ter zagotavlja funkcionalnosti, povezane z upravljanjem digitalne identitete. Uporabniku omogoča, da si ustvari identiteto pri osrednjem IdP, pri čemer lahko identifikator in pripadajočo poverilnico uporabi pri overjanju z različnimi SP. Z uporabo mehanizma enotne prijave (angl. Single Sign On - SSO) mu je tako omogočen dostop do vseh storitev, ki so odvisne od istega ponudnika identitete [1, 5]. Uporabnik se more posledično registrirati zgolj pri peščici IdP, ki služijo svojemu naboru SP [2]. Ta model je enostavnejši za uporabo in ponuja boljšo uporabniško izkušnjo, vendar centralizacija predstavlja dodatno ranljivost. Razkritje enega identifikatorja in pripadajoče poverilnice namreč zadostuje za dostop do vseh storitev naenkrat [1]. Poleg omenjenega pa neposredna vključenost v proces overjanja, omogoča IdP sledenje uporabnikom in učenje njihovih vedenj [2]. Podobno kot centraliziran, tudi *decentraliziran federativen model* temelji na zunanjih IdP in omogoča implementacijo SSO. Model zahteva vzpostavitev zaupanje med različnimi IdP in SP, ki so združeni v t. i. krog zaupanja (angl. Circle of Trust - CoT), ki pogosto temelji na sporazumih in skupni tehnološki platformi [1]. IdP, združeni v CoT, si lahko medsebojno delegirajo zahtevo za overjanje [2]. Posledično so funkcije IdM [5] in uporabniški podatki porazdeljeni med različnimi ponudniki znotraj CoT, kar zmanjšuje varnostna tveganja. Uporabniki se lahko overijo zgolj pri enem izmed IdP za dostopanje do storitev znotraj CoT [1]. Dobro znan primer tega modela je evropski, interoperabilni okvir eIDAS (angl. electronic IDentification, Authentication and Trust Services), ki združuje nacionalne sisteme IdM držav članic Evropske unije (EU) ter omogoča čezmejno elektronsko identifikacijo, overjanje in storitve zaupanja [2]. Interakcije med IdP in SP ter končnimi uporabniki so bile v *centraliziranem in decentraliziranem federativnem modelu* poenostavljene iz vidika upravljanja identifikatorjev in poverilnic ter standardizirane preko izmenjave žetonov, kot so SAML, OAuth, OpenID Connect (OIDC), itd. [3]. Pri čemer pa nadzor nad uporabniškimi podatki (identifikatorji in atributi) še vedno ostaja na strani IdP in SP, ki identitetne podatke shranjujejo, obdelujejo in tudi distribuirajo. Medtem ko je uporabnik primoran zaupati, da bodo spoštovane njegove pravice in zasebnost [1].

Za razliko od prejšnjih modelov, ki podatke uporabnika shranjujejo centralizirano, bodisi pri IdP ali SP, se v okviru modela, osredotočenega na uporabnika (angl. User-Centric model), podatki shranjujejo v uporabnikovi domeni (npr. na pametni kartici ali na mobilnem telefonu, kjer so zaščiteni z varnostnimi elementi na osnovi strojne opreme), kar povečuje varnost in zasebnost. Podatki so pod uporabnikovim nadzorom in so posredovani SP ob vsakem overjanju. Primeri takšnih rešitev so npr. nacionalne IdM rešitve [2]. eIDAS npr. za uporabo kvalificiranih digitalnih podpisov zahteva uporabo kvalificiranih naprav, kot so kriptografske kartice in USB-ji.



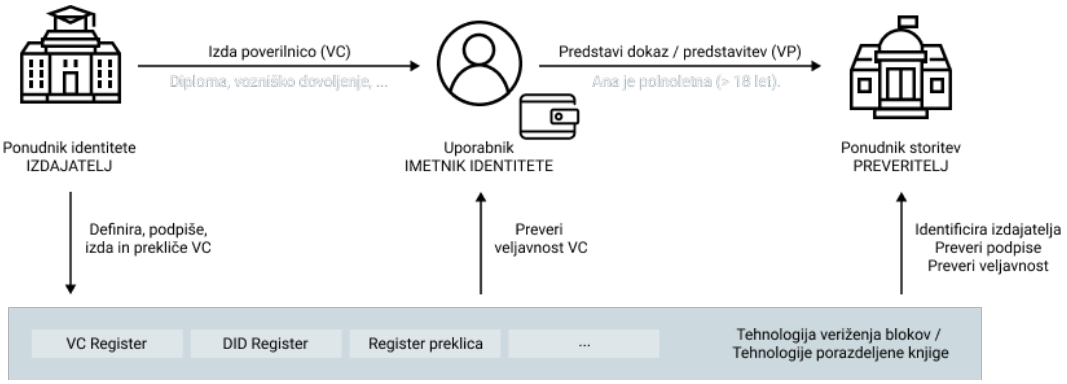
Slika 1: IdM modeli. Neprekinjene črte predstavljajo interakcije, črtkane črte pa zaupanje.
Vir: [3].

2.1 Decentralizirane in samoupravljane identitete

Naslednji korak na področju IdM predstavljajo decentralizirane in samoupravljanje identitete (angl. Self-Sovereign Identity - SSI). Gre za k uporabniku usmerjen decentraliziran pristop, ki entitetam oz. uporabnikom (posameznikom, organizacijam, stvarem) omogoča, da v celoti nadzirajo in upravljajo svojo digitalno identiteto (identifikatorje in povezane identitetne podatke) [13], brez da bi se v interakcijah zanašali na zunanje entitete [14]. Med uporabnikom in drugo entiteto tako ni nobenega posrednika, obstaja zgolj Peer-to-Peer povezava, preko katere si izmenjujeta podatke. Za razliko od ostalih modelov je v okviru modela SSI, vsak uporabnik sam odgovoren za administracijo, shranjevanje, upravljanje in distribucijo identitetnih podatkov. Uporabnik je tako v središču digitalnih interakcij in nadzoruje pretok svojih podatkov ter odloča kdaj, s kom in katere podatke želi deliti. Uporabniku ni potrebno ustvariti računa pri vsakem izmed SP, prav tako ni potrebe po IdP, ki bi uporabniku zagotovili identiteto in njeno upravljanje. Identitetni podatki se shranjujejo v domeni uporabnika, v digitalnih denarnicah, ki so pod popolnim nadzorom uporabnika.

Tudi v SSI modelu so ključne tri entitete, ki nastopajo v vlogi *izdajatelja* identitetnih atributov (angl. Issuer), *uporabnika oz. imetnika identitete* (angl. Identity Holder) in *preveritelja* (angl. Verifier) oz. ponudnik storitev (Slika 2). Pri čemer je potrebno poudariti, da lahko vsaka izmed entitet v različnih kontekstih deluje v drugi vlogi.

Izdajatelj potrdi določene atribute uporabnika oz. izda in digitalno podpiše t. i. *preverljivo poverilnico*, ki vsebuje enega ali več atributov oz. trditev, ki se nanašajo na *imetnika identitete*. Ta je odgovoren za pridobivanje, shranjevanje, upravljanje in deljenje svojih identitetnih podatkov s *preveriteljem*, ki običajno od uporabnika zahteva dokazilo o njegovi identiteti. Slednje omogoča identifikacijo in verifikacijo ter zagotavljanje dostopa do želenih storitev. Proces preverjanja ne zahteva vključitve izdajatelja poverilnic [23], zaupanje se lahko namreč vzpostavi z uporabo *decentraliziranih identifikatorjev* (angl. Decentralized Identifiers - DID), *preverljivih poverilnic* (angl. Verifiable Credentials - VC) in *tehnologije verižnja blokov* (angl. Blockchain, BC) (ali tehnologije porazdeljene knjige (angl. Decentralized Ledger Technology - DLT) ali druge decentralizirane tehnologije), ki predstavljajo ključne komponente SSI arhitekture in bodo predstavljene v nadaljevanju. Poleg omenjenega pa je bistvena komponenta v SSI ekosistemu, *digitalna denarnica*, s pomočjo katere uporabniki upravljajo svoje digitalne identitete in bodo podrobneje naslovljene v poglavju 4.



Slika 2: Interakcije in pretok podatkov med izdajateljem, imetnikom identitete in preveriteljem.
Vir: lasten.

Decentralizirani identifikatorji (DID) so globalni, edinstveni, preverljivi in trajni digitalni identifikatorji, popolnoma neodvisni od centraliziranih registrov, zunanjih entitet ali ponudnikov identitete, ki bi zagotavljala njihovo administracijo, upravljanje in obstoj. Omogočajo samostojno izvajanje operacij registracije, posodabljanja, razrešitve in preklica, brez centralizirane registracije, overjanja in avtorizacije. Omogočajo ustvarjanje edinstvenih, zasebnih in varnih povezav med dvema entitetama. Pri čemer si lahko vsaka entiteta ustvari in upravlja poljubno število DID-ov ter jih ločeno uporablja v različnih digitalnih interakcijah in kontekstih, kar preprečuje korelacijo podatkov. Vsak DID je predstavljen v obliki URI-ja in je povezan z DID subjektom (imetnikom identitete) in

DID dokumentom, ki opisuje subjekt, javne ključe, biometrične podatke in vse druge mehanizme, ki se uporabljajo za preverjanje prisotnosti lastništva nad DID-i [11].

