Pot k uvedbi Evropske denarnice za digitalno identiteto

Davorka Šel, Aleš Pelan, Alenka Žužek Nemec

Ministrstvo za digitalno preobrazbo Republike Slovenije, Ljubljana, Slovenija
davorka.sel@gov,si, ales.pelan@gov.si, alenka.zuzek@gov.si

Prizadevanje za vzpostavitev evropskega okvira za digitalno identiteto je leta 2024 doprineslo do pomembnega koraka naprej, saj je 20. maja 2024 začela veljati novela EU uredbe št. 910/2014 za e-identifikacijo in storitve zaupanja, ki jo poznamo tudi kot Uredba eIDAS 2.0. Ta vzpostavlja pravno podlago za uvedbo evropske denarnice za digitalno identiteto po vsej EU. Z denarnico bodo uporabniki lahko tudi varno pridobili, shranili in delili svoje pomembne dokumente, npr. o izobrazbi in licencah, pooblastila za zastopanje pravnih oseb, finančne podatke in podatke o družbah, ter elektronsko podpisovali oz. v primeru denarnic za podjetja elektronsko žigosali dokumente. Da bi dosegli interoperabilnost med denarnicami, izdanimi s strani držav članic, so v izvedbenih aktih k Uredbi eIDAS 2.0 določeni standardi za evropsko denarnico, ki jih morajo upoštevati vse implementacije denarnic po državah, pravila za certificiranje denarnic in sporočanje Evropski komisiji. Skupne zahteve za denarnico se pripravljajo v okviru Arhitekturnega in referenčnega okvirja (ARF), poleg tega pa Evropska komisija pripravlja tudi referenčno implementacijo denarnice. V prispevku so podrobneje predstavljene nekatere visokonivojske zahteve ARF, ki se nanašajo na področje zasebnosti, še posebej uporaba metod ničelno spoznalnih dokazov (angl. Zero knowledge Proof) za zagotavljanje zasebnosti v ekosistemu denarnic.

Ključne besede:

elektronska identiteta,

eIDAS 2.0,

evropska denarnica za digitalno identiteto,

ničelno spoznalni dokaz,

javne storitve.

Univerzitetna založba Univerze v Mariboru

ISBN 978-961-299-037-4
DOI https://doi.org/10.18690/um.feri.7.2025.14

1 Uvod

Evropska komisija si že vrsto let prizadeva za vzpostavitev enotnega evropskega okvira za digitalno identiteto. Ključni preboj na tem področju predstavlja posodobitev Uredbe (EU) št. 910/2014 [1], znana kot eIDAS 2.0 [2], ki med drugim uvaja Evropsko denarnico za digitalno identiteto (EUDIW).

Uporabniki bodo lahko s pomočjo EUDIW hranili in delili različna dokazila o identiteti, kot so elektronski osebni dokumenti, potrdila o izobrazbi, zdravstvene podatke in drugo. Denarnica bo omogočala tudi elektronsko podpisovanje in avtentikacijo z visoko ravnjo zaupanja. Ključen pogoj za uspeh EUDIW je zagotavljanje visoke ravni varnosti in zasebnosti, zlasti v kontekstu izmenjave podatkov med državami članicami, uporabniki in različnimi ponudniki storitev.

Namen EUDIW ni le tehničen, saj gre za temeljni gradnik digitalne identitete posameznika, ki mu omogoča, da v različnih državah EU dostopa do storitev na način, ki je varen, nadzorovan in zagotavlja zasebnost. S tem se udejanja tudi eden izmed temeljnih ciljev evropskega notranjega digitalnega trga: odprava ovir za čezmejno digitalno poslovanje in komunikacijo.

2 Evropska denarnica za digitalno identiteto

EUDIW je osebna digitalna aplikacija s pripadajočimi zalednimi sistemi, ki državljanom Evropske unije omogoča, da varno in enostavno dostopajo do različnih digitalnih storitev v javnem in zasebnem sektorju po vsej EU. V skladu z Uredbo eIDAS 2.0 denarnica deluje kot standardizirano, certificirano in interoperabilno sredstvo, v katerem lahko posameznik shranjuje, upravlja in deli svojo elektronsko identiteto ter digitalne dokumente oz. digitalna potrdila o atributih – kot so dokazila o izobrazbi, licencah, poklicnih pooblastilih, bančnih računih ali pravnih zastopanjih. Denarnica uporabniku omogoča elektronsko podpisovanje dokumentov ter dokazovanje identitete in pravic na način, ki zagotavlja visoko raven varnosti in zasebnosti. Ključna prednost EUDIW je, da je zasnovana z načelom "najmanjše nujne informacije", kar pomeni, da lahko uporabnik sam odloča, katere podatke bo delil in v kakšnem obsegu. Ta pa je pogosto brez razkritja celotne vsebine potrdila. Funkcionalnost temelji na uporabi naprednih kriptografskih tehnik, kot je metoda ničelno spoznalnih dokazov (angl. Zero-Knowledge Proof oz. ZKP), ki omogoča preverjanje trditev brez razkritja podatkov. Poleg tega EUDIW temelji na skupnih standardih, ki zagotavljajo medsebojno delovanje denarnic različnih držav članic in skladnost z zakonodajo o varstvu osebnih podatkov. S tem postavlja temelje za zanesljivo, zasebnosti prijazno in vključujočo digitalno družbo prihodnosti.