Preverljive poverilnice (VC), lahko podobno kot fizične, vsebujejo informacije, povezane z identifikacijo subjekta oz. imetnika identitete (npr. ime in priimek, identifikacijska številka, fotografija) in nabor trditev o subjektu (npr. državljanstvo, datum rojstva), skupaj z metapodatki, kot so izdajatelj (npr. Upravna enota Maribor), vrsta (npr. osebna izkaznica) in omejitve poverilnice (npr. obdobje veljavnosti, pogoji uporabe itn.), ter podatki o mehanizmu preverjanja in preklica. VC torej vsebuje metapodatke in eno ali več trditev oz. atributov ter je digitalno podpisan s strani izdajatelja, ki s podpisom potrjuje resničnost podatkov v VC. Uporaba kriptografskih mehanizmov, VC ščiti pred nedovoljenimi posegi ter omogoča *kriptografsko preverljivost*. Imetniki VC lahko ustvarijo preverljive predstavitve (angl. Verifiable Presentations - VP) in jih delijo s preveritelji z namenom dokazovanja identitete in identitetnih atributov [10]. Pri čemer lahko z uporabo metod, kot sta *selektivno razkritje* (angl. Selective Disclosure) in *dokaz o ničelnem znanju* (angl. Zero-Knowledge Proof - ZKP) ohranjamo zasebnost v interakcijah z drugimi entitetami. Z uporabo selektivnega razkritja lahko ustvarimo VP, sestavljen zgolj iz podmnožice atributov iz ene ali več poverilnic. Na drugi strani uporaba ZKP omogoča dokazovanje atributov, brez dejanskega razkritja vrednosti. Če moremo na primer dokazati svojo starost, lahko s pomočjo selektivnega razkritja delimo zgolj leto rojstva iz vozniškega dovoljenja, pri čemer pa ne razkrijemo preostalih atributov, kot so dan in mesec rojstva ter naslov itn. Z uporabo ZKP pa lahko dokažemo, da smo npr. starejši od 18 let, ne da bi razkrili datum svojega rojstva. Omenjeno je še posebej koristno v situacijah, ko ne zaupamo preveritelju.

Tehnologija verižnega blokov ali DLT lahko v okviru SSI služi kot preverljiv register podatkov (angl. Verifiable Data Registry - VDR) in vzpostavlja zaupanje med različnimi entitetami. V VDR se lahko shranjujejo (i) javni DID-i, (ii) definicije VC-jev, (iii) sheme, (iv) podatki o stanju VC-jev (register preklica) in (v) dokazi o interakcijah med entitetami. Posledično lahko deluje kot nadomestilo za centralizirani organ za registracijo v tradicionalnih sistemih za upravljanje identitete ter zagotavlja decentralizirano infrastrukturo javnih ključev (angl. Decentralized Public-key Infrastructure - DPKI) [26] ter shranjuje povezavo med identifikatorjem in metodo overjanja [23]. V takšnih DID registrih so shranjeni javni DID-i (angl. public DID) organizacij oz. izdajateljev VC-jev.

3 Evropske digitalne identitete

EU ima splošno znano kompleksno strukturo tako iz pravnih, ekonomskih in drugih sektorjev kakor tudi na področju upravljanja z digitalnimi identitetami (IdM). Vsaka država članica vodi lastno politiko IdM, pri čemer se loteva le te tudi s tehničnega vidika, na različne načine. Določene države, kot so npr. Estonija, Danska in Nemčija, imajo zelo dodelane politike in tehnično podporo IdM, med tem, ko imajo druge to poenostavljeno. Prav tako ima vsaka država članica drugačno filozofijo upravljanja, ki vključuje različne zaupne kvalificirane IdP in SP. Estonci tako ponujajo svojim državljanom številne načine upravljanja digitalnih identitet, kot npr. ID Card, DIGI-ID, RP-card. Med tem so v Avstriji izdali ID Austria, ki omogoča različne funkcionalnosti IdM, podobno novim osebnim izkaznicam v Sloveniji. Slovenija se je s storitvijo SI-PASS pomembno pozicionirala, saj smo pokazali, kako pod eno streho omogočiti različne ravni zaupanja, različne načine identifikacije itn.

Ne glede na dovršenost posameznih pristopov znotraj EU so le ti heterogeni in povzročajo preglavico ideji povezane EU, ki pa to ne more biti le v fizični obliki, temveč nujno tudi v digitalni. Evropska komisija (EK) je tako v prejšnjem desetletju sprejela idejo Enotnega digitalnega trga Evrope (angl. Single Digital Market) ter izdala uredbi eIDAS in SDGR (angl. Single Digital Gateway Regulation).

3.1 Uredba o elektronski identifikaciji in storitvah zaupanja - eIDAS

eIDAS je od leta 2014 glavni zakonodajni akt Evropske unije v zvezi z elektronskim podpisom in elektronskim poslovanjem. Navezuje se na t. i. eIDAS uredbo oz. Uredba (EU) št. 910/2014 - Uredba o elektronski identifikaciji in storitvah zaupanja [19], ki je osnova Zakonu o elektronski identifikaciji in storitvah zaupanja (ZEISZ) v

Republiki Sloveniji. Uredba in zakon urejata elektronsko identiteto posameznika ali podjetja, ki jo posamezna država članica EU dodeli svojim državljanom ali poslovnim subjektom. Del tega je tudi umestitev sredstev za elektronsko identifikacijo in podpisovanje, s katerim se prej omenjena identiteta dokazuje v pravni in tehnični prostor. Poglavitna ideja eIDAS je ta, da lahko ljudje in podjetja znotraj EU uporabljajo lastne nacionalne elektronske identifikatorje (eID) za dostop do (javnih) storitev, ki so na voljo na spletu v drugih državah EU. Primer teh storitev so oddaja davčnih napovedi, vpis na tujo univerzo, odpiranje bančnega računa na daljavo, ustanovitev podjetja v drugi državi članici, preverjanje pristnosti za internetna plačila, spletno zbiranje ponudb, javni razpisi idr. eIDAS tako opredeljuje interoperabilni nivo za združevanje obstoječih nacionalnih rešitev elektronske identifikacije, kot so slovenska SIGEN-CA ali SI-PASS, avstrijska državljanska kartica, belgijska eID kartica itn.

eIDAS prav tako uvaja regulatorni okvir, ki v primeru kvalificiranih digitalnih certifikatov in s tem povezanih podpisov, le te pravno enači z lastnoročnim podpisom. Takšna vrsta pravnih zagotovil je možna zgolj v primeru kvalificiranih digitalnih podpisov (angl. Qualified Electronic Signature - QES), za katere eIDAS zahteva uporabo t. i. kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa (angl. Qualified Electronic Signature/Seal Creation Device - QSCD). Primer takšnih naprav v primeru lokalne ali centralizirane uporabe so kriptografske kartice in kriptografski USB ter v primeru oddaljene uporabe so to varnostni moduli strojne opreme (angl. Hardware Security Module - HSM). Razen QES uvaja eIDAS tudi napredne digitalne podpise (angl. Advanced Electronic Signature - AdES), ki pa ne zahtevajo uporabe QSCD. S tem povezane so tudi t. i. ravni zanesljivosti (angl. Level of Assurance - LoA), pri čemer definira eIDAS kar tri nivoje: nizka, srednja in visoka raven zanesljivosti. Slednja je definirana ob uporabi kvalificiranih digitalnih podpisov. Prednost različnih ravni zanesljivosti je v tem, da lahko tako uporabnik kot ponudnik storitev, ki ne zahteva visoke ravni zanesljivosti, uporabita tisto z nižjo stopnjo, saj je le ta lažja za pridobiti in upravljati.

Splošna IT arhitektura eIDAS temelji na t. i. nacionalnih eIDAS vozliščih. Vsaka država članica EU upravlja lastno vozlišče, ki je povezano s ponudniki digitalne identitete. Vsako nacionalno vozlišče eIDAS je sposobno identificirati in overiti lastne državljane in sprejemati zahteve za overjanje od SP, ki se nahajajo v isti državi. Da bi omogočili interoperabilnost na nivoju EU, so vsa vozlišča eIDAS povezana ter omogočajo tudi medsebojno avtomatizirano podporo.

EK trenutno ocenjuje eIDAS, pri čemer je leta 2020 že izvedla prvo odprto posvetovanje. Cilj posvetovanja je bil zbrati povratne informacije o gonilih in ovirah za razvoj in uvedbo storitev zaupanja in eID v Evropi, pri čemer se je obravnavala tudi možnost ogrodja za zagotavljanje digitalne identitete EU.

3.2 Ogrodje evropske digitalne identitete

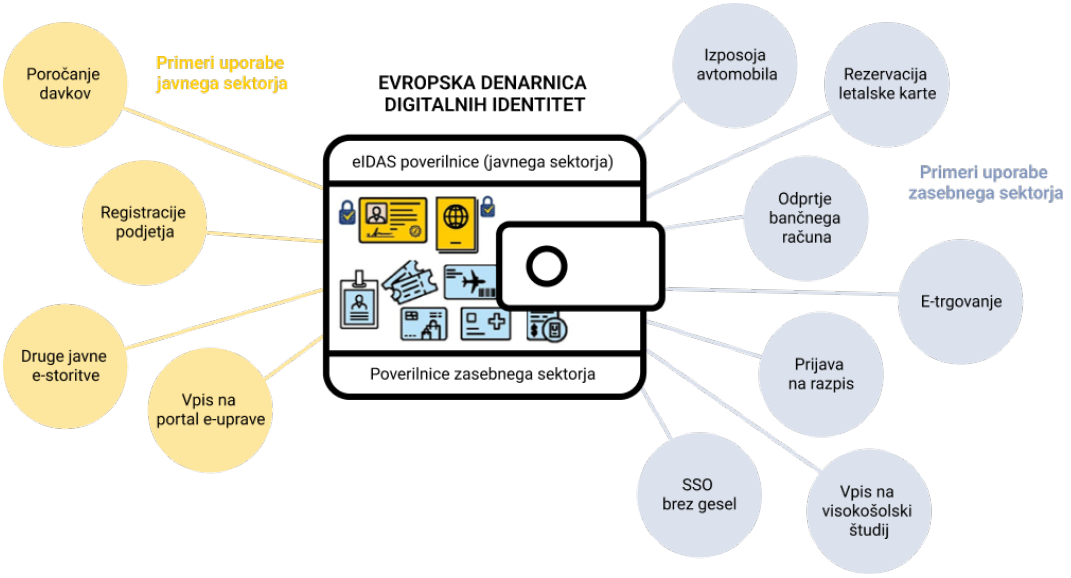
Po letu 2020, ko je EK izvedla širok posvet glede eIDAS, je bilo zaključeno, da je le ta sicer dobro zasnovan in tehnično izpolnjuje svoje osnovno poslanstvo, vendar se na nivoju EU uporablja zgolj 14 % [17]. Razlogov za slabšo sprejetost med prebivalci je mnogo, med njimi tudi dejstvo, da se v določenih državah že nacionalne eID uporabljajo v omejenem obsegu. Ne glede na slednje pa je EK identificirala tudi druge pomanjkljivosti, ki se nanašajo predvsem na vidik uporabniške prijaznosti, nadzora nad lastnimi podatki (tj. zasebnost), ter popolne interoperabilnosti med državami članicami. Slednje je posledica dejstva, da določene države še zmeraj niso oznanile svoje nacionalne sheme (med njimi tudi Slovenija) [18].

Upoštevajoč predstavljena dejstva je EK predlagala novo uredbo, imenovana tudi eIDAS 2.0, za ustvarjanje usklajene zmogljivosti digitalne identitete za vse državljane EU, ki jo je poimenovala tudi Evropske digitalne identitete (angl. European Digital Identity). Predlagana posodobitev si prizadeva uravnotežiti digitalni svet v korist posameznika in manj v korist korporacij, s tem, da ponudi večjo zasebnost, zaupanje in nadzor nad svojimi podatki oz. da se uporabnikom ponudi zaupanja vredno, varno in široko uporabno evropsko digitalno identiteto, ki bo vsem Evropejcem omogočila digitalno dokazovanje svoje identitete z namenom dostopanja do digitalnih storitev

po celotni EU. Ključnega pomena je dejstvo, da se želi graditi na dosežkih in dognanjih eIDAS 1.0 in ne začenjati iz točke nič.

Povzeto so osnovni stebri iskanja izboljšav na osnovi koncepta evropske digitalne identitete: (i) okrepljeni nacionalni sistemi eID znotraj eIDAS; (ii) ponujanje uporabniško nadzorovane digitalne identitete na osnovi digitalnih denarnic; ter (iii) zasebni sektor kot ponudnik digitalnih storitev, ki so povezane z ekosistemom evropske digitalne identitete [20].

Osrednja komponenta nove uredbe so torej t. i. evropske denarnice digitalnih identitet (angl. European Digital Identity Wallet - EUDIW). Te so primarno mišljene kot mobilne denarnice, saj uporabniki po svetu vedno bolj zahtevajo mobilno identifikacijo oz. vedno bolj uporabljajo pametne telefone za različne digitalne storitve (npr. spletno bančništvo, Covid potrdila itn.). Prav tako področje SSI ni ostalo neopaženo s strani EK, saj ponuja morebitno rešitev za številne izzive, ki jih želi EK nasloviti. Izpostaviti je potrebno dejstvo, da je *EK junija 2021 izdala zahtevo, da morajo države članice EU do leta 2023 ponuditi takšno digitalno denarnico vsem svojim državljanom* [22]. S tem želi EK na osnovi eIDAS 2.0 v celoti uresničiti svojo vizijo univerzalne in čezmejne evropske digitalne identitete, pri čemer je tudi zastavljen kazalnik, ki načrtuje, da bo do leta 2030 vsaj 80 % populacije EU imelo registrirano sredstvo elektronske identifikacije [21].



Slika 3: Primeri uporabe EUDIW.
Vir: [15].

EUDIW so torej mišljene kot kriptografsko varne digitalne denarnice, ki bi državljanom omogočile ne zgolj upravljanje svojih digitalnih identitet (kot oblik osebnih izkaznic) ter na osnovi teh identifikacijo, overjanje in avtorizacijo oz. dostop do javnih in / ali zasebnih storitev, temveč tudi varno shranjevanje in upravljanje drugih vrst digitalnih dokumentov oz. poverilnic, kot so vozniška dovoljenja, različne druge potne listine, bančne kartice, klubske izkaznice itn. [17]. V prihodnjih letih bodo EUDIW podpirale vedno večji nabor storitev in primerov uporabe (Slika 3). Že sedaj je jasno, da bo podatkovni model takšnih digitalnih dokumentov temeljil na preverljivih poverilnicah (VC). Dodatna pomembna lastnost EUDIW je tudi omogočanje *selektivnega razkritja atributov*, kot je starost uporabnika. Uporabnik mora imeti možnost s pomočjo EUDIW deliti le izbran, nujen in omejen nabor informacij, ki jih potrebuje potencialen SP. Če na primer uporabljate denarnico za dokazovanje svoje starosti, vam ni potrebno deliti drugih osebnih podatkov, kot so datum rojstva, ime ali naslov. S tehnološkega stališča je takšno funkcionalnost možno doseči z vpeljavo ZKP (angl. Zero-Knowledge Proofs) [16]. Seveda pa bodo EUDIW morale biti skladne tudi z obstoječimi pravnimi okvirji EU, kot so GDPR ter eIDAS, in sicer pri slednjem iz vidika,

da bodo EUDIW morale zagotavljati močno kriptografsko podporo in ponuditi visok nivo zanesljivosti, ki je nuja za zagotavljanje QES ali vsaj AdES.

Države članice si bodo lahko prizadevale za lastno zasnovo, izgled in funkcionalnost EUDIW, pri čemer bo nujna kompatibilnost z osnovnimi zahtevami EK ter posledično popolna interoperabilnost vseh EUDIW, ne glede na državo članico oz. zasebnega ponudnika EUDIW.

4 Tehnično ozadje denarnic digitalnih identitet

Ideja EUIDW ni nova in temelji na *digitalnih denarnicah*, ki že več let predstavlja varno plačilno sredstvo, in posledično, zamenjavo fizične denarnice. Primarno gre za finančne aplikacije za shranjevanje sredstev, izvedbo transakcij in sledenje zgodovini plačil, z uporabo prenosljivih naprav, kot so pametni telefoni, tablice in pametne ure. Omogočajo vnos in varno shranjevanje podatkov o plačilu (npr. podatki o kreditni kartici, debetni kartici ali bančnem računu) in plačevanje brez potrebe po predstavitvi fizičnih sredstev. Poleg omenjenega nekatere denarnice omogočajo tudi digitalizacijo in shranjevanje drugih fizičnih dokumentov, kot so vozniško dovoljenje, osebna izkaznica, razne članske izkaznice, kartice zvestobe, darilne kartice in kupone, pa tudi vstopnice za prireditve, letalske vozovnice in vozovnice za javni prevoz ter hotelske rezervacije [27].

Digitalne denarnice izkoriščajo zmogljivosti mobilnih naprav za izboljšanje dostopa do storitev in produktov ter odpravljajo potrebo po fizičnih denarnicah. Uporabljajo QR oznake ter brezžične tehnologije, kot so Bluetooth, Wifi in magnetne signale (Near-field communication - NFC, Magnetic Secure Transmission - MST), ki omogočajo zanesljive in varne transakcije in s tem prenos plačilnih podatkov med napravami [27]. Poleg znane uporabe plačevanja v trgovinah, restavracijah in na drugih prodajnih mestih, ki uporabnikom omogoča podobno uporabniško izkušnjo, kot pri uporabi brezstične kartice pa nekatere denarnice omogočajo tudi dvig denarja na bankomatih in izvedbo spletnih transakcij (npr. plačevanje preko spleta, potrjevanje spletnih plačil (Two Factor Authentication - 2FA), spletna nakazila ipd.).

Izbira digitalnih denarnic je vedno večja, znana primera sta npr. Google Wallet (Android) in Apple Wallet (iOS), ki podpirata plačevanje na fizičnih plačilnih mestih (NFC), v spletnih trgovinah in aplikacijah, vendar sta omejena na uporabnike pripadajočih operacijskih sistemov. Mobilne denarnice pa ponujajo tudi slovenske spletne banke. Komitentom (i) Nove KBM je na voljo denarnica mDen@rnica, (ii) NLB - NLB Pay, (iii) Banke Intesa Sanpaolo - Wave2Pay in (iv) Sberbank – mBills [28]. Med digitalne denarnice pa spadajo tudi kripto denarnice v obliki strojne ali programske opreme, ki omogočajo shranjevanje javnih in zasebnih ključev, potrebnih za prejemanje in plačevanje s kriptovalutami.

4.1 Osnovni koncepti

Z razvojem tehnologij in identitetnih modelov pa so se pojavile tudi t. i. *denarnice digitalnih identitet* (angl. Digital Identity Wallet - DIW), ki predstavljajo sredstvo, s katerim uporabniki nadzirajo in upravljajo svoje digitalne identitete. Predstavljajo ključen uporabniški vmesnik med končnimi uporabniki in decentralizirano infrastrukturo ter imajo pomembno vlogo pri identifikaciji, overjanju in avtorizaciji uporabnikov ter dostopanju do storitev. Gre za prenosljive in varne osebne repozitorije, običajno v obliki mobilne denarnice ali denarnice v oblaku, ki vključujejo programsko aplikacijo in šifrirano podatkovno bazo, v kateri uporabniki (imetniki identitete oz. upravljavci denarnice) shranjujejo identifikatorje oz. osebne identifikacijske podatke (angl. Personal Identification Data - PID), kriptografski material (zasebni ključi), digitalne dokumente/poverilnice oz. (ne)kvalificirane elektronsko potrjevanje atribute (angl. (Qualified) Electronic Attestation of Attributes - (Q)EAA) in druge občutljive, zasebne podatke. Poleg shranjevanja, morajo takšne DIW podpirati tudi pregled, upravljanje in uporabo oz. deljenje omenjenih podatkov.