2.1. Pravni okvir

Uredba eIDAS 2.0 [2], ki je bila sprejeta maja 2024, predstavlja prelomnico v razvoju digitalne identitete v Evropski uniji. Nadgrajuje in razširja izhodišča prvotne uredbe eIDAS [1] iz leta 2014, ki je vzpostavila temelje za čezmejno priznavanje sredstev elektronske identifikacije in storitev zaupanja. Novela uredbe uvaja ambiciozen cilj: vzpostavitev univerzalno dostopne, varne in zasebnosti prijazne evropske digitalne denarnice, ki jo bodo lahko uporabljali vsi prebivalci in podjetja v državah članicah EU. Uredba uvaja pravico vsakega državljana do brezplačne denarnice. Ta denarnica bo omogočala ne le preverjanje identitete, temveč tudi upravljanje z elektronskimi potrdili o atributih, uporabo za elektronsko podpisovanje in nadzorovano deljenje osebnih podatkov. Uredba določa, da mora biti denarnica zagotovljena brezplačno za fizične osebe in da mora biti interoperabilna s sistemi drugih držav EU. Poleg tehničnih zahtev uvaja tudi stroge pogoje glede varnosti, upravljanja s podatki in vloge deležnikov. Uredba daje poseben pomen uporabniški izkušnji, zato predvideva tudi minimalne standarde za dostopnost, prenosljivost in nadzor nad podatki. Uredba vzpostavlja tudi okvir za nadzor, poročanje in certifikacijo storitev in tehnologij EUDIW, s čimer želi zagotoviti trajnostno, zaupanja vredno in tehnološko odprto digitalno okolje.

eIDAS 2.0 torej ni le pravna podlaga, ampak tudi jasna razvojna vizija digitalne Evrope, ki temelji na zaupanju, zasebnosti in tehnični odličnosti.

Pravni okvir vključuje tudi stroge določbe o varstvu osebnih podatkov, kjer se eIDAS 2.0 neposredno navezuje na Splošno uredbo o varstvu podatkov (GDPR) [3]. Vsak obdelovalec ali izdajatelj podatkov mora ravnati v skladu z načelom minimizacije podatkov, zakonitosti in preglednosti obdelave.

Na podlagi uredbe so bili sprejeti tudi izvedbeni akti, ki opredeljujejo tehnične standarde, varnostne protokole, certifikacijske postopke in načine preverjanja skladnosti, ki služijo kot temelj za konkretno implementacijo digitalne denarnice. Izvedbeni akti se naslanjajo na Arhitekturni in referenčni okvir, ki podaja zahteve za implementacijo EUDIW. Z uveljavitvijo prvega paketa izvedbenih aktov, ki določa pravila za osnovne funkcionalnosti denarnic in njihovo certificiranje. je začel veljati tudi zakonski rok za uvedbo denarnic s strani držav članic, ki je 24. december 2026. Drugi paket izvedbenih aktov, poveznih z denarnico, naslavlja , , seznam certificiranih evropskih denarnic za digitalno identiteto, odzivanje na kršitve varnosti evropskih denarnic, registracijo na denarnice zanašajočih se strank in čezmejno ujemanje identitete fizičnih oseb je bil objavljen 6. maja 2025, razen akta z zahtevami za ponudnike elektronskih potrdil o atributih. Objava tega akta se pričakuje do septembra 2025.

Države članice pa morajo na podlagi Uredbe eIDAS 2.0 in spremljajočih izvedbenih aktov tudi opredeliti obveznosti v svoji nacionalni zakonodaji, da omogočijo uvedbo EUDIW.

2.2. Arhitektura in referenčni okvir (ARF)

Evropska komisija je v pomoč državam pri implementaciji EUDIW objavila Arhitekturni in referenčni okvir (ARF) [4], ki določa visokonivojske zahteve za vse implementacije v okviru ekosistema EUDIW.