Iz trgovin z mobilnimi aplikacijami (Google Play in Apple Store) si lahko že sedaj namestimo DIW, pri čemer mnoge med njimi temeljijo na konceptu SSI in podpirajo (i) ustvarjanje in upravljanje več nepovezanih identifikatorjev za različne interakcije, (ii) povezovanje in komuniciranje z drugimi entitetami, (iii) pridobivanje in shranjevanje identitetnih podatkov v obliki VC-jev od izdajateljev, (iv) ustvarjanje in deljenje VP-jev s preveritelji, ki zahtevajo dokazilo o identiteti za namen preverjanja in zagotavljanja storitev, ter (v) pregled nad podatki in njihovo uporabo. Zagotavljajo varno upravljanje kriptografskih ključev (zasebnih ključev), identifikatorjev in poverilnic ter s tem omogočajo storitve upravljanja identitete, ki je bilo predhodno v domeni IdP. Takšne DIW so npr. VIDwallet, Trinsic Wallet, esatus Wallet, Connect.Me DIW, Gataca, Lissi Wallet, itd. [8]. Pri čemer pa je bil letos objavljen tudi seznam interoperabilnih DIW, kompatibilnih z evropskim omrežjem EBSI (European Blockchain Services Infrastructure) [25].

4.2 Tipi denarnic

Kot omenjeno, DIW predstavljajo orodje, ki omogoča uporabnikom nadziranje in upravljanje digitalnih identitet [6]. Obstajajo različni tipi DIW, ki se razlikujejo glede na uporabljen IdM model in vrsto okolja, ki je lahko bodisi *lokalno* bodisi *oddaljeno*, odvisno od lokacije shranjenih podatkov. V lokalnem okolju uporabniki nadzorujejo in imajo v lasti zahtevano infrastrukturo, medtem ko infrastruktura v oddaljenem, oblačnem okolju ni neposredno v lasti in upravljanju uporabnikov, temveč ponudnikov okolja [2].

Poznamo (i) *namizne denarnice* in (ii) denarnice, ki predstavljajo *razširitev brskalnika* in so naložene na računalnik, (iii) *mobilne denarnice* v obliki mobilne aplikacije, ki jih uporabnik lahko prenese iz trgovin z aplikacijami, (iv) *denarnice v oblaku*, ki temeljijo na oddaljenem shranjevanju v oblaku, ter (v) *denarnice s strojno opremo* (fizične naprave, kot je trdi diska ali USB) [12], ki omogočajo uporabnikom prejemanje in pošiljanje poverilnic le, če je naprava povezana z računalnikom z dostopom do interneta.

Tako poznamo vse od (iv) *oblačnih* denarnic do resnično *SSI denarnic*, ki naj bi bile pod popolnim nadzorom uporabnikov, (iii) na mobilnem telefonu, (i, ii) osebnem računalniku, ali (iv) drugi napravi, izven dosega tretjih oseb. Pri čemer so mobilne denarnice in denarnice v oblaku najbolj enostavne za uporabo, ponujajo dobro uporabniško izkušnjo ter so najbolj prenosljive med omenjenimi možnostmi.

4.3 Funkcionalnosti

Na osnovi analize obstoječih DIW in osnutku arhitekture ter referenčnega okvirja evropske digitalne identitete [24] predstavljamo funkcionalne zahteve DIW, ki naj bi jih izpolnjevale EUDIW namenjene končnim uporabnikom oz. imetnikom identitete.

Slednje morajo v osnovi podpirati funkcionalnosti, povezane *z identifikacijo in overjanjem* ter funkcionalnosti, povezane s *pridobivanjem, shranjevanjem, upravljanjem in izmenjavo* podatkov in poverilnic ter *shranjevanje in upravljanje* kriptografskega materiala. Uporabnikom morajo omogočiti enostavno delovanje, izgradnjo digitalne identitete ter pridobivanje dostopa do (javnih in / ali zasebnih) storitev v digitalnem okolju.

Ključnega pomena je, da DIW zagotavlja *digitalno identifikacijo in overjanje*, ki se lahko izvede z eID, z uporabo kvalificiranih ali nekvalificiranih digitalnih potrdil ali z uporabo DID-ov v kombinaciji s preverljivimi izkaznicami (VID). Slednje je skladno s konceptom SSI in zahteva *obojestransko overjanje*. Uporabnik in ponudnik identitetnih atributov ali storitev morata namreč predhodno vzpostaviti dvosmerno, varno povezavo oziroma komunikacijski kanal med svojima DIW. Vključeni entiteti si morata izmenjati identifikatorje (DID-e) in druge metapodatke, ki so ključnega pomena za overjanje oz. dokazovanje identitete in podatke, pomembne za izvedbo posamezne transakcije. Inicializacija identifikacije in overjanja sta možni na *podlagi generiranja, predstavitve in skeniranja QR oznak*, ki omogoča šifriranje in enostavno posredovanje potrebnih podatkov za izvedbo procesa. Pri tem ni pomembna zgolj identifikacija in overjanje vključenih entitet, ampak tudi njunih DIW, kar povečuje zaupanje in varnost ekosistema ter zagotavlja interoperabilnost z uporabo ustreznih naprav in denarnic.

Uporabniki morajo imeti možnost *zahtevati in pridobiti identitetne atribute*. V okviru EUDIW je govora o t. i. kvalificiranih in nekvalificiranih elektronsko potrjenih atributih (angl. (Qualified) Electronic Attestation of Attributes - QEAA in EAA), ki jih bo najverjetneje možno pridobiti v obliki VC-jev. Posledično mora imeti DIW integrirano funkcionalnost varnega *shranjevanja in upravljanja VC-jev (vključno z brisanjem)*, kar omogoča predstavitev oz. deljenje podatkov na zahtevo, ne da bi uporabnik moral ob vsaki zahtevi pridobiti podatke od ponudnika takšnih atributov. Slednje zmanjšuje možnost sledenja, vpletenost posrednikov v digitalne interakcije ter daje uporabnikom nadzor nad shranjevanjem in deljenjem svojih podatkov. *Shramba DIW* je lahko *lokalna, oddaljena ali hibridna* (z lokalnim shranjevanjem pointerjev do oddaljene shrambe) in mora poleg preverljivih poverilnic, identifikatorjev oz. osebnih identifikacijskih podatkov omogočati tudi shranjevanje kriptografskega materiala, ki omogoča nadzor sredstev in dokazovanje lastništva [7, 9], vključno z elektronsko *identifikacijo, overjanjem in digitalnim podpisovanjem* dokumentov in poverilnic. V primeru uporabe eID, je potrebno zagotoviti hrambo (ne)kvalificiranih digitalnih potrdil. V primeru uporabe DID-ov pa hrambo zasebnih kriptografskih ključev. Kriptografske funkcije so poleg shranjevanja in upravljanja kriptografskega materiala, ključne za večino funkcionalnosti denarnic, kot so npr. kvalificirano digitalno podpisovanje, identifikacija in overjanje, selektivno razkritje ipd. Upravljanje vključuje kreiranje, shranjevanje, uporabo, modificiranje in brisanje kriptografskega materiala, pri čemer lahko vmesnik za zagotavljanje funkcionalnosti izkorišča programske in / ali strojne rešitve.

DIW morajo zagotavljati *deljenje oz. distribucijo* identitetnih atributov, zahtevanih s strani tretjih oseb oz. ponudnikov storitev. Osnovno funkcionalnost *deljenja*, ki omogoča posredovanje podatkov, lahko razširja funkcionalnost *kombiniranja* in *selektivne izbire oz. razkritja ter minimizacije podatkov*, ki omogoča razkritje minimalne količine podatkov, potrebnih za uspešno izvedbo posamezne transakcije. Posledično lahko uporabnik iz nabora atributov v shranjenih poverilnicah, izbere zgolj peščico atributov, pomembnih v specifičnem kontekstu, s čimer pridobi nadzor nad deljenjem lastnih podatkov. Uporabnik mora torej imeti možnost, da selektivno izbere atribute iz enega ali več VC-jev in generira VP ob upoštevanju minimalnega razkritja podatkov ter VP digitalno podpiše z uporabo (ne)kvalificiranih digitalnih potrdil ali zasebnega ključa. DIW morajo posledično zagotavljati funkcionalnost digitalnega podpisovanja dokumentov in poverilnic.

Podatki (identifikatorji, poverilnice in kriptografski material) morajo biti v denarnici vedno dostopni in na razpolago, ko jih uporabnik potrebuje. Omogočen mora biti *hiter in enostaven dostop* ter zagotovljena dobra *uporabniška izkušnja*. Za uspešno upravljanje in deljenje podatkov je ključen intuitiven, nazoren, jasen in nedvoumen prikaz podatkov. Za uporabnike je ključen prikaz pridobljenih identitetnih dokumentov oz. preverljivih poverilnic in prikaz deljenih podatkov iz poverilnic, ter prikaz zgodovine izvedenih transakcij, kar lahko uporabniku olajša nadzorovanje in upravljanje svoje identitete. V okviru koncepta SSI je koristen tudi prikaz kontaktov oziroma t. i. vzpostavljenih DID povezav s tretjimi osebami (ponudniki preverljivih poverilnic in storitev).