ARF predstavlja osrednji tehnični dokument Evropske komisije, katerega namen je usmerjati razvoj, uvedbo in interoperabilnost EUDIW. Evropska komisija ga oblikuje v sodelovanju z organi za standardizacijo, industrijskimi konzorciji in predstavniki držav članic. ARF sicer ni pravno zavezujoč dokument, a je zaradi svoje povezave z eIDAS 2.0 in izvedbenimi akti, na katere vpliva, de facto standard, katerega uporaba je za države članice nujna za zagotovitev interoperabilnosti in enotne uporabniške izkušnje. ARF vključuje sistemski pogled na vse ključne komponente in vloge v ekosistemu elektronskih denarnic, vključno z EUDIW, izdajatelji identitet in atributov, ponudniki storitev ter varnostnimi komponentami, kot so varni kriptografski moduli. Poleg funkcionalnih zahtev definira tudi tehnične protokole, specifikacije vmesnikov, vrste in formate potrdil, načine preverjanja in prenosa podatkov, ter priporočene kriptografske algoritme.

Dokument je strukturiran tako, da omogoča prilagodljivo implementacijo, ki upošteva različne nacionalne pristope in obstoječe tehnične zmogljivosti, hkrati pa zagotavlja interoperabilnost na evropski ravni. ARF se osredotoča tudi na življenjski cikel EUDIW, od inicializacije do ponovne uporabe in preklica, ter vključuje napredne koncepte, kot so mehanizmi zaščite pred sledenjem uporabnikov. Pomemben del ARF predstavljajo tudi tokovi informacij med deležniki, ki so jasno opisani skozi komunikacijske scenarije in uporabniške tokove, vključno z vlogami ponudnika identitete, ponudnika potrdil o atributih in drugih zanašajočih strank.

Zaradi nenehnega tehnološkega razvoja se ARF redno posodablja, kar omogoča vključevanje novih rešitev in postopno nadgrajevanje obstoječih sistemov.

Ključno sporočilo ARF je, da tehnična interoperabilnost ni dosegljiva le s spoštovanjem minimalnih zahtev, temveč z aktivnim sodelovanjem držav članic, standardizacijskih teles in industrije, pri čemer mora biti vedno v ospredju uporabnik in varovanje njegove zasebnosti.

2.3. Referenčna implementacija in standardizacija

Evropska komisija poleg ARF aktivno razvija tudi referenčno implementacijo EUDIW. Njena glavna naloga je podpreti države članice pri razvoju lastnih nacionalnih rešitev, zagotoviti minimalne funkcionalnosti, preveriti skladnost s tehničnimi zahtevami in olajšati doseganje čezmejne interoperabilnosti. Referenčna implementacija ni obvezna za uporabo, vendar služi kot osnovni vzorec oziroma dokaz koncepta, ki upošteva vse bistvene komponente ARF. S tem omogoča testiranje in integracijo z različnimi deležniki v ekosistemu, kot so ponudniki identitet, izdajatelji potrdil o atributih in ponudniki storitev.

Ob tem imajo standardi v ekosistemu evropske denarnice za digitalno identiteto ključno vlogo pri zagotavljanju skladnosti, varnosti in interoperabilnosti. Brez skupno dogovorjenih specifikacij bi vsak ponudnik in vsaka država lahko razvijala rešitve, ki bi bile medsebojno nezdružljive, kar bi neposredno ogrozilo uspešnost EUDIW. Zato Evropska komisija v tesnem sodelovanju z evropskimi in mednarodnimi standardizacijskimi telesi (npr. ETSI, CEN, ISO, W3C) pripravlja nabor tehničnih standardov, ki vključujejo definicije struktur elektronskih potrdil, varnostne protokole, kriptografske algoritme, formate potrdil o atributih in komunikacijske protokole med komponentami sistema.

Posebno pomembni so standardi, ki omogočajo selektivno razkritje podatkov, zaščito pred sledljivostjo ter uporabo varnih kriptografskih aplikacij in naprav. Prav tako so določeni tudi varnostni profili za mobilne naprave in zahteve glede certificiranja programske ter strojne opreme. Ključno pri tem je, da vsi standardi niso le tehnične narave, ampak zajemajo tudi organizacijske in upravljavske vidike, kot so postopki izdaje in preklica potrdil, beleženje revizijskih sledi ter mehanizmi za obvladovanje incidentov. Referenčna implementacija tako služi kot laboratorij za uveljavljanje teh standardov v praksi, kar je bistven korak za uspešno implementacijo nacionalnih denarnic. Le s skupno uporabo odprtih, preverljivih in široko sprejetih standardov bo mogoče zagotoviti, da bo EUDIW resnično delovala kot zanesljivo, varno in univerzalno orodje za digitalno identiteto med državami članicami.

2.4. Ekosistem evropske denarnice za digitalno identiteto

Ekosistem EUDIW je kompleksen in večslojen sistem, v katerem sodelujejo številni akterji, vsak z jasno določeno vlogo in odgovornostmi. Arhitektura sistema EUDIW temelji na modularnem in decentraliziranem modelu, ki omogoča interoperabilno delovanje različnih nacionalnih rešitev znotraj enotnega evropskega okvira.

Slika 1 prikazuje poenostavljeno arhitekturo ekosistema EUDIW s ključnimi deležniki in tokovi podatkov med njimi. V jedru ekosistema je komponenta same denarnice, ki jo uporabnik uporablja za hranjenje osebnih podatkov, elektronskih potrdil o atributih in za izvajanje elektronskih transakcij, kot so prijava v spletne storitve, dokazovanje lastnosti ali elektronsko podpisovanje dokumentov. Denarnico izdaja zaupanja vreden *ponudnik denarnice* v skladu s pravnim okvirjem iz poglavja 2.1.

Temeljni akter v ekosistemu je tako imenovani ponudnik identitet (ang. Person Identification Data Provider, v nadaljevanju *ponudnik PID*), ki je običajno državni organ in skrbi za izdajo osnovne digitalne identitete uporabniku. Ta identiteta vključuje podatke, kot so ime, priimek, datum rojstva, kraj rojstva in državljanstvo, ki tvorijo osnovo za preverjanje posameznika. Poleg ponudnika PID v ekosistemu sodelujejo tudi ponudniki elektronskih dokumentov oz. *ponudniki elektronskih potrdil o atributih* (angl. Attestation Providers), kot so državni organi, izobraževalne institucije, poklicne zbornice, delodajalci ali drugi organi, ki potrjujejo dejstva o uporabniku, npr. izobrazbo, licenco, pravico do zastopanja podjetja ipd. Medtem ko elektronska potrdila za podpisa izdaja *ponudnik kvalificiranih potrdil za elektronski podpis*. V podporo celotnemu ekosistemu so vzpostavljeni tudi varnostne komponente, kot so varne kriptografske naprave (angl. wallet secure cysptographic device - WSCD), ki zagotavljajo, da so zasebni ključi in občutljivi podatki zaščiteni na ustrezni ravni, ter orodja za upravljanje življenjskega cikla potrdil, njihovo preklicevanje in ponovno izdajo.

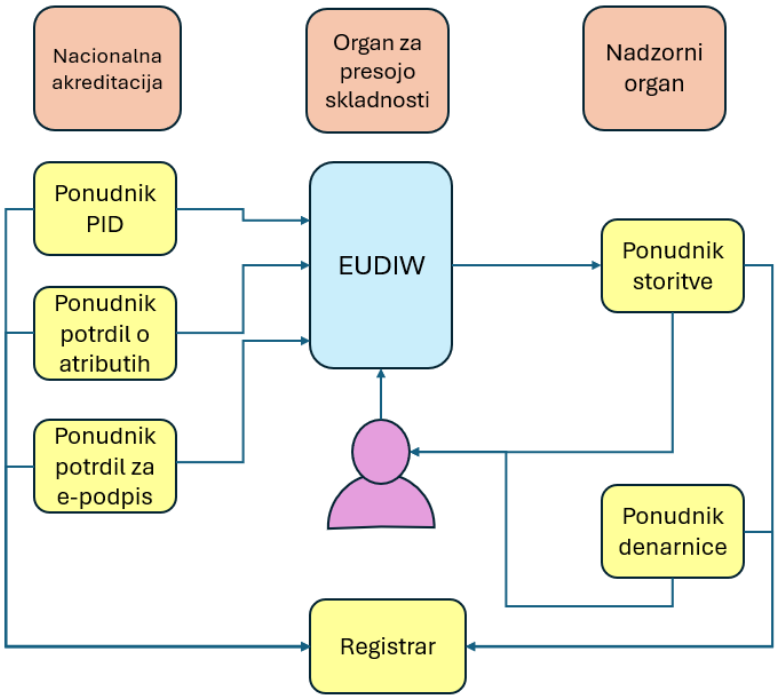
Na drugi strani so *ponudniki storitev* (angl. Relying Parties), ki dostopajo do uporabnikovih podatkov preko standardiziranih protokolov in vmesnikov. Vsa komunikacija med temi akterji poteka prek varnih protokolov, ki vključujejo identifikacijo, preverjanje pristnosti, prenos selektivno razkritih podatkov ter uporabo podpisov.

Pomembno vlogo igra tudi *registrar*. Registrar je odgovoren za preverjanje identitete zanašajočih strank in potrditve seznama atributov, do katerega lahko dostopajo, preden izda potrdilo zanašajoči stranki (angl. access certificate), da se lahko vključi v ekosistem.