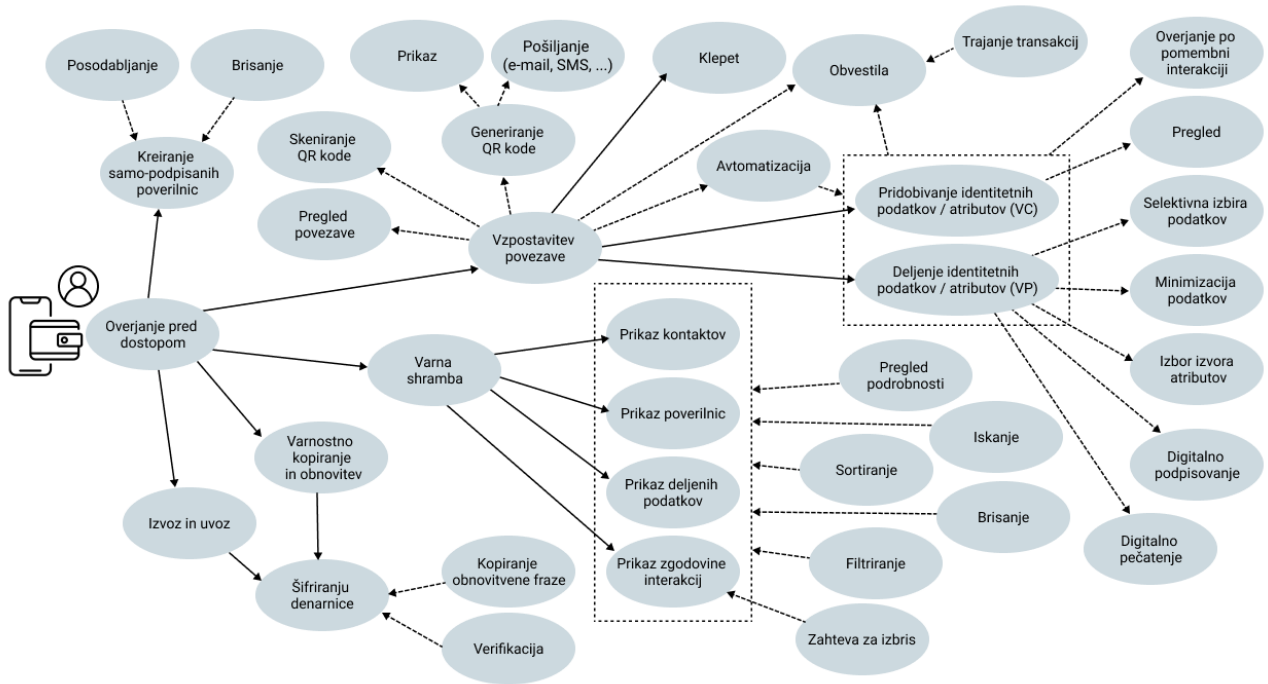
Uporabniki morajo biti *obveščeni* o pomembnih informacijah v povezavi s svojo DIW ter o informacijah in korakih v interakciji z drugimi entitetami. DIW lahko v ta namen uporabljajo opozorilna okna in potisna obvestila, ki so povezana z informiranjem in uspešnimi ali neuspešnimi transakcijami (npr. ob identifikaciji in overjanju, ob prejeti ponudbi za sprejem poverilnic, ob prejeti zahtevi za deljenje podatkov ipd.). Zaradi rokovanja z osebnimi podatki morajo DIW uporabnikom zagotoviti možnost, da podajo zavestno, namerno in dobro razumljivo privolitev za sprejem, uporabo in deljenje podatkov oziroma, možnost zavrnitve in preklica. V ta namen se lahko uporabijo pojavna polja, kot so polja z opozorilom, potrditvijo ali pozivom, ki od uporabnikov zahteva pregled podatkov pred potrditvijo transakcije. Uporabniki morajo biti informirani o identiteti entitet, s katerimi komunicirajo, o razlogu za deljenje podatkov, o vrsti operacije in pravici do varstva podatkov (GDPR) ipd.

Ključnega pomena je tudi funkcionalnost *(avtomatiziranega) varnostnega kopiranja in obnovitve*. V obstoječih DIW omenjena funkcionalnost temelji na šifriranju DIW z obnovitveno frazo, ki je potrebna pri obnovi. Pri tem predstavlja dobro prakso *kopiranje obnovitvene fraze z enim klikom* in njena *verifikacija* pred shranjevanjem. Verifikacija lahko temelji na označevanju navedenih besed ali njihovem vpisu, v ustreznem vrstnem redu, kar zmanjšuje strah pred morebitnimi napakami, ki bi uporabniku preprečile uspešno obnovitev ter s tem povezano izgubo podatkov. Varnostne kopije se shranijo lokalno ali v oblaku pri izbranem ponudniku, odvisno od preferenc uporabnika. Brez ustreznih mehanizmov varnostnega kopiranja in obnovitve lahko v primeru decentraliziranih in samoupravljanih

identitet uporabniki namreč v primeru težav (npr. izgubljen mobilni telefon, pozabljeno geslo za dostop do denarnice itn.) ostanejo brez vseh svojih podatkov ter so primorani začeti s ponovnim zbiranjem in izgradnjo digitalne identitete. V primeru uporabe mobilnih denarnic z lokalno shrambo je ključnega pomena tudi *možnost izvoza in uvoza* podatkov, ki omogoča možnost prenosa podatkov iz ene naprava in / ali denarnice v drugo, kar je skladno z načelom interoperabilnosti. Funkcionalnost, podobno kot varnostno kopiranje in obnovitev temelji na šifriranju najnovejše kopije denarnice, pri čemer mora biti izvedena manualno, na zahtevo uporabnika.

Shranjeni identifikatorji, kriptografski material, osebni podatki, dokumenti in poverilnice morajo biti v DIW pod popolnim nadzorom uporabnika, zaščiteni z eno izmed metod *overjanja*, ki ohranja varnost, zasebnost in preprečuje nepooblaščen dostop do podatkov v DIW ter izvedbo transakcij, ki vključujejo pridobivanje podatkov in poverilnic (VC), njihovo deljenje (VP) ter komunikacijo z drugimi entitetami. DIW lahko zahtevajo *overjanje pred dostopom* do podatkov in *overjanje ob potrditvi* pomembnih interakcij, kar uvaja dodaten sloj zaščite ter preprečuje zlorabe in napake pri rokovanju z občutljivimi podatki. Za overjanje se lahko uporabi biometrija, pin ali alfa-numerično geslo ter drugi mehanizmi overjanja.

Poleg omenjenega so lahko za zagotavljanje boljše uporabniške izkušnje določene akcije *avtomatizirane* na zahtevo uporabnikov. Kljub temu da morajo imeti uporabniki nadzor in možnost podati zavestno, namerno in dobro razumljivo privolitev za overjanje ter prejemanje in pošiljanje podatkov, je lahko izbira atributov in odobritev oz. zavrnitev vsake izmed interakcij z drugo entiteto za uporabnike časovno potratno ter lahko predstavlja nepotreben miselni napor, ki vodi v frustracijo in slabšo uporabniško izkušnjo. Ključnega pomena je tako možnost *avtomatizacije določenih interakcij*, pri čemer je pomembno, da uporabniki ohranjajo nadzor nad stopnjo avtomatizacije z upravljanjem nastavitev. Avtomatizirajo se lahko npr. sprejem povezav in poverilnic ter generiranje in deljenje predstavitev. Uporabniki lahko omogočijo npr. zgolj avtomatiziran sprejem povezav, ki se po skeniranju QR oznak samodejno shranijo v denarnico, ali zgolj sprejem poverilnic od določenih entitet, ki jim zaupajo. Pomembna je tudi avtomatizacija selektivne izbira podatkov, ki omogoča samodejno ustvarjanje predstavitev na podlagi zahtev preveriteljev. Uporabnikom tako ni potrebno iskati zahtevanih poverilnic in atributov, ampak je potreben zgolj njihov pregled in odobritev.



Slika 4: Funkcionalnosti digitalnih identitetnih denarnic.
Vir: lasten.

4.4 Scenariji uporabe

Obstajajo številni primeri uporabe DIW, ki nam omogočajo poenostavljeno identifikacijo, overjanje in dostopanje do različnih produktov in storitev ter nam nasploh olajšajo digitalne interakcije.

V nadaljevanju predstavljamo nekaj scenarijev, ki se osredotočajo na uporabo koncepta SSI ter temeljijo na uporabi DID-ov in VC-jev. Scenariji lahko pomagajo pri razumevanju samega koncepta DIW, prikazujejo uporabo funkcionalnosti ter nakazujejo na široko uporabnost takšnih denarnic.

Zaradi poenostavljene razlage scenarije predstavljamo preko fiktivne persone Ane, ki je zaključila študij na Fakulteti za elektrotehniko, računalništvo in informatiko na Univerzi v Mariboru (FERI UM) in pridobila naziv diplomirana inženirka informatike in tehnologij komuniciranja. Svoj študij želi nadaljevati v tujini, na Tehnični univerzi v Münchnu v Nemčiji (v nadaljevanju univerza). Z uporabo svoje digitalne identitete lahko prijavo opravi hitro in enostavno kar preko spleta, z uporabo svoje DIW, priznane s strani EU, ki si jo je namestila iz ene izmed trgovin z aplikacijami.

Ana preprosto obišče spletno stran univerze v Münchnu in izpolni prijavnico. V primeru izpolnjevanja prijavnice na računalniku se po potrditvi zgenerira QR oznaka, v kateri so šifrirani zahtevani podatki. Ana s svojim mobilnim telefonom skenira QR oznako in na tak način vzpostavi dvosmerno povezavo z univerzo, kar ji omogoči varno komunikacijo in izmenjavo podatkov, vse dokler je povezava vzpostavljena. Po skeniranju je Ana preusmerjena v denarnico, kjer izbere zahtevane dokumente oz. poverilnice, ki jih je predhodno pridobila od drugih (zaupanja vrednih) entitet, in jih sedaj želi deliti z univerzo. Izbere osebno izkaznico, ki jo je izdala Upravna enota Maribor, in diplomo, ki jo je izdal FERI UM ter preprosto potrdi prijavo. Ko univerza prejme Anino prijavo, se lahko začne avtomatiziran proces verifikacije poverilnic, ki vključuje preverjanje, ali so bile vse poverilnice izdane Ani, ali so v izvorni obliki in ali jih je izdala ustrezno akreditirana entiteta, ki ji univerza zaupa.

Univerza, ki nastopa v vlogi preveritelja je torej sposobna preveriti veljavnost poverilnic, njihov status, izdajatelje, imetnika identitete in trditve, ne da bi v sam proces morala vključevati izdajatelje poverilnic (FERI, Upravna enota Maribor).

Po uspešnem preverjanju lahko univerza potrdi Anino prijavo, o čemer je Ana obveščena preko potisnih obvestil, preko katerih je obveščena tudi ob uspešnem vpisu in ostalih pomembnih interakcijah.