Na najvišji ravni nadzora in zagotavljanja skladnosti nad sistemom so *slovenska akreditacija, nacionalni nadzorni organ, upravljavec certifikacijske sheme, organ za presojo skladnosti*. Organ za presojo skladnosti skrbi za presojo skladnosti in varnosti EUDIW v ekosistemu. Ta organ izvaja certifikacijo EUDIW na podlagi nacionalne certifikacijske sheme s čimer zagotavlja, da so tehnične rešitve skladne z zahtevami eIDAS 2.0, ARF in relevantnimi varnostnimi standardi ter potrjuje skladnost komponent (denarnic, WSCD modulov, …) s tehničnimi in varnostnimi zahtevami, opredeljenimi v nacionalni shemi. Poleg tega arhitektura vključuje tudi upravljavske mehanizme, kot so beleženje transakcij, upravljanje soglasij uporabnikov, sistemi za obvladovanje incidentov ter mehanizmi za preklic in ponovno izdajo potrdil.

Vzpostavljena je hierarhija zaupanja, kjer nacionalni nadzorni organi nadzirajo delovanje ponudnikov v državi, Evropska komisija pa vzdržuje nadzor nad usklajenostjo celotnega sistema. Sistem mora podpirati tudi različne uporabe – od spletnih prijav in podpisovanja do uporabe v fizični prisotnosti (angl. proximity use), pri čemer mora vsak podatek biti predstavljen v kriptografsko zaščiteni, preverljivi in zanesljivi obliki.

V arhitekturnem smislu gre torej za porazdeljen sistem, v katerem so vsi akterji med seboj povezani preko standardiziranih tehničnih protokolov in se zanašajo na enoten varnostni model. Poudarek na decentralizaciji, interoperabilnosti in varstvu podatkov uporabnika predstavlja temeljno razliko v primerjavi z dosedanjimi centraliziranimi sistemi identitet, kar EUDIW postavlja kot inovativno, zaupanja vredno in trajnostno rešitev v evropskem digitalnem prostoru.



Slika 1: Poenostavljena arhitektura ekosistema EUDIW.

2.5. Izzivi interoperabilnosti

Vzpostavitev ekosistema EUDIW temelji na ideji čezmejne uporabnosti in enotne uporabniške izkušnje, ne glede na državo članico, v kateri je bila denarnica izdana. Vendar pa to zahteva izjemno visoko stopnjo tehnične in organizacijske usklajenosti, kar predstavlja enega največjih izzivov v trenutni fazi uvajanja. Interoperabilnost pomeni, da sistemi različnih držav medsebojno razumejo podatkovne strukture, protokole, varnostne zahteve in postopke preverjanja, kar pa je težko doseči ob dejstvu, da imajo države različne tehnične zmogljivosti, obstoječe nacionalne sheme e-identitet in zakonodajne posebnosti. Nekatere države razvijajo EUDIW na podlagi referenčne implementacije, druge pa vzpostavljajo povsem nove platforme, kar lahko privede do razlik med implementacijami.

Poleg tehničnih razlik obstajajo tudi neenotnosti v razumevanju pravnih zahtev uredbe eIDAS 2.0 in izvedbenih aktov. Pomanjkanje končnih standardov in zamude pri potrjevanju tehničnih specifikacij še dodatno otežujejo prizadevanja držav, da bi začele pravočasno testiranje in integracijo svojih rešitev. Pomanjkanja končnih standardov in specifikacij zlasti na področjih formatov potrdil, primernosti WSCD, protokolov za predstavitev podatkov in zagotavljanja zasebnosti pri uporabi denarnice bistveno otežuje nadaljnji razvoj denarnic. Poleg tega obstajajo tudi izzivi glede vključevanja ponudnikov storitev in ponudnikov potrdil o atributih, ki morajo biti tehnično in pravno usposobljeni za sodelovanje v ekosistemu.

Interoperabilnost pa ni odvisna le od enotnih specifikacij, temveč tudi od ustrezne razpoložljivosti testnih okolij, učinkovitega certificiranja in natančno opredeljenih vlog v ekosistemu. Pomembno je tudi zagotoviti, da bodo implementacije denarnic, ki temeljijo na referenčni implementaciji ali neodvisnih rešitvah, sposobne varnega preverjanja in predstavitve podatkov ne glede na državo ali tip ponudnika storitve. Evropska komisija poskuša s pomočjo pilotnih projektov, ko so POTENTIAL [5], v katerem sodeluje tudi Slovenija ter EU Digital Wallet Consortium (EWC) [6], Nobid [7] in DC4EU [8], zagotoviti podporo državam pri razvoju interoperabilnih rešitev. Kljub temu pa se izkušnje iz teh projektov še niso povsem prenesle v enotno prakso.

Na dolgi rok bo uspeh EUDIW močno odvisen od tega, ali bo mogoče zagotoviti neprekinjeno sodelovanje med regulatorji, razvijalci, ponudniki storitev in uporabniki. Interoperabilnost ne pomeni le tehnične usklajenosti, temveč zahteva tudi vzpostavitev trajnih mehanizmov sodelovanja, izmenjave znanja in skupnega nadzora nad kakovostjo storitev. Zato je bistveno, da se interoperabilnost razume kot dinamičen proces, ki ga bo treba redno nadgrajevati in prilagajati novim razmeram, tehnologijam in uporabniškim pričakovanjem.

3 Elektronska potrdila o atributih in vloga njihovih ponudnikov

Elektronska potrdila o atributih so temeljni gradniki ekosistema EUDIW, saj omogočajo prenos zaupanja iz preverjenih virov na način, ki je strojno berljiv, interoperabilen in varen. Atributi predstavljajo značilnosti posameznika ali organizacije, kot npr. da ima vozniško dovoljenje, končano izobrazbo, stalno bivališče, pooblastilo za zastopanje podjetja, poklicne kvalifikacije, članstvo v zbornici, davčno številk, ipd. Ti atributi so shranjeni v obliki strukturiranih podatkovnih zapisov, ki jih izdajajo zaupanja vredne ustanove. Ključni element sistema je, da uporabnik lahko te podatke hrani v svoji denarnici in jih po potrebi predstavi različnim ponudnikom storitev, ne da bi ob tem razkril prekomerne količine osebnih podatkov oz. uporabi t.i. selektivno razkritje atributov [9].

Osrednjo vlogo pri izdaji osnovne digitalne identitete ima ponudnik PID. Ponudnik PID zagotovi temeljno identiteto uporabnika, ki je podlaga za izdajanje drugih potrdil. Vzporedno z njim delujejo izdajatelji drugih potrdil o atributih kot so univerze, zdravstvene ustanove, poklicne zbornice, podjetja in druge institucije, ki so pooblaščene za potrjevanje specifičnih dejstev o posamezniku. Ta dva tipa izdajateljev se razlikujeta predvsem po obsegu odgovornosti in naravi podatkov, ki jih potrjujeta, vendar morata oba zagotavljati visoko stopnjo zaupanja, doslednost pri izdaji in skladnost s predpisi uredbe eIDAS 2.0 ter splošno uredbo o varstvu podatkov GDPR.

Pomembno je, da se vsa potrdila izdajo v skladu s standardi, opredeljenimi v izvedbenih aktih in ARF, ter da se omogoči njihova poznejša ponovna izdaja brez ogrožanja zasebnosti. To pomeni, da mora biti proces obnove

potrdil možen brez potrebe po celoviti ponovni registraciji uporabnika, kar zahteva zanesljivo vezavo potrdil na identiteto, ne da bi se pri tem razkrile nepotrebne informacije. Zanesljivost in razširjenost potrdil o atributih sta neposredno odvisni od tehnične in organizacijske usklajenosti ponudnikov. Zato se znotraj ARF natančno opredeljujejo formati potrdil, življenjski cikel izdajanja in preklica, možnosti ponovne izdaje ter postopki preverjanja veljavnosti. Poleg tega morajo biti izdajatelji vključeni v mehanizme, ki omogočajo interoperabilnost na ravni EU, kar vključuje registracijo, certificiranje in obveščanje o izdanih oziroma preklicanih potrdilih. Elektronska potrdila o atributih tako ne predstavljajo zgolj digitalne različice papirnih dokumentov, temveč omogočajo bolj finozrnat, varnejši in nadzorovan način izmenjave informacij, ki je nujen za vzpostavitev zaupanja vrednega digitalnega okolja v Evropi.

Zaradi potrebe po visoki ravni zaščite podatkov je nujno, da tako ponudnik PID kot ponudniki potrdil o atributih delujejo v skladu s predpisi o varstvu osebnih podatkov (GDPR) in uporabljajo tehnike, kot je ZKP.

4 ZKP kot temelj za varovanje zasebnosti v EUDIW

ARF namenja posebno pozornost zaščiti zasebnosti uporabnikov. Eden ključnih mehanizmov za doseganje tega cilja je uporaba kriptografskih metod ZKP. ZKP predstavlja sredstvo, s katerim lahko uporabnik EUDIW dokaže določeno lastnost (npr. da je polnoleten ali da ima določeno licenco) brez razkritja same vrednosti atributa ali dodatnih podatkov.