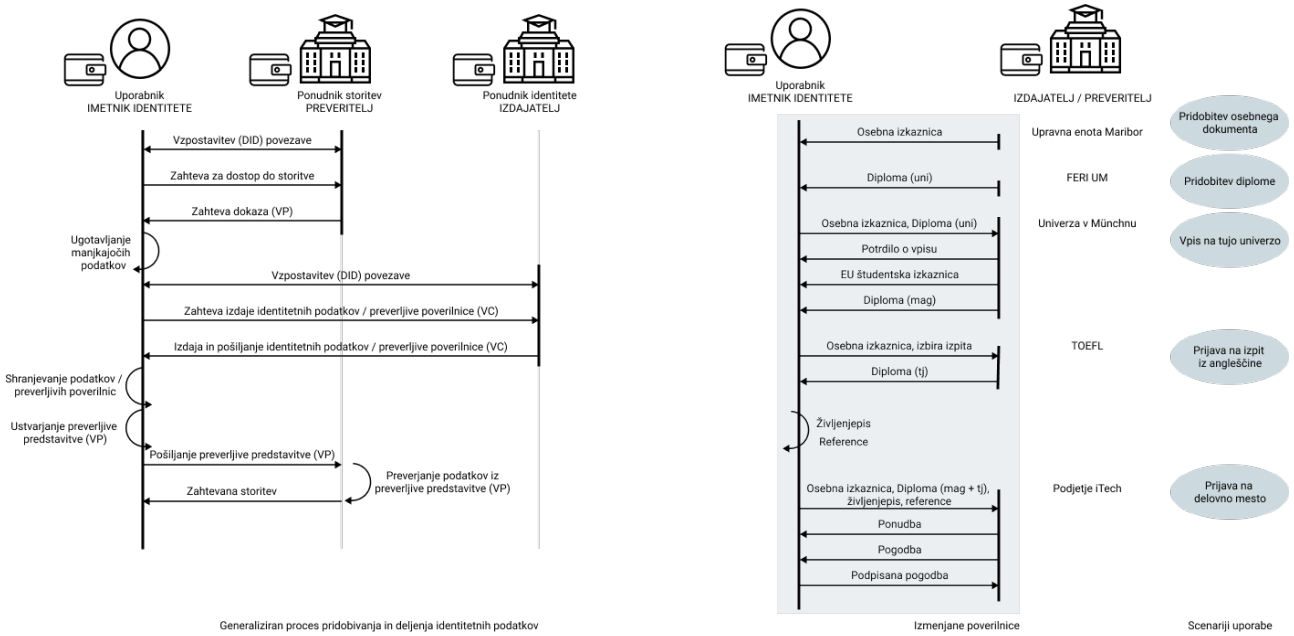
Poleg omenjenega vzpostavljena povezava omogoča tudi, da univerza Ani izda in posreduje različne poverilnice. Ana je tako preko potisnih obvestil obveščena o izdanem potrdilu o vpisu, evropski študentski izkaznici, diplomi itn., pri čemer more ponujene poverilnice pregledati in eksplicitno potrditi ali zavrniti njihov sprejem in shranjevanje v denarnico.

Po zaključku študija se Ana želi prijaviti na delovno mesto razvijalca spletnih aplikacij (v podjetju iTech). Potencialni delodajalec od nje zahteva predložitev dokazila o izobrazbi, dokazilo o opravljenem izpitu iz tujega jezika, življenjepis in reference. Ana, podobno kot pri vpisu na univerzo, obišče spletno stran podjetja, tokrat z mobilnim telefonom, zaradi česar je potreben zgolj klik na gumb za prijavo, ki omogoči vzpostavljanje povezave s podjetjem in Ano preusmeri v denarnico, kjer je obveščena o manjkajočih poverilnicah, ki jih mora pridobiti od ustreznih ustanov.

Ana se odloči za opravljanje spletnega izpita TOEFL. Obišče uradno spletno stran TOEFL in klikne na gumb za začetek procesa prijave, kar vzpostavi povezavo z organizacijo in jo preusmeri v denarnico, kamor prejme zahtevo za deljenje osebnih podatkov iz osebne izkaznice. Po potrditvi zahteve je Ana preusmerjena nazaj na spletno stran, kjer jo čaka izpolnjen prijavni obrazec s podatki iz deljene osebne izkaznice. Ani tako ni potrebno vnašati zahtevanih podatkov, izbrati mora zgolj izpit, ki ga želi opravljati ter potrditi prijavo. Po verifikaciji podatkov je Ana obveščena o terminu in načinu izvedbe izpita. Po uspešno opravljenem izpitu prejme obvestilo in diplomo, ki jo shrani v svojo denarnico.

Pred nadaljevanjem s procesom prijave na delovno mesto naloži še dokument z življenjepisom in ga digitalno podpiše ter samo-potrdi povezavo do spletne strani s svojimi referencami. Sedaj je pripravljena, da nadaljuje predhodno opisanim postopkom prijave. Vzpostavi povezavo, izbere zahtevane poverilnice ter potrdi prijavo.

Po verifikaciji poverilnic in po uspešnem razgovoru Ana prejme obvestilo o ponudbi in po njenem sprejemu še obvestilo o ponujeni pogodbi, ki jo digitalno podpiše, in s pomočjo denarnice posreduje svojemu novemu delodajalcu. Zaradi aktivne dvosmerne povezave lahko tudi v tem primeru od delodajalca prejme različne poverilnice.



Slika 5: V obeh primerih ponudnikov govorimo o klasičnih IT podatkov z uporabo DIW.
Vir: lasten.

V zgoraj opisanih scenarijih lahko opazimo podobnosti, zaradi česar lahko sam proces pridobivanja in deljenja identitetnih podatkov generaliziramo (Slika 5) in posledično apliciramo na mnoge druge primere uporabe.

Pred začetkom interakcije je potrebno vzpostaviti dvosmerno varno povezavo med vključenima entitetama. Ne glede na to, ali želi uporabnik zahtevati izdajo preverljive poverilnice ali želi dostopati do storitve, se mora najprej vzpostaviti komunikacijski kanal med denarnico uporabnika in denarnico druge entitete (izdajatelja ali preveritelja oz. ponudnika storitve).

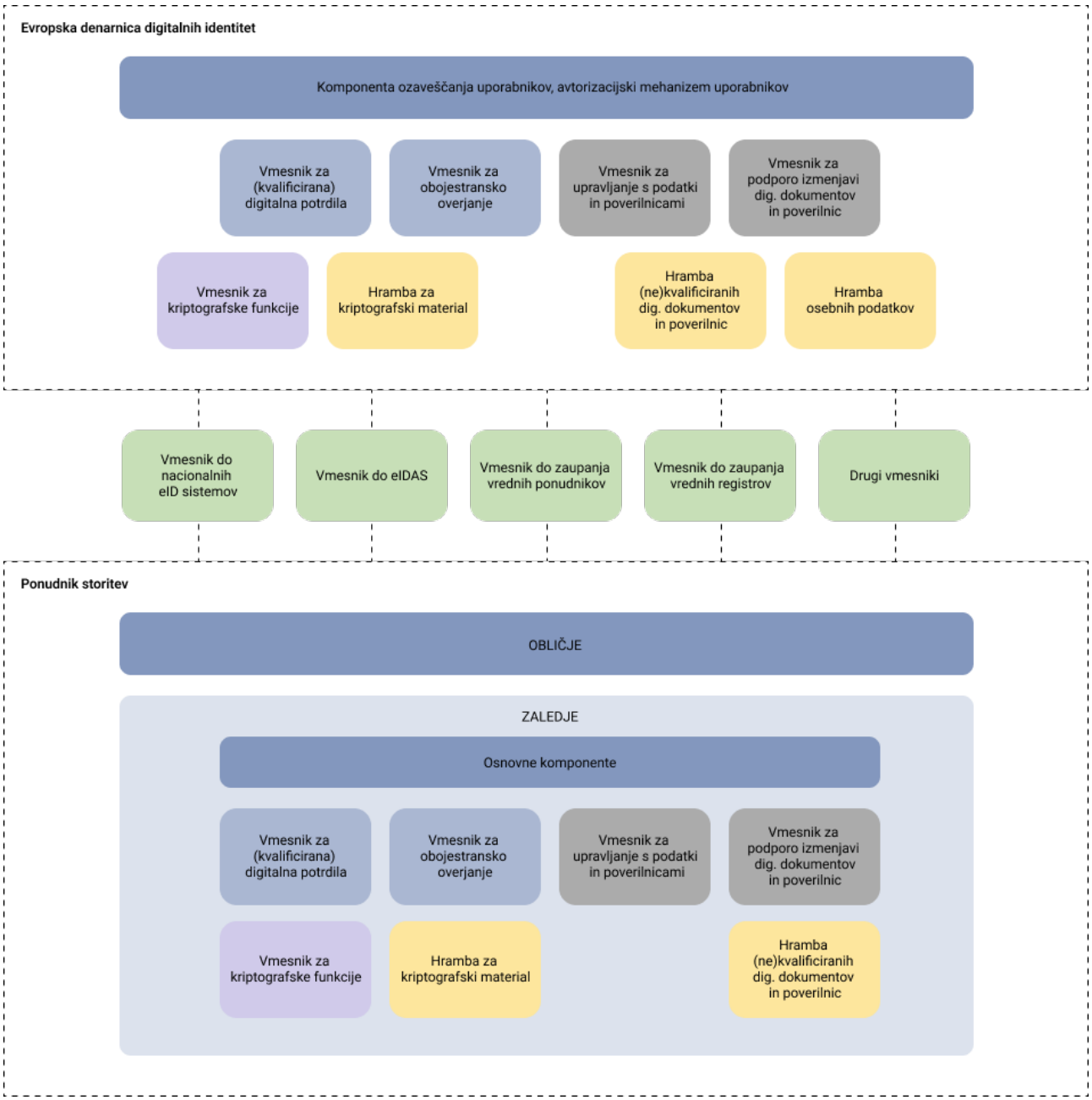
Po vzpostavljeni povezavi lahko uporabnik oz. imetnik identitete (i) zahteva dostop do produkta ali storitve, ali pa (ii) zahteva izdajo preverljive poverilnice, ki vsebuje enega ali več identitetnih atributov. (i) Pri pridobivanju dostopa do produkta ali storitve, tretja oseba oz. preveritelj običajno zahteva posredovanje dokazil/a (npr. potrdilo o izobrazbi oz. diploma itn.), kar omogoča identifikacijo in verifikacijo uporabnika. V primeru, da ima uporabnik v denarnici vse zahtevane poverilnice, lahko nadaljuje s postopkom, tako, da izbere in posreduje zahtevane identitetne atribute ali celotne poverilnice (odvisno od zahtev preveritelja). Uporabnik pravzaprav zgenerira t. i. preverljivo predstavitev (VP), ki omogoča selektivno izbiro in razkritje zgolj minimalne količine podatkov, potrebnih za posamezno interakcijo. (ii) V nasprotnem primeru mora uporabnik pridobiti ustrezne poverilnice (VC) od zaupanja vrednih izdajateljev. Poverilnice se nato shranijo v uporabnikovi digitalni denarnici, skupaj z identifikatorji ter jih je mogoče posredovati tretjim osebam na zahtevo.