Pomembna prednost ZKP je tudi preprečevanje povezljivosti med različnimi transakcijami uporabnika. Če bi uporabnik za vsako storitev vedno znova razkrival iste identifikacijske podatke, bi to omogočilo sledenje in profiliranje. Z ZKP pristopi pa lahko vsakokrat ustvari edinstven dokaz, ki ne razkriva identitete in ne omogoča povezovanja različnih transakcij. Tako se bistveno izboljša varstvo zasebnosti in zmanjša tveganje zlorabe osebnih podatkov.

Tehnologija ZKP pa ne pomeni le prednosti za uporabnika. Tudi ponudniki storitev imajo od nje koristi, saj jim omogoča zanesljivo preverjanje pogojev brez potrebe po shranjevanju ali obdelavi osebnih podatkov. To zmanjšuje obremenitve glede skladnosti z GDPR, saj ponudniki ne prevzemajo odgovornosti za varovanje podatkov, ki jih sploh ne prejmejo. Poleg tega ZKP odpira vrata za uporabo EUDIW v sektorjih, kjer je varovanje zasebnosti še posebej pomembno – na primer v zdravstvu, financah ali pri glasovanju na daljavo.

Izvedba ZKP v evropskem kontekstu pa prinaša tudi svojevrstne izzive. Tehnologija mora biti standardizirana, preverljiva in izvedljiva v vseh državah članicah. Zahteva tudi močno podporo na ravni infrastrukture, vključno z varnimi kriptografskimi napravami in digitalnimi podpisi, ki zagotavljajo integriteto dokazov. V okviru delovnih skupin Evropske komisije se pripravljajo visoko nivojske zahteve, ki pa še niso potrjene. Končne verzije zahtev bodo objavljene v eni naslednjih verzij ARF. V nadaljevanju pa je podanih nekaj kandidatov zahtev iz delovnega dokumenta Evropske komisije [10] za vključitev v ARF:

- *Temeljne funkcije ZKP*: Shema ZKP mora omogočati dokazovanje prisotnosti atributov v PID ali potrdilih, njihove veljavnosti, nepreklicanosti in vezave na WSCD, pri čemer so vsi atributi skriti. Poleg tega naj podpira možnost prikritja izdajatelja potrdila.
- *Dokaz posedovanja*: Shema mora omogočati dokazilo, da uporabnik razpolaga z določenim tipom potrdila.
- *Zasebna vezava*: ZKP naj omogoča zasebno povezovanje PID in potrdila, tako da dokaže prisotnost istega atributa v obeh.
- *Psevdonimi*: Shema naj omogoča ustvarjanje preverljivih psevdonimov, izpeljanih iz tajnega atributa in identifikatorja ponudnika storitve, brez razkritja samega atributa.

- *Uporabnost v različnih kontekstih*: ZKP mora biti uporabna v bližnjih (npr. osebna prisotnost) in oddaljenih (npr. spletna storitev) scenarijih, brez bistvenega vpliva na uporabniško izkušnjo.
- *Združljivost z obstoječimi formati*: Naj omogoča dokazovanje nad PIDs in potrdili v formatih ISO/IEC 18013-5 in SD-JWT VC.
- *Brez sledenja*: ZKP ne sme uvajati nobenih komunikacij ali metapodatkov, ki bi omogočali sledenje uporabniku.
- *Standardizirani algoritmi*: Vsi uporabljeni algoritmi morajo biti standardizirani pri telesih, ki jih priznava Evropska komisija.
- *Skladnost z visoko ravnjo zanesljivostjo*: Uporaba ZKP ne sme ovirati zagotavljanja visoke ravni zanesljivosti avtentikacije uporabnika.

4.1. Implementacija in uporaba ZKP v EUDIW

Obstajata dva prevladujoča pristopa k ZKP, ki se obravnavata v okviru procesa priprave zahtev ARF: to sta BBS+ in zk-SNARK. Prvi omogoča ustvarjanje več-sporočilnega podpisa, pri katerem je mogoče razkriti le podmnožico podatkov iz posameznega sporočila, hkrati pa ohraniti dokaz o pristnosti celote. Entiteta, ki pozna podpis in izvirni niz podpisanih sporočil, lahko ustvari dokaz s katerim razkrije samo podmnožico teh sporočil. Tak dokaz je mogoče preveriti zgolj z uporabo javnega ključa podpisnika in razkritih sporočil iz te podmnožice. BBS+ velja za bolj primernega za okolja z omejenimi viri, kot so mobilne naprave, saj ne zahteva visoke računske moči, vendar pa zahteve spremembe v procesu podpisovanja potrdil o atributih. Po drugi strani pa zk-SNARK temelji na dokazovanju veljavnosti trditev z uporabo aritmetičnih vezij in ponuja visoko stopnjo prilagodljivosti. Omogoča dokazovanje kompleksnih pogojev (npr. dohodek nad določenim pragom), pri čemer so vhodni podatki popolnoma skriti.