5 Interakcija denarnice z obstoječimi IKT rešitvami

Četudi je na nivoju EK veliko fokusa na vpeljavi EUDIW, je razen dobro definiranih funkcijskih zahtev, še zmeraj veliko nejasnosti glede tehničnih podrobnosti. Februarja letos je EK izdala t. i. osnutek tehničnega ogrodja in referenčne arhitekture za Evropsko digitalno identiteto, ki pušča veliko odprtih vprašanj [24]. Osnutek referenčne arhitekture nam je služil kot osnova za visokonivojski pregled komponent in vmesnikov EUDIW ter ponudnikov storitev, ki je prikazan na sliki 6.

Upoštevajoč funkcijske zahteve EUDIW, mora ta zagotavljati v osnovi podporo upravljanju s kvalificiranimi digitalnimi potrdili ter po možnosti tudi nekvalificiranimi. Ideja je, da uporabnikom EUDIW omogoči, da jim le ta postane zamenjava za QSCD, pri čemer omogoča vse s tem že podprte funkcionalnosti, tj. digitalno (kvalificirano) podpisovanje, identifikacijo itn., in sicer tako na nacionalni kot čezmejni (EU) ravni. V ta namen je potrebna integracija vmesnikov za kvalificirana digitalna potrdila ter vmesnikov do nacionalnih eID sistemov in omrežja eIDAS. Kadar govorimo o ponudnikih storitev, velja izpostaviti, da v primeru zahtev po visoki zanesljivosti, ti že sedaj morebiti podpirajo možnosti identifikacije in overjanja na osnovi QR digitalnih potrdil, in sicer v povezavi s prej omenjenimi vmesniki za eID in eIDAS. Primeri takšnih ponudnikov storitev v Sloveniji so npr. AJPES, ki že sedaj omogoča vpis na osnovi SI-PASS. Primer uporabe nekvalificiranih digitalnih potrdil za identifikacijo pa je nekaj, kar je v Sloveniji prav tako že sedaj podprto na osnovi SI-PASS, saj omogoča ta identifikacijo tudi z nižjimi ravnmi zanesljivostmi (npr. na osnovi mreže AAI). Ne smemo pa zanemariti dejstva, da se EK poigrava tudi z idejami vpeljave konceptov SSI, pri čemer bi kvalificiranih ali nekvalificiranih digitalnih potrdil lahko zamenjali DID-i in / ali preverljive izkaznice (angl. Verifiable ID - VID). V tem primeru sta tako na strani EUDIW kot na strani ponudnika storitev nujno aktivirana vmesnika za obojestransko overjanje ter upravljanje s preverljivimi poverilnicami, kakor tudi vmesnik za kriptografske funkcije, ki omogoča upravljanje z DID-i, ter ob izdaji VC-jev tudi njihovo digitalno podpisovanje. S tem je tehnično povezano tudi dejstvo, da se lahko povezava in identifikacija na osnovi DID-ov vzpostavi tudi po protokolu DIDComm (po novem tudi DIDComm2) in v odvisnosti od uporabljene DID metode tudi s tem povezanimi mehanizmi za pridobitev DID dokumentov (npr. iz javnih verig blokov). Prav tako je sama inicializacija identifikacija in overjanja možna na podlagi generiranih in predstavljenih QR oznak, ki hranijo potrebne podatke za izvedbo procesa. Drug način je uporaba protokolov OpenID Connect (OIDC) ali SAML. Pri čemer slednji ne podpira DID-ov, medtem ko jih OIDC v določeni meri omogoča ter nudi tudi podporo izmenjavi VC-jev. Ravno vmesnik za podporo izmenjavi digitalnih dokumentov in VC-jev je tisti, ki nudi omenjeno podporo, pri čemer je v primeru uporabe SAML protokola za identifikacijo in overjanje, nujna namenska podpora izmenjavi na osnovi REST-a ali kaj temu podobnega. V vsakem primeru je ponudnik storitev tisti, ki bo s svojo infrastrukturo in z implementacijo vmesnikov moral podpreti omenjene možnosti.

Upravljanje s preverljivimi poverilnicami (VC) je prav tako ena od osnovnih funkcionalnosti, ki jih EUDIW morajo zadostiti. Za zagotavljanje takšne podpore je potrebno zagotoviti upravljanje z VC-ji na strani uporabnika kakor tudi izmenjavo teh med uporabnikom ter ponudnikom storitev oz. ponudnikom preverljivih poverilnic. V obeh primerih ponudnikov, govorimo o klasičnih IT arhitekturah, ki imajo svoja zaledja in obličja. Tako uporabnik v sklopu EUDIW, kakor tudi ponudniki morajo privzeto podpirati vmesnike za upravljanje z VC-ji in VP-ji. Med tem, ko EUDIW mora uporabniku nuditi možnost izbire VC-jev in generiranje VP-jev ob upoštevanju možnosti selektivnega razkritja, pa mora ponudnik storitev imeti možnost sprejeti VP-je ter jih temu primerno verificirati ter pregledati. Za namen selektivnega razkritja kakor tudi verifikacije VP-jev je potreben primeren vmesnik kriptografskih funkcij, saj se VC-ji in VP-ji primerno digitalno podpisujejo, pri čemer je le to ponovno odvisno od tega, ali bodo za generiranje VC-jev uporabljeni DID-i ali kvalificirani eID-ji kot osnovni identifikatorji. Vmesnik za kriptografske funkcije mora tako na strani ponudnika storitev podpreti preverjanje digitalnih podpisov, pri čemer bo v primeru uporabe DID-ov nujna povezava tudi z vmesniki zaupanja vrednih registrov, kot je npr. evropsko omrežje EBSI ali kaj podobnega. Omeniti je potrebno, da je v odvisnosti od izbire uporabljenih identifikatorjev, kakor tudi drugih komponent, potrebna temu primerna podpora posameznih kriptografskih funkcij, saj si le te niso med seboj kompatibilne. Prav tako je s tem povezana potrebna podpora hrambi kriptografskih materialov, in sicer od zasebnih ključev DID-ov do kvalificiranih digitalnih potrdil, v primeru, da se DID-i ne uporabljajo.



Slika 6: Visokonivojski pregled komponent in vmesnikov EUDIW ter ponudnikov storitev.
Vir: lasten.

Interakcije z EUDIW lahko temeljijo na več možnostih implementacije ob upoštevanju njihovega arhitekturnega ozadja in tehničnih podrobnosti. Te izvedbene možnosti lahko razdelimo na štiri ravni, tj. (1) identiteta, (2) overjanje, (3) komunikacija in (4) podatkovna plast.

(1) Prva raven se ukvarja z *digitalno identiteto* uporabnika EUDIW. Identiteto uporabnika je mogoče obravnavati na dva načina, tj. na osnovi nacionalnih eID ali eIDAS, ali na osnovi decentraliziranih identifikatorjev (DID). Če se uporabijo slednji, uporabnika, kot fizične osebe samega po sebi ni mogoče identificirati, saj zaradi skrbi glede zasebnosti dokumenti DID niso shranjeni na javno dostopni končni točki – v primeru DID-ov so to javno dostopne porazdeljene knjige.

(2) Druga raven je *raven overjanja*, ki se lahko spet razlikuje glede na izbiro izvedbe prve ravni in glede na uporabljeni postopek overjanja. Overjanje je tako mogoče izvesti z uporabo klasičnih protokolov, kot so SAML, ki je bolje integriran v poslovne rešitve ali z uporabo novejših protokolov, kot so OIDC. Izbira je odvisna od ravni zanesljivosti, ki jo postopek oz. ponudnik storitev zahteva. Prvi omogoča višjo raven zanesljivosti, drugi pa nižjo.

Vendar te možnosti niso edine. Če bi bili znotraj prve ravni uporabljeni DID-i, bi lahko overjanje bilo odvisno od dokumentov DID in / ali preverljivih poverilnic (VC). Zgolj uporaba DID-ov zadostuje, če je uporabnik pravna oseba in so njegovi DID dokumenti shranjeni in dostopni v javno dostopni porazdeljeni knjigi (tj. zaupanja vredni registri). DID dokumenti pravnih oseb lahko namreč poleg javnih ključev vsebujejo tudi druge določljive pravne podatke uporabnika. Če pa je uporabnik fizična oseba, mora biti postopek overjanja podprt s preverljivimi izkaznicami (VID), ki so sami po sebi QEAA v obliki VC, ki jih izdajo kvalificirani ponudniki identitete (angl. Qualified Identity Provider - QIdP). Kljub temu je treba upoštevati, da izvedbene možnosti druge ravni niso nujno vezane na izbiro prve ravni.