Tabela 1 prikazuje razlike med tehnologijama ZKP, ki sta kandidata za uporabo v kontekstu EUDIW.

Tabela 1: Primerjava BBS+ in zk-SNARK pristopov.

4.1.1.	**Lastnost**	**4.1.2.**	**BBS+**	**4.1.3.**	**Zk-SNARK**
4.1.4.	**Selektivno razkritje**	4.1.5.	DA	4.1.6.	DA
4.1.7.	**Podpora za kompleksne trditve**	4.1.8.	NE	4.1.9.	DA
4.1.10.	**Računska zahtevnost**	4.1.11.	NIZKA	4.1.12.	VISOKA
4.1.13.	**Zahteva začetni setup**	4.1.14.	NE	4.1.15.	OBIČAJNO DA

Vir: G - Zero Knowledge Proof (delovni dokument) [6]

Tabela kaže, da je izbira tehnologije močno odvisna od konkretnega primera uporabe, tehničnih zmožnosti uporabniške naprave in zahtev glede zasebnosti. Možnost uporabe in izbira konkretnih tehnologij ZKP je še vedno predmet razprave v skupinah EU, ki se ukvarjajo s pripravo ARF in tehničnih specifikacij, zato končni mehanizmi uporabe ZKP še niso potrjeni.

Za ilustracijo je v nadaljevanju naštetih nekaj primerov uporabe ZKP v EUDIW:

- Uporabnik želi dokazati, da je starejši od 18 let, za dostop do spletne trgovine ali dogodka. ZKP omogoča, da se iz potrdila izlušči zgolj ta podatek, ne da bi se razkril točen datum rojstva, ime ali kakršna koli druga osebna informacija.
- Namesto CAPTCHA lahko spletne strani uporabijo ZKP, s katerim uporabnik dokaže, da je človeško bitje s potrjeno identiteto. Rešitev povečuje dostopnost, zlasti za invalide, in zmanjšuje zlorabe.
- Uporabnik, ki večkrat obišče isto spletno stran, se lahko identificira z istim psevdonimom, brez razkrivanja svoje identitete. ZKP omogoča takšno vezavo prek derivacij atributov, ki ostajajo skriti.
- ZKP podpira t. i. "privacy-preserving revocation", kjer se lahko preveri, ali je potrdilo še veljavno, ne da bi razkrili identitete uporabnika ali podatka o njegovi dejavnosti.

5 Zaključek

Uvedba EUDIW je eden najambicioznejših projektov digitalne preobrazbe Evropske unije. Predstavlja tehnološki, pravni in organizacijski izziv, ki zahteva usklajeno sodelovanje vseh držav članic, razvijalcev, zakonodajalcev, ponudnikov storitev in končnih uporabnikov.

Ključ do uspešne uvedbe leži v vzpostavitvi trdnega zaupanja med vsemi deležniki. To zaupanje lahko temelji le na transparentnih pravilih, interoperabilnih standardih, varnosti ter učinkovitem varovanju zasebnosti. Tehnologija ZKP se v tem kontekstu kaže kot nepogrešljiv gradnik, saj ščiti uporabnika pred neželenim razkritjem podatkov in hkrati poenostavlja protokole za preverjanje identitete. Vendar pa so končne zahteve glede uporabe ZKP še predmet razprav in usklajevanja med državami članicami in komisijo. Pričakovati je, da se bo razprava na to temo nadaljevala v drugi polovici leta 2025.

Literatura

[1] Uredba (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu, https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng, pridobljeno 1. 8. 2025

[2] Uredba (EU) 2024/1183, https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng, pridobljeno 1. 8. 2025

[3] Uredba (EU) št. 2016/67, https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016R0067, pridobljeno 1. 8. 2025

[4] EUDI Wallet Architecture and Reference Framework 2.4.0, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework, pridobljeno 1. 8. 2025

[5] European Digital Identity Wallet, https://www.digital-identity-wallet.eu, pridobljeno 1. 8. 2025

[6] EUDI Wallet Consortium, https://eudiwalletconsortium.org, pridobljeno 1. 8. 2025

[7] NoBID Consortium, https://www.nobidconsortium.com, pridobljeno 1. 8. 2025

[8] DC4EU, https://www.dc4eu.eu, pridobljeno 1. 8. 2025

[9] ETSI TR 119 476 V1.2.1, https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.02.01_60/tr_119476v010201p.pdf, pridobljeno 1. 8. 2025

[10] EU Digital Identity Wallet , https://eu-digital-identity-wallet.github.io, pridobljeno 1. 8. 2025