(3) Tretja raven je *komunikacijska* in ima dve možnosti implementacije, to je klasična SOAP komunikacija s pomočjo HTTP/S, kjer sta zahteva in odziv osnova za komunikacijo, druga možnost pa je DID-komunikacija (DIDComm), ki predstavlja dvosmerni komunikacijski kanal med dvema subjektoma, kjer deležnika poznata DID drug drugega.

(4) Zadnja raven je *podatkovna plast*, ki predstavlja obliko, v kateri se podatki izmenjujejo med obema stranema. V večini primerov je to XML, ki temelji na vnaprej določenih shemah XLS in je usklajen s strukturami SOAP/WSDL. Ta je bolj usklajen s trenutnimi poslovnimi sistemi. Vendar bo verjeten de facto format podatkov v prihodnosti VC v formatu JSON, ki je sam po sebi bolj usklajen s trenutnimi novimi koncepti IKT, kot so REST, mikrostoritve itd. Sam VC je standard W3C in lahko na osnovi definiranih shem podpira veliko podatkovnih vrst dokumentov, kot je QEAA ali kateri koli drug tip dokumentov. Matrica implementacijskih rešitev ni trdno definirana, saj je možnih več izbir glede na možnosti slojev, pri čemer je trenutno verjetno najbolj priročna možnost uporaba eID, SAML ali OIDC in VC.

6 Zaključek

Področje digitalnih identitet je v zadnjih letih ponovno pritegnilo pozornost stroke. Razlog temu so predvsem težnje po večji zasebnosti, kakor tudi uporabniški prijaznosti. V luči teh izzivov in požetih lovorik po vpeljavi GDPR se je EU s predlogom EK po novi uredbi v povezavi z Evropsko digitalno identiteto ponovno samozavestno postavila na globalno prizorišče kot vodilna na tem področju. Izziv, s katerim se EK sedaj sooča, je ta, da je za razliko od predlagane nove uredbe, GDPR sam po sebi ostal na nivoju regulatornih aktov in ni zahteval tehničnih rešitev oz. referenčnih IT arhitektur v že tako kompleksnem prostoru čezmejnih digitalnih identitet. Piko na i pa je dodalo še sunkovito razvijajoče se področje SSI, ki ponuja veliko uporabniško usmerjenih prednosti iz vidika zasebnosti, varnosti in prijaznosti, da se ga ne more ignorirati in ga je kljub nedozorelosti tehnologije, smiselno vključiti v potencialno referenčno IT arhitekturo, in s tem tudi v novo uredbo.

Če bo eIDAS 2.0 dobro implementiran, bo spremenil trenutni pristop k spletni varnosti, zasebnosti in uporabniški izkušnji evropskih državljanov ter se podobno kot GDPR na globalni ravni postavil kot vodilo. Učinkovito vpeljan eIDAS 2.0 bo na račun spodbujanja digitalne preobrazbe prihranil veliko časa in stroškov tako javnemu, kot tudi zasebnemu sektorju. EU si prav tako nadeja, da bo le ta spodbujal nove inovacije in morebitne nove samoroge (tokrat iz EU). Če pa bo eIDAS 2.0 na nivoju EU slabo načrtovan in vpeljan, se ne bo uveljavil, ne bo sprejet med državljani, in borci za zasebnost ga bodo raztrgali na koščke. Takšen morebitni izhod, ki si ga ne želimo, pa je tudi sam Avast slikovito opisal, kot "Velike IT korporacije in njihov nadzorni kapitalizem bosta zapolnila vakuum in prevladala".

Za ponudnike storitev in IKT sektor je smiselno dogajanje in razvoj budno spremljati in se počasi adaptirati v smer podpore EUDIW, ki se bo v roku dveh let izkristaliziral.

Literatura

[1] LAURENT Maryline, DENOUËL Julie, LEVALLOIS-BARTH Claire, WAELBROECK Patrick "1 - Digital Identity," Digital Identity Management, M. Laurent, S. Bouzefrane Ed., Elsevier, 2015, str. 1–45, doi: 10.1016/B978-1-78548-004-1.50001-8.

[2] B. Podgorelec, L. Alber, T. Zefferer, "What is a (Digital) Identity Wallet? A Systematic Literature Review," 2022, doi: 10.1109/COMPSAC54236.2022.00131.

[3] SCHARDONG Frederico, CUSTÓDIO Ricardo, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," Sensors 2022, letnik 22, številka 15, 2022, doi: 10.3390/s22155641.

[4] SEIGNEUR Jean-Marc, EL MALIKI Tewfiq, "Chapter 17 - Identity Management," Computer and Information Security Handbook, J. R. Vacca, Ed., Boston: Morgan Kaufmann, 2009, str. 269–292, doi: 10.1016/B978-0-12-374354-1.00017-0.

[5] SHENG Quan Z., QIN Yongrui, YAO Lina, BENATALLAH Boualem, "Chapter 14 - Security Issues of the Web of Things," Managing the Web of Things, Q. Z. Sheng, Y. Qin, L. Yao, B. Benatallah, Eds., Boston: Morgan Kaufmann, 2017, str. 389–424, doi: 10.1016/B978-0-12-809764-9.00018-4.

[6] SOLTANI Reza, NGUYEN Uyen Trang, AN Aijun, "Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets," 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2019, str. 320–325, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[7] AYDAR Mehmet, CETIN Salih Cemil, AYVAZ Serkan, AYGUN Betul, "Private key encryption and recovery in blockchain," 2019, doi: arXiv:1907.04156v2.

[8] SARTOR Sebastian, SEDLMEIR Johannes, RIEGER Alexander, HEIDI ROTH Tamara, "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets," Conference: 30th European Conference on Information Systems (ECIS 2022), 2022.

[9] NAIK Nitin, JENKINS Paul, "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2020, str. 90–95, doi: 10.1109/MobileCloud48802.2020.00021.

[10] https://www.w3.org/TR/vc-data-model/, SPORNY Manu, LONGLEY Dave, CHADWICK David, "Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web," 2021, obiskano 27. 7. 2022.

[11] https://www.w3.org/TR/did-core/, SPORNY Manu, LONGLEY Dave, SABADELLO Markus, REED Drummond, STEELE Orie, ALLEN Christopher, "Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations," 2022, obiskano 27. 7. 2022.

[12] LÓPEZ Marcos Allende, DA SILVA Marcelo, VEGEZZI, Alejandro Pardo, Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain, Inter-American Development Bank, 2020.

[13] XU Jie, XUE Kaiping, TIAN Hangyu, HONG Jianan, WEI David S. L., HONG Peilin, "An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks," IEEE Transactions on Vehicular Technology, letnik 69, številka 6, str. 6688–6698, 2020, doi: 10.1109/TVT.2020.2986041.

[14] TERZI Sofia, SAVVAIDIS Charalampos, VOTIS Konstantinos, TZOVARAS Dimitrios, STAMELOS Ioannis, "Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities,", 2020 IEEE International Conference on Blockchain (Blockchain), 2020, str. 462–469, doi: 10.1109/Blockchain50366.2020.00067.

[15] https://blog.avast.com/eidas-2.0-avast, TOBIN Andy, "eIDAS 2.0: How Europe can define the digital identity blueprint for the world," 2022, obiskano 27. 7. 2022.

[16] PODGORELEC Blaž, TURKANOVIĆ Muhamed, "ZKP (Zero-Knowledge Proof) pod drobnogledom," 2019, doi: 10.18690/978-961-286-282-4.12.

[17] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/eidas-regulations, Thales, "eIDAS 2: the countdown to a single European Digital ID Wallet has begun," 2022, obiskano 27. 7. 2022.

[18] https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS, KIROVA Marina, EICHHOLTZER Marie, "Overview of pre-notified and notified eID schemes under eIDAS," 2019, obiskano 27. 7. 2022.

[19] COHEN Sara, NUTT Werner, SAGIV Yehoshua, "Deciding equivalences among conjunctive aggregate queries," Journal of the ACM, letnik 54, številka 2, str. 5-es, 2007, doi: 10.1145/1219092.1219093.

[20] https://www.worldbank.org/content/dam/photos/1440x300/2022/feb/eID_WB_presentation_BS.pdf, STEFAN Bogdan, "Get to know ID used across borders in the European Union: An ID4D Webinar Series. A European Framework for Decentralized Digital Identity Wallets," 2022, obiskano 27. 7. 2022.

[21] https://www.cuatrecasas.com/en/latam/article/new-eidas-2-proposal-the-new-paradigm-of-european-digital-identification, MORGADO Claudia, "New eIDAS 2 proposal. The new paradigm of European Digital Identification," 2021, obiskano 27. 7. 2022.

[22] https://www.dw.com/en/eu-unveils-plan-for-new-digital-id-wallet/a-57769145, Deutsche Welle, "EU unveils plan for new digital ID wallet," 2021, obiskano 27. 7. 2022.

[23] MÜHLE Alexander, GRÜNER Andreas, GAYVORONSKAYA Tatiana, MEINEL Christoph, "A survey on essential components of a self-sovereign identity," Computer Science Review, letnik 30, str. 80–86, 2018, doi: 10.1016/j.cosrev.2018.10.002.

[24] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline, European Commission, "European Digital Identity Architecture and Reference Framework – Outline," 2022, obiskano 27. 7. 2022.

[25] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets, European Blockchain Partnership, "Conformant Wallets with EBSI," 2022, obiskano 27. 7. 2022.

[26] YUE Liu, LU Qinghua, PAIK Hye-Young, XU Xiwei and CHEN Shiping, ZHU Liming, "Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity," IEEE SOFTWARE, letnik 37, številka 5, str. 30–36, 2020, doi: 10.1109/MS.2020.2992783.

[27] https://www.investopedia.com/terms/d/digital-wallet.asp, KAGAN Julia, "Digital Wallet," 2022, obiskano 27. 7. 2022.

[28] https://www.zps.si/osebne-finance-sp-1406526635/10842-kaj-ponujajo-mobilne-denarnice-slovenskih-bank, MEŠKO Alina, "Kaj ponujajo mobilne denarnice slovenskih bank?", 2021, obiskano 27. 7. 2022.